

Guildhall Gainsborough
Lincolnshire DN21 2NA
Tel: 01427 676676 Fax: 01427 675170

AGENDA

This meeting will be recorded and the video archive published on our website

Corporate Policy and Resources Committee

Thursday, 13th April, 2017 at 6.30 pm

Council Chamber - The Guildhall, Marshall's Yard, Gainsborough, DN21 2NA

Members: Councillor Jeff Summers (Chairman)
Councillor Mrs Anne Welburn (Vice-Chairman)
Councillor Owen Bierley
Councillor Matthew Boles
Councillor David Cotton
Councillor Michael Devine
Councillor Adam Duguid
Councillor Steve England
Councillor Ian Fleetwood
Councillor John McNeill
Councillor Tom Regis
Councillor Reg Shore

1. Apologies for Absence

2. Public Participation Period

Up to 15 minutes are allowed for public participation. Participants are restricted to 3 minutes each.

3. Minutes of Previous Meeting/s

To confirm as a correct record the Minutes of the previous meeting on 9 February 2017 and the Special meeting on 28 February 2017.

a) For Approval

To confirm as a correct record the Minutes of the previous meeting on 9 February 2017 and the Special meeting on 28 February 2017. (PAGES 1 - 16)

b) For Noting

Joint Staff Consultative Committee meetings on 30 January and 2 March 2017 (PAGES 17 - 24)

Agendas, Reports and Minutes will be provided upon request in the following formats:

Large Clear Print: Braille: Audio: Native Language

4. **Declarations of Interest**
Members may make declarations of Interest at this point or may make them at any point in the meeting.

5. **Matters Arising Schedule** (PAGES 25 - 26)
Setting out current position of previously agreed actions as at 5 April 2017

6. **Public Reports for Approval:**
 - a) Fixed Term Contract Procedure (PAGES 27 - 40)
 - b) Bullying and Harassment Policy (PAGES 41 - 62)
 - c) Review of Information Governance Policies (2) (PAGES 63 - 208)
 - d) Implementation of PCI-DSS Security Policy (PAGES 209 - 226)
 - e) Mayflower 400 Resources (PAGES 227 - 230)
 - f) Gainsborough Transport and Development Study (PAGES 231 - 240)
 - g) Commercial Delivery Plan 12 month update (PAGES 241 - 272)
 - h) Committee Work Plan (PAGES 273 - 274)

7. **Exclusion of Public and Press**
To resolve that under Section 100 (A)(4) of the Local Government Act 1972, the public and press be excluded from the meeting for the following item of business on the grounds that it involves the likely disclosure of exempt information as defined in paragraph 3 of Part 1 of Schedule 12A of the Act.

8. **Exempt Report/s**
 - a) Commercial Investment Portfolio

M Gill
Chief Executive
The Guildhall
Gainsborough

Wednesday, 5 April 2017

This page is intentionally left blank

Corporate Policy and Resources Committee- 9 February 2017
Subject to Call-in. Call-in will expire at 5pm on Tuesday 21 February 2017

WEST LINDSEY DISTRICT COUNCIL

MINUTES of the Meeting of the Corporate Policy and Resources Committee held in the Council Chamber - The Guildhall, Marshall's Yard, Gainsborough, DN21 2NA on 9 February 2017 commencing at 6.30 pm.

Present: Councillor Jeff Summers (Chairman)
Councillor Mrs Anne Welburn (Vice-Chairman)

Councillor Owen Bierley
Councillor David Cotton
Councillor Michael Devine
Councillor Adam Duguid
Councillor Steve England
Councillor Ian Fleetwood
Councillor John McNeill
Councillor Tom Regis
Councillor Reg Shore

In Attendance:

Ian Knowles	Director of Resources and S151 Officer
Eve Fawcett-Moralee	Director Economic & Commercial Growth
Tracey Bircumshaw	Financial Services Manager
Steve Anderson	Information Governance Officer
Mark Sturgess	Chief Operating Officer
Dinah Lilley	Governance and Civic Officer

Apologies: Councillor Matthew Boles

Membership: No substitutes were appointed

94 PUBLIC PARTICIPATION PERIOD

There was no public participation.

95 MINUTES OF PREVIOUS MEETING/S

- a) **RESOLVED:** That the minutes of the Corporate Policy and Resources Committee meeting of 12 January 2017 be approved as a correct record.
- b) **RESOLVED:** That the minutes of the Joint Staff Consultative Committee meeting of 24 November 2016 be noted.

96 DECLARATIONS OF INTEREST

There were no declarations of interest at this point of the meeting

97 MATTERS ARISING SCHEDULE

The Governance and Civic Officer updated the Committee on the Matters Arising in terms of Councillor Shore's previous question on Flexible Working. In the three previous years there had been 13, two and seven requests respectively, all of which had been granted, bar one. As far as the implications and impact on the authority were concerned, each case was assessed on an individual basis, according to particular circumstances and the effects were difficult to quantify.

It was noted that this was almost 100%. The Chairman questioned the effects of remote working and its impact. The Chairman of the Joint Staff Consultative Committee stated that there was a legal requirement that if a request was made for remote working then there had to be valid, justifiable reasons to deny that request. Concerns were expressed that few staff would be available in the office, however even when working remotely staff should still be contactable, subject to connectivity.

98 REVIEW OF INFORMATION POLICIES

The Information Governance Officer presented the report stating that there was a requirement to review and maintain policies on a regular basis to comply with legislation. The report presented the first five of a range of policies to be reviewed, these being:-

- **Data Protection Policy**
- **Information Management and Protection Policy**
- **Data Quality Policy**
- **Remote Working Policy**
- **IT Access Policy**

The changes made to each policy were set out at the end of the report and the policies themselves at appendices a)-e).

The reviewed policies had been considered by the Council's Management Team and the Joint Staff Consultative Committee and recommended to the Corporate Policy and Resources Committee for approval.

RESOLVED that:

- a) the attached information policies for implementation to all staff, elected members, and partners where appropriate, be approved; and
- b) delegated authority be granted to the Director of Resources to make minor housekeeping amendments to the policies in future, in consultation with the chairmen of the Corporate Policy and Resources Committee and Joint Staff Consultative Committee.

99 PROGRESS & DELIVERY Q3

The Chief Operating Officer introduced the Progress and Delivery report for the third quarter, which highlighted the authority's Services.

The summary was structured to highlight those areas that were performing above expectations, those areas where there was a risk to either performance or delivery and those areas where further work was required for next year's report.

Areas described as performing well included: Building Control; Development Management; Projects and Growth; and the Trinity Arts Centre.

Those areas described as risks included: Local Land Charges; Enforcement; Markets; and Home Choices.

Further information was given on each of the above. Data relating to Complaints, Comments and Compliments were being reconsidered to present a more sophisticated way of monitoring. A measure around section 106s and CIL was also to be introduced to give members greater visibility. A further report specific to Markets was to be submitted to the Prosperous Communities Committee in due course.

One Member noted that a pattern had emerged over the years and that things such as sickness absences and markets were continually risk issues and did not appear to ever be resolved. Although it was good that the Trinity Arts Centre was now showing good progress, but was it actually making a profit?

The Chief Operating Officer responded to the points raised and stated that sickness absence rates were due primarily to a particular work area due to the nature of the work and the age profile of the staff, the figures were expected to fall. Regarding Trinity Arts, it was noted that, as a Grade II listed building, there would be a cost to close the establishment and that it did cover its running costs, and was a social asset to local residents. It was suggested that care was needed not to subsidise a Gainsborough asset at the expense of other areas in the district, however there was no subsidy involved.

The Chairman of the Joint Staff Consultative Committee responded to the comments on sickness absences and noted that West Lindsey was one of the best performing authorities compared with its benchmarked neighbours, and was a caring authority which would be sympathetic to an individual with a long term or serious illness.

Issues around recycling rates were then discussed, whilst the data was awaited it was felt important to know the contamination rates as this had implications for the new Technically, Environmentally and Economically Practicable (TEEP) legislation, as if contamination was high then recycling was not working. The Chief Operating Officer agreed that this was a good point and he would look into gaining statistics and work with the Operations Team Manager. It was agreed that there was room for promotion and education in the matter.

Note was made of the Leisure provision at De Aston and Caistor to be addressed within the new contract, and the Caistor Heritage Initiative, and the Ward Member for Caistor extended an invitation to Members to see the achievements made in the area.

The publication of the Housing White Paper was welcomed and addressed some outstanding issues, and it was hoped that West Lindsey would take part in the consultation through the Prosperous Communities Committee. The final section of the White Paper included reference to the Community Infrastructure Levy (CIL) of which it was important for Members to be aware. The Chief Operating Officer noted the next sessions of Planning Training for Members could include a session on CIL and dates for the next year would be issued shortly.

The Economic and Commercial Growth Director informed Members that the authority was writing its own Housing Strategy and the Improvement Plan would be submitted for Committee consideration and could perhaps be utilised as the authority's response to the White Paper.

The Chairman requested that the Chief Operating Officer undertake discussions with himself regarding the development of leisure facilities at Caistor Top, and also provide Schedule of BC Inspections and the process taken.

RESOLVED that having reviewed the performance information contained in the Progress and Delivery Report, the report be accepted.

100 CORPORATE PLAN

The Director of Resources introduced the Corporate Plan report, reminding Members that the Plan had been signed off last year and it had been agreed to produce an Action Plan to set out delivery intentions. Appendix 1 showed the key strategic actions which matched the Corporate Plan themes and were colour coded accordingly. A summary leaflet was to be produced for publication and wider circulation. Appendix 2 of the report showed the actions undertaken and the progress made.

The report was moved and seconded for approval and on being voted upon it was

RESOLVED that:

- a) the key activity detailed within the report which will facilitate the delivery of the objectives of the Corporate Plan be supported;
- b) the activity set out be used as the basis for an external publication be agreed; and
- c) the report be approved for submission to Council on 6 March 2017.

101 BUDGET AND TREASURY MANAGEMENT Q3

The Financial Services Manager informed Members of the Committee that the Council was currently forecasting a £560k surplus (after taking into account carry forwards of £238k, the significant element of which related to projects which were being funded from earmarked reserves and which would continue into the new financial year). There was a reduction of £15k since the Quarter 3 forecast. The major variances being contained within the report.

With regard to capital out turn forecasts this was expected to be £9.4m, a request for approval by this Committee of carry forwards totalling £1.9m where schemes and potential acquisitions were now likely to continue into the new year. The details of which could be found at Page 15 of the report.

Items of note were the use of Earmarked Reserves at paragraph 2 and successful grant bids at paragraph 3.

With regard to Treasury Management investment rates were at an all time low with overnight money at 0.26%. However the Council continued to exceed its benchmark and had achieved a rate of 1.17% compared to 0.23%.

There had been no breaches of prudential indicators and no actual borrowing undertaken.

The previous Committee Chairman welcomed the fact that interest rates had improved over time, and the Members commended the report without further discussion.

RESOLVED

- a) the forecast out-turn position as at 31 December 2016 be accepted;
- b) the use of Earmarked Reserves approved by the Director of Resources using Delegated powers be accepted;
- c) the amendments to the Capital and Revenue budget, including creating budgets for projects funded by grants and not included in the original Capital Programme be approved;
- d) the Capital budget carry forwards of £1,879k and Revised Capital Budget of £9,707k be approved; and
- e) the Treasury Management Report and Treasury position to 31 December 2016 be accepted.

102 REVENUE BASE BUDGETS 2017-18

The Financial Services Manager presented the Committee's base budget for 2017/18 as well as those recommended by Prosperous Communities Committee, and noted that a high audit assurance had been received.

The base budget showed a £1m reduction against the 2016/17 base budget.

The significant variances were contained within the report, the capital investment of £13m in commercial property was expected to achieve a net additional income of £270k, with £625k being reflected in the Committee's services base budget.

The withdrawal of the LCTS grant to Parish Councils previously approved by this Committee contributed a further £169k towards this saving.

One other outstanding consideration for this Committee in relation to the proposed increase in burial charges and members were referred to paragraph 1.5 within the report. The overall budgetary impact of a stepped change over two years would result in additional income in year 2 of £381. There was no budgetary impact from the removal of charges for exclusive rights of burials for children under 12. The Committee were now requested consider their

recommendation to Council.

Note Councillor David Cotton declared a personal interest on this item as in his ministerial capacity he conducted burials.

Discussion ensued on the burial costs with it being questioned that in the second year of increase, a further 65% would equate to greater than 130% in total. Clarification was sought on the actual figures rather than percentages, these were read out by the Financial Services Manager. The Director of Resources stated that the second year increase could be at the percentage necessary to equal 130% in total, if Members preferred.

It was affirmed that only two burial grounds were affected and that these had had six burials in the last year. The authority was below the benchmark figure and the service was below cost recovery. Charges were not increased for customers when from out of the area as was the case with some cemeteries and crematoria. This could be borne in mind for future cost assessments.

With the amendment as agreed the Committee Members moved, seconded and voted upon the recommendations.

RESOLVED that:

- a) having given consideration to the Fees and Charges, in relation to burials, it to be recommended to Council, that the increase be 65% for the first year, and increasing further to a total of 130% for the two year period;
- b) the Corporate Policy and Resources Committee Budget 2017/18 be approved and recommended to Council for inclusion in the Medium Term Financial Plan 2017/18 – 2021/22; and
- c) the Prosperous Communities Committee Budget be accepted and recommended to Council for inclusion in the Medium Term Financial Plan 2017/18 – 2021/22.

103 FINANCIAL STRATEGY AND MEDIUM TERM FINANCIAL PLAN 2017/18 TO 2021/22

The Director of Resources introduced the report which set out the financial context both local and national within which the budget and council tax for 2017/18 had to be agreed.

The paper was based on the provisional settlement announced on 15 December 2016, (the final settlement was expected in the next week or so) and would need to reflect any changes in the final paper for full Council. The final position on NNDR was also awaited due to late changes required by Government on the method of calculation

The document was the Council's primary strategic financial document and met a number of regulatory requirements. Firstly the authority was required to agree a balanced budget for the coming financial year 2017/18. Secondly the requirement to set the level of council tax, and also meet the best practice of setting the 17/18 budget in a medium term context

The Financial Plan was designed to deliver the corporate objectives set out in the Corporate

Plan 2016-20 which were covered in paragraph 2 of the Executive Summary.

Over the last four years the authority had delivered bottom line improvements of £4.4m through efficiencies and income generation. Efficiencies and increased income were continually sought through the five year plan and it was possible to show that the plans deliver a balanced budget for the next two years. With a deficit of over £400k remaining in 2020/21. This was in an environment where the authority's core spending power, as calculated by Government had reduced over that time by 11% and the Government Grant had reduced by £2m since 2015/16. The reduction from 16/17 to 17/18 was £626k.

The balanced position was achieved primarily by the assumptions as set out in paragraph 4.11.2

- Employee Pay Award 1% per annum
- Council Tax increase at £4.95 per annum and growth 0.5%
- Commercial Property Investment of £20m to generate £0.6m savings by 2020/2021
- No growth in NNDR
- Contractual inflation only applied to service expenditure budgets
- 4 year funding settlement in line with draft figures issued by Government
- New Homes bonus is based on Government estimates and payable over 4 years.
- NNDR 1.8% (August RPI)
- Electricity 4%
- Gas 4% from 2018/19
- Capital Programme – total investment; total borrowing; use of reserves; balances at end of five years

During the year a number of initiatives, projects and reviews were undertaken with the aim of achieving £2m of savings in five years. The projected savings requirement for 2017/18 was £0.382m. The Council had been successful in identifying these savings against this target. The significant savings have been achieved from;

- Budget and service reviews £0.147m
- Fees and Charges £0.043m
- Staffing Restructures £0.231
- Removal of Localisation of Council Tax Support (LCTS) Parish Grant £0.169m
- Contract Renewals £0.520m
- Planning Fee Income £0.086

This was against pressures identified during the budget process and legislative impacts

- No charging for Green Waste in 2017/18 £0.502m
- Apprenticeships incl Levy £0.48m

In addition to the above the continued focus on maximising New Homes Bonus through capital investment and identification and intervention measures relating to empty homes had resulted in a further £0.208m per annum of additional grant having been generated. However the New Homes Bonus scheme had been reviewed and allocations would be for a four year period reduced from a six year period. Further reductions may be required in future years to support other public services. The total allocation for 2017/18 was £1.889m. Future projections were based on Government estimates.

The Council continued to set aside New Homes Bonus to support growth and housing regeneration investment (many other authorities require this grant to support their revenue budgets).

The Medium Term Financial Plan also included an ambitious Capital Programme of over £53m which was to be funded from a mix of our own reserves, Grant Funding and borrowing.

Appendix M to the Strategy provided Members with a comparison against other authorities using standard financial measures and due to the level of reserves West Lindsey compared reasonably well in many areas.

The Rural Services Network representative thanked the authority for taking the lead role in the previous year in lobbying for a better settlement for rural areas, the same success was not expected for the 2017/18 year. Reductions in Government funding were greater for rural areas and the gap was widening. It was necessary to take all opportunities to lobby for rural support.

The changes to the New Homes Bonus were unprecedented. The Council currently used this to support regeneration investment, however in future years this may be required to support other public services.

Members gave further consideration to the proposals and the recommendations were moved and seconded, and on being voted upon it was **RESOLVED** that:

- a) the Draft Financial Strategy and Medium Term Financial Plan 2017/18 to 2021/22 (which may be subject to change once the final settlement is announced) be recommended to Council for approval;
- b) the Capital Investment Programme 2017/18 to 2021/22 be recommended to Council for approval; and
- c) any housekeeping changes (including any required by the final settlement) be delegated to the Draft Financial Strategy and Medium Term Financial Plan to the Director of Resources following consultation with the Chairman of the Corporate Policy and Resources Committee prior to the final consideration by Council on 6 March 2017.

104 COMMITTEE WORK PLAN

RESOLVED that the Work Plan be noted.

105 EXCLUSION OF PUBLIC AND PRESS

RESOLVED that under Section 100 (A)(4) of the Local Government Act 1972, the public and press be excluded from the meeting for the following items of business on the grounds that they involve the likely disclosure of exempt information as defined in paragraph 3 of Part 1 of Schedule 12A of the Act.

106 SUN INN AND JOINT VENTURE COMPANY

Councillor Cotton sought clarification regarding the item in terms of those Councillors who were also Members of the Planning Committee. The Director of Resources assured Members that the project was for 'in principle' agreement only at this time, and should an application be presented to the Planning Committee in due course, Members of this Committee should then declare their involvement at that time.

The Economic and Commercial Growth Director reminded Members that 'in principle' approval had been agreed in September 2016, by both the Prosperous Communities and Corporate Policy and Resources Committees, following which negotiations had continued with the developer, and the viability gap acknowledged.

Members had acknowledged that securing a hotel in Gainsborough would have a significant and positive economic impact on the town; and with regard to the joint venture company the strong rationale as summarised below:

- DPL/NSGL ownership of the adjacent property required to deliver a hotel;
- DPL's matching funding with the Council's equity share investment;
- DPL's track record of delivering successful regeneration in the town;
- enabling the Council to deliver key regeneration objectives and generate potential commercial return to the Council.

In short, both projects would accelerate the physical and economic regeneration of the town centre. Officers at that time had been delegated to negotiate and prepare a Grant Funding Agreement (GFA). Joint Venture Agreement (JVA) and Articles of Association in line with the Heads of Terms agreed by these committees.

When first considering these proposals Members stressed the importance of securing high quality development and the need to maximise the environmental and regenerative impact of the projects to be commensurate with the level of Council support. In response to this Officers had worked up the Joint Venture Agreement, and Articles of Association to incorporate a wider area of benefit, to include Market, North and Church Streets and Market Place.

The Council and its commercial advisors had continued to work on an "open book" basis with DPL to scrutinise the cost and value of the hotel. A detailed scheme had been worked up and would form a planning application to be submitted to a future meeting of the Planning Committee.

Officers had augmented and quantified the business case to support the redevelopment of the hotel and restaurant, and Joint Venture Company through a bespoke economic impact

assessment undertaken by an independent specialist 31TEN.

Further specialist legal advice had been taken in developing these proposals specifically with regards to State Aid and procurement, in addition to in-house legal advice, which had appraised the final suite of agreements to implement the recommendations. These Agreements followed the Heads of Terms Members agreed in September/October 2016 and provided a robust basis to manage the release of the Council's funding, delivery of outputs and ensure value for money.

Members debated the report and its proposals at some length and generally agreed that this was an exciting opportunity to develop part of the town. Concerns were however expressed at the lack of a Councillor on the board, as this was felt to be an opportunity to have close scrutiny. It was clarified however that a Councillor's primary role was allegiance to West Lindsey District Council, but as a board member would be required to support the company which would lead to a conflict of interest. It was therefore recommended that one of the Council's independent Governance and Audit Committee Members be allocated the place on the board, which would alleviate that conflict.

Officers were congratulated for undertaking a thorough job on the project, and that the risks had been mitigated as far as was possible. This would be a bold and enterprising venture and would turn Gainsborough's fortunes and perception positively.

RESOLVED that:

- a) the Council enters into a Grant Funding Agreement (as attached as Appendix 1 to the report), to enable the redevelopment of the Sun Inn to a new 56 bedroom hotel with an independent ground floor restaurant, be approved;
- b) the Council becomes a member of Market Street Renewal Limited (a 50/50 joint venture company with DPL to facilitate the regeneration of Market, Church and North Streets and Market Place area) by subscribing for shares in the company in accordance with the Joint Venture Agreement, Articles of Association and associated company formation documents (attached at Appendix 2 to the report), be approved;
- c) the Council enters into the Joint Venture Agreement, and the Shareholders Loan Agreement (attached as Appendix 2 to the report) to form, finance and govern the operation of "Market Street Renewal Limited", be approved;
- d) the release of the requisite funding set out in recommendations a), b) and c) above and to include a capped grant of up to £1,400K to NSGL, pursuant to the GFA, and loan funding of £250K pursuant to a Shareholders Loan Agreement to Market Street Renewal Limited, be approved;
- e) the sale of the Council's long leasehold interest in properties in North Street into Market Street Renewal Limited at market value subject to a business case and in compliance with the Council's Disposal Policy be approved in principle;
- f) the appointment of the Economic and Commercial Growth Director plus one other officer or independent, as Directors of Market Street Renewal Limited and approve that the Council enters into the Deed of Indemnity (attached as Appendix 3 to the report) in respect of each such appointee, be agreed;
- g) the appointment of the Director of Resources to represent the Council as

- the shareholder in Market Street Renewal Limited, be agreed;
- h) delegation be given to the Chief Executive, following consultation with Chairmen of Corporate Policy and Resources and Prosperous Communities Committees, to take such decisions and execute such documents as shall give effect to the above decisions.

107 SURE STAFF BUSINESS PLAN

The Director of Resources introduced the report which had been agreed to be required to provide an annual business plan for consideration.

The background was set out in the executive summary:

The original proposal to buy Surestaff was based on four potential benefits:

- To have a reliable local provider of agency staff to WLDC
- To minimise the cost of managing suppliers within the Operational establishment (cost avoidance)
- To generate an income stream from charged in services
- To generate a shareholder return

The report provided an update on current performance and had the full business plan for the following three years attached.

The acquisition of Surestaff had proved to be a success from a business perspective, with a smooth re-entry into the market following the previous “winding down” of the agency. Losses were expected to be relatively small over the first two years with an overall benefit to the Council when recharged income, costs avoided and security of supply were taken into account. Over the longer term, these indirect benefits would be supplemented by a stream of positive profit contributions generated by the new venture.

A recent reforecast, compiled on a relatively prudent basis, illustrated the potential for a positive contribution resulting from a local enterprise which was already generating a social return for the local communities of WLDC.

Members sought assurance on the ethical aspect of the company, that agency staff were not exploited through desperation, nor being employed to replace permanent workers at a cheaper rate on zero hours contracts.

The Director of Resources reassured members that the Council’s own arrangements were to cover needs at particular, usually seasonal, times. Contracts were temporary rather than part-time, and staff were paid at similar rates to permanent staff. There was no evidence that agency staff were replacing permanent jobs, however as a shareholder he would raise this with the board.

It was acknowledged that agency work could be a route for individuals to get into work, and it could also suit some individuals to be temporary instead of permanent.

Note was made of the intention to not continue the employment of migrant workers for practical/ethical reasons.

Reference was made to the reduced gross margin prediction set out on page 10 of the report. The Director of Resources responded that whilst the profit margins were currently less than predicted, the intention was that there would be two companies, one of which would be TECKAL, which would enable services to be provided to other local authorities, and this would make a positive contribution to the bottom line of the Council and it was hoped for profit in year 3.

RESOLVED that the Business Plan be **RECOMMENDED** to Council, as the single shareholder, for agreement.

The meeting concluded at 8.38 pm.

Chairman

WEST LINDSEY DISTRICT COUNCIL

MINUTES of the Meeting of the Corporate Policy and Resources Committee held in the Council Chamber - The Guildhall, Marshall's Yard, Gainsborough, DN21 2NA on 28 February 2017 commencing on the rising of the Prosperous Communities Committee, at 7.36pm.

Present: Councillor Jeff Summers (Chairman)

Councillor Sheila Bibb
Councillor Owen Bierley
Councillor Matthew Boles
Councillor David Cotton
Councillor Michael Devine
Councillor Adam Duguid
Councillor Steve England
Councillor Ian Fleetwood
Councillor John McNeill
Councillor Sheila Bibb

In Attendance:

Manjeet Gill	Chief Executive
Ian Knowles	Director of Resources and S151 Officer
Alan Robinson	SL - Democratic and Business Support
Dinah Lilley	Governance and Civic Officer
Eve Fawcett-Moralee	Director Economic & Commercial Growth
Jo Walker	Team Manager Projects and Growth
Manjeet Gill	Chief Executive

Apologies: Councillor Mrs Anne Welburn
Councillor Tom Regis
Councillor Reg Shore

Membership: Councillor Sheila Bibb substituted for Councillor Welburn

108 DECLARATIONS OF INTEREST

Councillors England, Bierley, Devine and Bibb declared that they had sat on the previously held Prosperous Communities Committee but retained an open mind as to the proposals for this meeting.

109 EXCLUSION OF PUBLIC AND PRESS

RESOLVED that under Section 100 (A)(4) of the Local Government Act 1972, the public and press be excluded from the meeting for the following items of business on the grounds that they involve the likely disclosure of exempt information as defined in paragraph 3 of Part 1 of Schedule 12A of the Act.

110 DEVELOPMENT PARTNER

The report before the Committee, having been circulated previously, contained the legal and financial implications of the proposals.

The Council proposed to enter into a joint venture company (limited by shares) with its preferred partner in due course, and subject to testing through the ISOP process. The purpose of the joint venture company was to regenerate West Lindsey and generate a commercial return over the medium to long term.

Funding had been earmarked for the Development Partnership to support the regeneration programme and would be seeking not only regeneration but a potential commercial return in addition to business rates. A grant bid had also been made to support housing delivery via the Greater Lincolnshire Local Enterprise Partnership. The procurement of specialist legal and commercial advice (via the NEPRO framework) had been approved in July 2016, funded from the Regeneration and Growth Earmarked Reserve.

The procurement process was being conducted in accordance with the Competitive Dialogue procedure pursuant to Regulation 30 of the Regulations which allowed development and financial solutions to be fully considered and refined with a shortlist of pre-qualified developers. A key benefit of this procedure was the ability to commence the dialogue with a long list of sites/projects and test the cohesiveness and viability of “the preferred solution”.

Having given consideration to the proposals put to the Prosperous Communities Committee, (which immediately preceded the Corporate Policy and Resources meeting and at which all Corporate Policy and Resources Members were present), and the details as set out in the powerpoint presentation, and having raised relevant questions during that meeting, Members were satisfied that they had been provided with sufficient information to make the decisions as recommended by the Prosperous Communities Committee, as per the minute below.

... it was unanimously **RESOLVED** that:

- a) it be recommended to the Corporate Policy and Resources Committee, that the proposed ISOP documents appended to the report be approved;
- b) it be recommended to Corporate Policy and Resources Committee that subject to further testing of the legal structures, in principle the Council enters into a Joint Venture with a selected development partner for the delivery of the regeneration programme as part of the ISOP process;
- c) it be agreed to delegate any final changes to the ISOP document to the Chief Executive, following consultation with the Chairs of Prosperous Communities and Corporate Policy and Resources Committees; and
- d) it be recommended to Corporate Policy and Resources Committee, that a further budget of £75,000 to support and conclude the procurement process for the development partner and legal costs of the creation of the Joint Venture

Company, to be funded from the Investment for Regeneration and Growth Earmarked Reserve, be approved.

The recommendations set out in the report and the minute above were moved and seconded, and Committee Members called for the vote to be taken. The Chairman verified that no Members had any further questions for officers and moved to the vote.

It was therefore **RESOLVED**, unanimously, that:

- a) the proposed ISOP documents appended to the report be approved;
- b) subject to further testing of the legal structures, in principle the Council enters into a Joint Venture with a selected development partner for the delivery of the regeneration programme as part of the ISOP process;
- c) delegation be agreed for any final changes to the ISOP document to the Chief Executive, following consultation with the Chairs of Prosperous Communities and Corporate Policy and Resources Committees; and
- d) a further budget of £75,000 to support and conclude the procurement process for the development partner and legal costs of the creation of the Joint Venture Company, to be funded from the Investment for Regeneration and Growth Earmarked Reserve, be approved.

The meeting concluded at 7.42 pm.

Chairman

This page is intentionally left blank

WEST LINDSEY DISTRICT COUNCIL

MINUTES of a Meeting of the Joint Staff Consultative Committee held in the Council Chamber at the Guildhall, Gainsborough on Monday 30 January 2017 commencing at 4.00pm.

Present: Councillor David Cotton (Chairman)
Councillor Matthew Boles
Councillor Jackie Brockway
Councillor Jessie Milne

Representatives of Union members: Paul Key
Karen Lond (Vice-Chairman)

Representatives of Non union staff: Kate Hearn
Rachel Parkin

In attendance:
Alan Robinson Monitoring Officer
Emma Redwood Team Manager – People and Organisational Development
Steve Anderson Information Governance Officer
Katie Coughlan Governance and Civic Officer
Jana Randle Governance and Civic Officer

Also in Attendance: Helen Stokes, UNISON - Lincoln Branch Secretary

Apologies: No formal apologies received

40 MINUTES (JSCC.28 16/17)

(a) Meeting held on 24 November 2016

RESOLVED that the Minutes of the meeting of the Joint Staff Consultative Committee held on 24 November 2016 be confirmed and signed as a correct record.

41 MEMBERS' DECLARATIONS OF INTEREST

There were no declarations of interest made.

42 MATTERS ARISING SCHEDULE (JSCC.28 16/17)

Members gave consideration to the Matters Arising Schedule which set out the current position of all previously agreed actions as at 24 November 2016.

It was noted that all actions had been completed.

RESOLVED that progress on the matters arising schedule as set out in report JSCC.28 16/17 be received and noted.

43 NEW BULLYING AND HARASSMENT POLICY (JSCC.30 16/17)

The Committee gave consideration to a report which presented a new Bullying and Harassment Policy for consideration and subsequent adoption by the Corporate Policy and Resources Committee.

The Council had a Bullying and Harassment Policy in place, however due to updates in legislation, changes to the Acas definition and incorporating best practice a review had been required to provide employees with the most up to date information. Rather than making amendments a new policy had been written.

The policy would apply to all staff including employees, contractors, casual and agency staff and volunteers of the organisation for matters relating to issues of bullying or harassment and directed staff to resolve matters through an informal as well as a formal process.

The policy covered all situations both within the workplace and in any work-related setting outside the workplace, including for example, business trips, conferences and work-related social events.

It was noted that the policy had been developed by the People and OD Team Manager. Independent advice had been sought from an external specialist. The policy had also been sent to Unison and staff reps for consultation. Staff reps had given positive feedback to support the new policy and Unison had indicated their support also.

In response to questions from the Lincoln Branch Secretary, the People and OD Team Manager confirmed that the new Policy moved away from the previous approach of having harassment advisors. The organisation was now smaller and capacity for this role was limited. However the Council did have an Employee Assistance Programme, through which staff could receive guidance and advice on range of matters including Bullying Harassment. It was also confirmed that members of the HR Team would be trained to deal with bullying and harassment cases. Training had already commenced around the organisation for a number of managers on related issues such as Dignity at Work and the Policy still had an emphasis on resolving such matters informally in the first instance.

It was suggested that a flow chart of the procedure be included in the Policy, to make it simple for both managers and staff to understand at a glance. The People and OD

Team Manager indicated she would be happy to include such a diagram, prior to submitting the Policy to the Corporate Policy and Resources Committee for formal adoption.

The Lincoln Branch Secretary further suggested that the Policy should include reference to the Whistle Blowing Policy and again the People and OD Team Manager indicated she would be happy to include a reference prior to submitting the Policy to the Corporate Policy and Resources Committee for formal adoption.

The Branch Secretary indicated she would be happy to review the proposed amends prior to submission to the Policy Committee.

The Lincoln Branch Secretary also requested that Unison representatives be included in any training and guidance offered to staff and Managers, in order that all understood the Policy and all were interpreting it in the same way. This would allow them to fulfil their role to the best of their ability.

RESOLVED that it be **RECOMMENDED** to the Corporate Policy and Resources Committee that: -

- (a) the Bullying and Harassment Policy be approved for formal adoption; subject to the inclusion of a flow chart of the process and reference to the Whistleblowing Policy being included; and
- (b) delegated authority be granted to the Director of Resources to make minor house-keeping amendments to the Policy in the future, in consultation with the Chairmen of the Corporate Policy and Resources Committee and Joint Staff Consultative Committee.

Note: Councillor Brockway joined the meeting at this point.

44 INFORMATION GOVERNANCE POLICY REVIEWS (JSCC.31 16/17)

The Committee were asked to give consideration to the first five, of a raft of Information Governance Policies which required review. These were the Data Protection Policy; the Information Management and Protection Policy; the Data Quality Policy; the Remote Working Policy; and the IT Access Policy. The purpose of each Policy was briefly summarised to the Committee, and was set out in the report, along with the main revisions which had been made to each policy and the reasons for change.

The Committee indicated they found the revision sheet pages, most useful and this approach should be adopted wherever possible.

In response to a questions it was confirmed that the new Password Policy had not been applied to the PSN Network.

RESOLVED that it be **RECOMMENDED** to the Corporate Policy and Resources Committee that: -

- (a) The Five Information Governance Policies, namely: -
- Data Protection Policy
 - Information Management and Protection Policy
 - Data Quality Policy
 - Remote Working Policy; and
 - IT Access Policy
- be approved for formal adoption; and
- (b) delegated authority be granted to the Director of Resources to make minor house-keeping amendments to the Policy in the future, in consultation with the Chairmen of the Corporate Policy and Resources Committee and Joint Staff Consultative Committee.

45 WORK PLAN (JSCC.32 16/17)

Members gave consideration to their future work plan as set out in report JSCC.32 16/17. It was noted that if any Committee Member wished to see a report on a particular issue, this could also be raised.

The Lincoln Branch Secretary urged the Committee to give some precedent to the Bomb Threat and Suspicious Package procedure, in light of recent events at other local authorities.

RESOLVED that the Work Plan, as set out in report JSCC.32 16/17 be received and noted.

46 TO NOTE THE DATE OF THE NEXT MEETING

- 30 March 2017 at 4.00 pm.

The meeting closed at 4.26 pm.

Chairman

Following an informal discussion at the conclusion of the meeting it was agreed to hold an additional meeting on 2 March to consider the next raft of Information Governance Policies.

WEST LINDSEY DISTRICT COUNCIL

MINUTES of a Meeting of the Joint Staff Consultative Committee held in the Council Chamber at the Guildhall, Gainsborough on Monday 2 March 2017 commencing at 4.00pm.

Present: Councillor Matthew Boles
Councillor Jackie Brockway
Councillor Jessie Milne

Representatives of Union members: Karen Lond (Vice-Chairman) (In the Chair)

Representatives of Non union staff: Kate Hearn
Rachel Parkin

In attendance:
Ian Knowles Director of Resources
Emma Redwood Team Manager – People and Organisational Development
Steve Anderson Information Governance Officer
Katie Coughlan Governance and Civic Officer

Apologies: No formal apologies received

47 MINUTES (JSCC.33 16/17)

(a) Meeting held on 30 January 2017

RESOLVED that the Minutes of the meeting of the Joint Staff Consultative Committee held on 30 January 2017 be confirmed and signed as a correct record.

48 MEMBERS' DECLARATIONS OF INTEREST

There were no declarations of interest made.

49 MATTERS ARISING SCHEDULE (JSCC.34 16/17)

Members gave consideration to the Matters Arising Schedule which set out the current position of all previously agreed actions as at 22 February 2017.

It was noted that all actions had been completed.

RESOLVED that progress on the Matters Arising Schedule as set out in report JSCC.34 16/17 be received and noted.

50 INFORMATION GOVERNANCE POLICY REVIEWS (PART 2) (JSCC.35 16/17)

- **DATA PROTECTION BREACH POLICY**
- **FREEDOM OF INFORMATION AND ENVIRONMENTAL INFORMATION POLICY**
- **RECORDS MANAGEMENT POLICY**
- **IT INFRASTRUCTURE SECURITY POLICY**
- **REMOVABLE MEDIA POLICY**

The Committee were asked to give consideration to the second five, of a raft of Information Governance Policies which required review. These were the Data Protection Breach Policy; the Freedom of Information and Environmental Information Policy; the Records Management Policy; the IT Infrastructure Security Policy; and the Removable Media Policy.

The purpose of each Policy was briefly summarised to the Committee, and was set out in the report, along with the main revisions which had been made to each policy and the reasons for change.

The Committee indicated they found the revision sheet pages most useful and this approach should be adopted wherever possible.

Members asked a number of questions in relation to the Policies.

In respect of the Data Protection Breach Policy, an Elected Member made reference to a previous IT incident at the County Council which had made it difficult for Officers to contact one another in the absence of IT systems. Officers confirmed that each Member of the 'Emergency Business Continuity Team' had several hard copies of the Plan, which included contact details, available in varying locations.

In relation to the Freedom of Information and Environmental Information Policy, it was confirmed that the fee related to an Environmental Information request only and was a statutory one, set at cost recovery and was included in the schedule of charges published by the Authority.

Regarding the Records Management Policy, any documentation which could be of future local historical or heritage value, was not destroyed but offered to the Lincolnshire Archive.

Finally, in relation to the Removable Media Policy, in response to the Committee's questions, Officers advised that all mobile phones were procured and configured by the IT department. Lost phones could be instantly wiped and shut down. Similarly with USB sticks; these were all procured by and issued through the IT Department. Furthermore, USB sticks were only issued to those employers who had an approved Business Case for use and were encrypted before issue. The introduction of the Lite Show technology had further reduced the need for USBs.

Employees not issued with a mobile phone by the Authority were permitted to have their work e-mails forwarded through, or synced, with their personal mobile devices. However, this was subject to them also agreeing to have a number of safeguards installed on their own personal devices, to facilitate quick data cleansing, in the event of loss, for example. This scenario was covered by the Bring Your Own Device to Work Policy, which would be submitted for the Committee's consideration at their next meeting.

There were no questions regarding the IT Infrastructure Security Policy.

On that basis it was:-

RESOLVED that it be **RECOMMENDED** to the Corporate Policy and Resources Committee that: -

- (a) The Five Information Governance Policies, namely: -
- Data Protection Breach Policy
 - Freedom Of Information And Environmental Information Policy
 - Records Management Policy
 - It Infrastructure Security Policy
 - Removable Media Policy
- be approved for formal adoption; and
- (b) delegated authority be granted to the Director of Resources to make minor house-keeping amendments to the Policy in the future, in consultation with the Chairmen of the Corporate Policy and Resources Committee and Joint Staff Consultative Committee.

51 WORK PLAN (JSCC.36 16/17)

Members gave consideration to their future work plan as set out in report JSCC.36 16/17. It was noted that if any Committee Member wished to see a report on a particular issue, this could also be raised.

RESOLVED that the Work Plan, as set out in report JSCC.36 16/17 be received and noted.

52 TO NOTE THE DATE OF THE NEXT MEETING

- 30 March 2017 at 4.00 pm.

The meeting closed at 4.33 pm.

Chairman

Corporate Policy & Resources Committee Matters Arising Schedule

Purpose:

To consider progress on the matters arising from previous Corporate Policy & Resources Committee meetings.

Recommendation: That members note progress on the matters arising and request corrective action if necessary.

Matters arising Schedule

Status	Title	Action Required	Comments	Due Date	Allocated To
Black	Housing Strategy	Minute Extract 09/02/17 The Economic and Commercial Growth Director informed Members that the authority was writing its own Housing Strategy and the Implementation Plan would be submitted for Committee consideration and could perhaps be utilised as the authority's response to the White Paper.	We are providing a response to DCLG for the 2nd May to the Housing White Paper based on the report to PC committee last week, discussion at committee and subsequent comments from members received by email. Officers supported by ARC 4 are preparing a Housing Strategy, to be ready later this month. This will address/implement the objectives of the White Paper.	21/03/17	Eve Fawcett-Moralee
	Recycling Contamination	Minute extract 09/02/17 The Chief Operating Officer agreed that (...) he would look into gaining statistics (of contamination of recycling) and work with the Operations Team Manager.	The issue has been looked at and whilst it is possible to record the proportion of contaminated waste in our recycling stream there are currently no resources available to make any changes should the level of contamination be at unacceptable levels. It therefore not recommended the a measure is included in the progress and delivery report concerned with contaminated waste.	13/04/17	Mark Sturgess

	Planning Training	The dates for the next year of Planning Training to be issued to Members and consideration be given to a session on CIL.	Next cycle of dates confirmed and circulated to all Members. CIL arranged for first session 11 June	15/06/17	Mark Sturgess
Green					
	Surestaff Business Plan	Minute extract 090217 There was no evidence that agency staff were replacing permanent jobs, however as a shareholder (IK) would raise this with the board.	Verbal update to be given at 13/04 meeting	31/03/17	Ian Knowles



**Corporate Policy and
Resources Committee**

13 April 2017

Subject: New Fixed Term and Temporary Contract Policy and Procedure

Report by:

Director of Resources
Ian Knowles

Contact Officer:

Emma Redwood
People & OD Team Manager
Emma.redwood@west-lindsey.gov.uk

Purpose / Summary:

To propose a new Fixed Term and Temporary
Contract Policy & Procedure for staff

RECOMMENDATION(S):

That Corporate Policy and Resources Committee approve the Fixed Term and Temporary Contract Policy & Procedure and the policy is adopted for all employees of the council.

Delegated authority be granted to the Director of Resources to make minor housekeeping amendments to the policy in future, in consultation with the chairman of the Corporate Policy & Resources committee and chairman of JSCC.

IMPLICATIONS

Legal: The main Acts and Regulations covering workers on fixed-term contracts are:

The Employment Act 2002

The Fixed-term Employees (Prevention of Less Favourable Treatment) Regulations 2002 (SI 2002/2034) which implement the provisions of the Fixed-term Work Directive (1999/70/EC) into UK law

The Fixed-term Employees (Prevention of Less Favourable Treatment) (Amendment) Regulations 2008 (SI 2008/2776).

Financial : None FIN/6/18

Staffing : None

Equality and Diversity including Human Rights :

West Lindsey District Council has a commitment to equal opportunities. It seeks to ensure that no potential or current employee receives less favourable treatment than another on the grounds of age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

Risk Assessment :

Climate Related Risks and Opportunities :

Title and Location of any Background Papers used in the preparation of this report:

Call in and Urgency:

Is the decision one which Rule 14.7 of the Scrutiny Procedure Rules apply?

i.e. is the report exempt from being called in due to urgency (in consultation with C&I chairman)

Yes

No

x

Key Decision:

A matter which affects two or more wards, or has significant financial implications

Yes

No

x

1. Introduction

The council employs some staff on temporary or fixed term contracts and as such it is good practice to have a policy and procedure document in place to ensure that guidance is given to managers and that the council meets the legislative requirements that are in place.

2. Purpose

The council recognises the importance of providing staff and managers with consistent information and guidance when navigating through the fixed term workers legislation and has therefore drafted and consulted on a new policy/procedure document,

3. Scope

The document applies to all staff employed on fixed-term or temporary contracts with the exception of:

- Apprentices
- Placement students
- Agency Workers

4. Engagement

The policy has been developed by the People and OD Team Manager and feedback has been sought from the management team, staff representatives and Unison, it has also been agreed by Legal Services.

The policy was considered at JSCC on 30th March 2017 and was fully supported by Members, Unison and Staff Representatives.

5. Training and Awareness

This policy will be made available to view on the Minerva site and hard copies available at the depots once formally agreed.

A clear communication will be sent to Managers to make them aware that the policy has been reviewed and to update them on their responsibilities.

6. Recommendation

That Corporate Policy and Resources Committee approve the Fixed Term and Temporary Contract Policy & Procedure and the policy is adopted for all employees of the council.

Delegated authority be granted to the Director of Resources to make minor housekeeping amendments to the policy in future, in consultation with the chairman of the Corporate Policy & Resources committee and chairman of JSCC.

Fixed Term And Temporary Contract Policy & Procedure

JSCC Approved – 30 March 2017

P&R Approved –

FIXED TERM AND TEMPORARY CONTRACTS POLICY & PROCEDURE

1. Purpose

The purpose of this policy and procedure is to explain the requirements of the legislation and to outline how fixed-term and temporary contracts will be used within the council.

2. Scope

This procedure applies to all staff employed on fixed-term or temporary contracts with the exception of:

- Apprentices
- Placement students
- Agency workers

3. Introduction

The Fixed-term Employees (Prevention of Less Favourable Treatment Regulations 2002), afford fixed-term or temporary employees important rights that have an impact on the use of such contracts, which include:

- The right not to be treated less favourably than a comparable employee on a permanent contract in respect of pay, contractual terms and conditions, the opportunity to receive training or be subjected to any other detriment on grounds of status as a fixed-term or temporary employee. However, where it is deemed appropriate, the council may adjust terms and conditions providing they can be objectively justified but be in line with the guidance in the section 'Objective Justification'.
- The right to a redundancy payment where the expiry (i.e. dismissal) of a fixed-term or temporary contract gives rise to a redundancy situation. This does not normally apply if the dismissal is for 'some other substantial reason' e.g. brought in to provide temporary cover, normally for less than 2 years.
- The right not to be selected for redundancy or be unfairly dismissed if the principal reason for the selection was because the employee is on a fixed term contract.
- Limiting the use of successive fixed-term contracts to no more than 4 years, after which a fixed-term or temporary contract should become permanent unless the continued use of a fixed-term contract can be justified on objective grounds.
- The right to be informed and have access to information regarding permanent employment opportunities within the organisation.

4. General Position

The employee on the fixed-term contract should not expect their employment to last longer than the term of the first contract. Should the contract be ended early i.e. before the contracted length of time then a dismissal will occur and the relevant notice period will apply.

A decision to offer, renew or not renew a fixed term or temporary contract places certain obligations on the council depending on the reason for the offer, renewal or non-renewal and the length of service accrued by the post-holder.

An employee on a fixed term or temporary contract may be eligible for a redundancy payment if they have previous continuous employment with an employer on the Redundancy Modification Order which takes them beyond two years by the final day of their employment. This is contractual and means that any redundancy pay due by the council will be based on all previous continuous employment. Depending on the length of continuous service, this could be costly. A period of seven calendar days, counts as a break in continuous service. See section 11

There is a statutory duty to appoint on merit and applicants who have previous continuous service with an employer on the Redundancy Modification Order should not be discounted because of this.

5. Difference between a Fixed-Term Contract and a Temporary Contract

A fixed-term contract will be issued to an employee when the end date or length of the contract is known. The contract must state clearly the reason for the fixed-term status to establish those specific elements of the role which could attract a redundancy payment; or whether the role is to provide cover, backfill etc.

A temporary contract will be issued to an employee when the end date or length of the contract is unknown, however, the contract will indicate the anticipated length of the contract. The contract should also state the reason for the temporary status.

6. When to use a fixed term or temporary contract

A fixed term or temporary contract is a contract that comes to an end:

- Upon reaching a specified date
- When a specific task has been completed; or
- When a specific event does or does not occur.

Managers should only use fixed term or temporary contracts for specific purposes. Some of the most common examples of when a fixed-term or temporary contract would be appropriate are:

1. Where funding for a particular post is dependent on external sources which cannot be guaranteed to continue in the long-term
2. Engaging employees to undertake seasonal work
3. Engaging employees to cover periods of peaks in demand
4. Implementation of a specific project
5. Cover for maternity leave, sickness absence etc.
6. Cover for secondment

7. Advertising a fixed-term or temporary contract

When advertising a fixed-term or temporary vacancy the advert must specify the length of the appointment (where this is known or the anticipated length must be specified) and the purpose of the contract. If there is a possibility of permanency or renewal on expiry period, this should also be included in the advert.

8. End of Fixed Term or Temporary Contract

The termination of a fixed-term or temporary contract, or non-renewal of a fixed-term or temporary contract beyond its expiry date is regarded as a dismissal.

The reason for the dismissal will be due to either:

Redundancy – for example where the requirement for the work to be undertaken has diminished or ceased

SOSR (Some other substantial reason) – for example where the requirement for the work to be undertaken has not reduced and the substantive post holder has returned to work or a permanent employee is recruited.

9. Non – Renewal

The non-renewal of a fixed term or temporary contract at the end of its natural expiry date constitutes a dismissal in law and as such care requires to be exercised to ensure that any such dismissal is procedurally fair.

In common with an employee with permanent contractual status, a temporary or fixed-term employee who has at least two year's continuous service will be entitled to lodge a claim of unfair dismissal to an Employment Tribunal (ET) claiming that the ending of their fixed term contract was not undertaken fairly. It should also be noted that an individual need not have had one year's continuous service to claim unfair dismissal if the reason for termination amounts to discrimination or one of the other automatically unfair reasons for dismissal.

The specific steps that managers should follow when ending a fixed term contract are set out at section 2 of this document.

In addition to following a fair procedure, additional obligations on the council may arise depending on the reason for non-renewal. For example, if a fixed term contract is for a purpose **other than maternity leave cover, cover for long- term sick absence or secondment etc**, the decision not to renew is likely to constitute dismissal on the grounds of redundancy and a redundancy payment entitlement will arise if the individual has accrued at least 2 years continuous service.

Employees who move from a permanent post to a temporary post in a redundancy situation, in order to avoid immediate redundancy, and who then reach the end of the temporary period in the new job and are not offered an extension or renewal, will normally be regarded as dismissed for redundancy, because in such cases the ending of their employment is mainly attributable to the original redundancy situation.

Cases which will normally not attract a redundancy payment include those where the employee was recruited on a temporary or fixed term basis to provide cover for another employee during that employee's absence on maternity, adoption or parental leave, or long term sick leave, or on secondment, or the employee is recruited to provide cover during a recruitment process to replace an employee who has left. The reason that a redundancy payment would not be payable in such cases is that the reason for the dismissal is the return to the post of the absent employee, not a reduction in the employer's requirements for employees to perform the particular job, this would be classed as a dismissal for Some Other Substantial Reason – SOSR.

10. Renewal

Managers must look at their establishment and their staffing regime and consider whether a fixed term or temporary contract is appropriate by weighing up the pros and cons of using them. If a vacant post is likely to be filled permanently then this should be considered at the outset.

Managers should be aware that after one year of continuous employment an employee has the right to be redeployed and an employee who has two or more year's continuous service may be entitled to receive a redundancy payment.

11. Does the post-holder have at least 2 years continuous service?

If a fixed term or temporary contract is not to be renewed and the circumstances are deemed to meet the statutory definition of redundancy (ie. non – renewal due to the cessation or diminution of the work being undertaken), a redundancy payment will be payable providing he or she has at least 2 years continuous service. Continuous service includes service with other public bodies listed under the Redundancy Modification Order. The RMO provides that continuous service with a local authority and other specified public bodies can be counted for the purpose of establishing entitlement to and calculation of redundancy/severance payments.

Where a post holder has a dual job, only the continuous service under the contract to be ended will be considered when determining whether a redundancy payment is payable.

There may be a pension consideration which could give rise to substantial pension fund strain costs. Such costs will require to be factored into the budget provision. You should seek advice from Human Resources.

12. Will the post-holder accrue at least 4 years continuous service if their current fixed term contract is renewed or extended?

Post-holders who have been employed on a series of fixed term or temporary contracts for a continuous period in excess of 4 years will automatically acquire permanent employment status unless continued employment on a fixed term basis can be 'objectively justified'. In assessing whether 'objective justification' exists, the

reason for the last renewal at the date on which the renewal took effect is the relevant consideration. Reasons for the first engagement on a fixed-term contract and reasons for previous renewals will not be relevant.

Advice from Human Resources should be sought when determining continuous service, particularly where the pattern of employment indicates that breaks in service may have occurred.

13. Does the post-holder have a dual job and what impact does this have on a potential claim for right to permanency?

Where an employee has two contracts, there exists two separate and distinct contractual relationships and so two separate and distinct sets of statutory rights. Therefore, each contract must be considered separately when determining length of service and right to permanency. Accrued service from two contracts cannot be combined to achieve the 4 years' service necessary to invoke a right to permanency.

14. What if a number of fixed term contracts are not being renewed within a service for the same reason?

The non-renewal of a number of fixed term contracts over a specific period may trigger specific obligations on the council in terms of statutory consultation and notification requirements.

This will apply where the council proposes to dismiss 20 or more employees at one establishment within a ninety-day period. For the purposes of determining whether a collective redundancy situation exists, it will be appropriate to take into account fixed term employment contracts that are due to expire during that 90 day period.

Advice from Human Resources must always be sought where it is proposed to end a number of fixed term contracts within a service over a specific period. The total number of terminations across the whole council has to be taken into account for statutory consultation and notification purposes.

15. Conclusion

Fixed term or temporary contracts should only be entered into following full consideration of the requirements for the contract and of the length of time necessary to fulfil the function or complete the task. The contract should be kept under review and extended only where necessary.

Should you have any queries on the application of fixed term or temporary contracts, please contact the HR team.

SECTION 2 - PROCEDURE

Non-renewal/termination of a fixed-term or temporary contract

The following procedural steps should be followed when it is expected that the fixed term or temporary contract will not be renewed or extended.

Step 1

The manager should notify the employee in writing that their fixed-term or temporary contract will not be renewed and as such will result in the termination of employment on the grounds of redundancy or SOSR, and arrange to meet the employee as soon as possible. Advise the employee that he/she may be accompanied at the meeting by their Trade Union Representative or a work colleague.

The manager should hold an initial meeting with the employee in advance of the date the employee's fixed term contract is due to end. Ensure the meeting is arranged sufficiently early in the process to enable a further follow-up meeting to take place before the date on which the employee requires to be served with their statutory notice of termination of employment (a week for each year of continuous service).

Advise the employee that the contract is coming to an end and is unlikely to be renewed. A final decision should not be taken at this stage – that decision should be confirmed only after the process of discussion and consultation with the employee has been concluded. The employee should be given the opportunity to consider their position and be invited to express any views they may have on, for example, alternatives to non-renewal of the contract. Following the meeting, confirm the substance of the discussions in writing and arrange a further meeting again advising of the right to be accompanied.

Step 2

Meet again and consider any representations from the employee. If the outcome does not affect the original proposal not to renew the contract, this should be confirmed to the employee together with the reason for the non-renewal.

Advise the employee of current vacancies elsewhere in the council and provide access to the vacancy list together and offer any assistance with job applications etc.

Step 3

Following the meeting, confirm the decision in writing giving the appropriate contractual or statutory notice of termination and advise of the right of appeal. Confirm the amount (if any) of any redundancy payment that may be due.

Step 4

Complete the appropriate termination paperwork (including redundancy details) and pass for action to human.resources@west-lindsey.gov.uk

Appeal

Any subsequent appeal will be heard by an officer that has not been involved in the original process. The decision of that officer will be final and no further right of appeal will be offered.

Objective Justification

The objective grounds must apply at the start of the fixed-term contract or, if it has been renewed, at the date the last renewal took effect. The position when the first fixed-term contract or previous renewals were put in place will not be the determining factor. Objective grounds are not defined by legislation but must relate to the needs of the service. It must be more than a matter of convenience and as such it should;

- achieve a legitimate objective, for example a genuine business objective;
- be necessary to achieve that objective; and
- be an appropriate way to achieve that objective.

It is essential that when renewing a fixed term contract that would result in an individual accruing 4 years continuous service, that the reason for the further renewal is clearly stated within the written terms of the extension/renewal. It is good practice to include a statement of the reasons for a fixed-term contract at all stages. The table attached at Appendix 1 provides examples of the types of scenarios where objective grounds for retaining fixed-term employment may exist. However if there is no objective justification then the individual's employment status should then be classed as 'permanent.'

It should be noted that an employee does not need to make a formal request for permanent employment status for the change from temporary to permanent to occur. It happens by operation of the law as a result of the criteria being met in the absence of justifiable objective grounds to the contrary. However, employees with four or more years' continuous service under fixed-term contracts have the right to ask the council for a statement that their employment status is now permanent. The council has **21 days** to provide a written statement either confirming permanent employment status or providing objective justification as to why the individual should continue to be employed on a fixed term basis.

EXAMPLES OF OBJECTIVE JUSTIFICATIONS

CRITERIA	JUSTIFICATION FOR RETAINING FIXED TERM STATUS (Strong)	JUSTIFICATION FOR RETAINING FIXED TERM STATUS (Weak)
External Funding	External funding that has restrictions regarding contract status (e.g. European funding)	External funding that is medium to long term with no restrictions on contractual status
	External funding that is short term and has a known end date	External funding that is medium to long term
	External funding from a single source	External funding is from several sources and renewal of funding is likely or the loss of some funding can be sustained
	Self funded posts with unpredictable income	Self funded posts where the post holder has a proven history of income generation
Specific Purpose	Posts that are for a clearly defined purpose or project that is time limited	Posts that were initially devised for a specific purpose but where post holder has become integral

		to the objective of project/event's success
	Requirement for post has diminished	Requirement for post continues and is integral to Service's business plans
Legal Restrictions	The position cannot be made permanent due to work permit or visa restrictions	n/a
Career Development	Post is designed to provide a career development opportunity	n/a
Temporary Cover Arrangement	Post is to cover period of absence (e.g. secondment, maternity, sick leave)	n/a
Contribution to Business	The post-holder's contribution is limited in respect of the service's business objectives	
Specialist Skills	The post requires specialist skills/knowledge for a limited period of time (e.g. to set up or devise a system or service)	The Service requires the continued specialist knowledge/skills to meet its academic/business objectives or maintain the project/service/system etc
Capacity for Redeployment	The post-holder does not have transferable skills	The post-holder has transferable skills
	There is little prospect of a suitable post becoming available	Opportunities exist or are likely to become available within the organisation to enable redeployment to take place

Policy Statement

West Lindsey District Council has a commitment to equal opportunities. It seeks to ensure that no potential or current employee receives less favourable treatment than another on the grounds of age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

تامول عمل انم دي زم قباصع 01427 676676
За повече информация пръстен 01427 676676
Lisainformatsiooni ring 01427 676676
अधकि जानकारी के लए रगि 01427 676676
További információ gyűrű 01427 676676
Lai iegūtu vairāk informācijas gredzenu 01427 676676
Norēdami gauti daugiau informācijas žiedo 01427 676676
Aby uzyskać więcej informacji na ring 01427 676676
Pentru mai multe informații inel 01427 676676
За више информација назовите 01427 676676
رے یٹوگنا 01427 676676 72410 رے تامول عم دی زم

If you would like a copy of this in large, clear print, audio, Braille or in another language, please telephone

01427 676676

Guildhall, Marshall's Yard
Gainsborough, Lincolnshire DN21 2NA
Tel: 01427 676676 Fax: 01427 675170
DX 27214 Gainsborough

www.west-lindsey.gov.uk



This page is intentionally left blank



13 April 2017

**Corporate Policy and
Resources Committee**

Subject: New Bullying and Harassment Policy

Report by:

Director of Resources
Ian Knowles

Contact Officer:

Emma Redwood
People & OD Team Manager
Emma.redwood@west-lindsey.gov.uk

Purpose / Summary:

To propose a new Bullying & Harassment Policy
for staff, to replace the existing policy

RECOMMENDATION(S):

That Corporate Policy and Resources Committee approve the Bullying & Harassment Policy and the policy is adopted for all employees of the council.

Delegated authority be granted to the Director of Resources to make minor housekeeping amendments to the policy in future, in consultation with the chairman of the Corporate Policy & Resources committee and chairman of JSCC.

IMPLICATIONS

Legal: The council is required to have a bullying and harassment working policy to ensure that legislative requirements are met for employees

Financial : There are no changes to the policy which impact the finances of the council, however there are financial risks to the council if it does not have a robust policy on place FIN/135/17

Staffing : None

Equality and Diversity including Human Rights :

West Lindsey District Council has a commitment to equal opportunities. It seeks to ensure that no potential or current employee receives less favourable treatment than another on the grounds of age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

Risk Assessment :

Climate Related Risks and Opportunities :

Title and Location of any Background Papers used in the preparation of this report:

Wherever possible please provide a hyperlink to the background paper/s
If a document is confidential and not for public viewing it should not be listed.

Call in and Urgency:

Is the decision one which Rule 14.7 of the Scrutiny Procedure Rules apply?

i.e. is the report exempt from being called in due to urgency (in consultation with C&I chairman)

Yes

No

Key Decision:

A matter which affects two or more wards, or has significant financial implications

Yes

No

1. Introduction

The council has a Bullying and Harassment Policy in place, however due to updates in legislation, changes to the Acas definition and incorporating best practice a review was required to provide employees with the most up to date information.

2. Purpose

The council recognises the importance of providing staff and managers with accurate information and guidance when navigating through the bullying and harassment legislation and requirements and has therefore fully reviewed the policy and proposes implementing a new updated policy.

3. Scope

This policy applies to all staff including employees, contractors, casual and agency staff and volunteers of the organisation for matters relating to issues of bullying or harassment and directs staff to resolve matters through an informal as well as a formal process.

The policy covers all situations both within the workplace and in any work-related setting outside the workplace, including for example, business trips, conferences and work-related social events.

4. Main Changes

The old policy has been reviewed and rather than making amendments a new policy has been written to ensure a robust policy and procedure is in place for the council, its staff and managers.

5. Engagement

The policy has been developed by the People and OD Team Manager. Independent advice has been sought from an external specialist and Unison has been consulted regarding this policy.

The policy has also been considered at JSCC and was fully supported by Members, Unison and Staff Representatives. Some amendments were made following a request from Unison at JSCC and this has been incorporated into the proposed policy for CP&R.

6. Training and Awareness

This policy will be made available to view on the Minerva site and hard copies available at the depots once formally agreed.

A clear communication will be sent to Managers to make them aware that the policy has been reviewed and to update them on their responsibilities. Training has already been rolled out to managers to raise awareness of their responsibilities with regards to this matter.

An e-learning awareness module will be rolled out to all staff.

7. Recommendation

That Corporate Policy and Resources Committee approve the Bullying & Harassment Policy and the policy is adopted for all employees of the council.

Delegated authority be granted to the Director of Resources to make minor housekeeping amendments to the policy in future, in consultation with the chairman of the Corporate Policy & Resources committee and chairman of JSCC.

Bullying And Harassment Policy

JSCC Approved – 30 Jan 2017

CP&R Approved –

Policy Statement

The council is committed to creating a work environment free of bullying and harassment, where everyone is treated with dignity and respect.

This policy explains:

- The behaviours that you are expected to demonstrate
- What bullying, harassment and victimisation means
- What you need to do if you think you are being bullied, harassed or victimised.

The council is under a legal obligation of a duty of care to provide both a safe place and a safe system of work. If it is considered that bullying or harassment is taking place, the council cannot derogate this duty of care and will be obliged to investigate and take appropriate action (including disciplinary action) against the harasser, if circumstances justify this.

Aim of this Policy

Bullying or harassment at work can have serious consequences for all those involved. It can have serious consequences for individuals. It may make people unhappy, may cause them stress, and affect their health, family and social relationships. It may also affect their work performance and could cause them to take time off from work or leave their jobs.

For the council, it can adversely affect the working environment, reduce productivity, impair performance, increase absence rates and staff turnover, create legal claims and cause damage to the council's reputation.

Through this policy we aim to:

- Ensure the dignity at work of all employees
- Respect and value differences
- Ensure that employees are aware of the types of behaviour which may constitute bullying or harassment
- Identify individual responsibility in preventing such behaviour
- Provide procedures which recognise and take account of the sensitivity of the issues raised
- Provide procedures which enable complaints to be investigated promptly and appropriately, within agreed time scales
- Provide a framework to ensure that bullying or harassment is dealt with effectively, and that action is taken to prevent any recurrence
- Provide a working environment in which employees feel confident to bring forward complaints of bullying or harassment without fear of victimisation
- Provide access to mediation in appropriate circumstances
- Provide access to confidential counselling in appropriate circumstances
- Provide appropriate training and guidance for all individuals involved in the handling of bullying or harassment complaints

Scope

This policy applies to all staff including employees, contractors, casual and agency staff and volunteers of the organisation for matters relating to issues of bullying or harassment and directs staff to resolve matters through an informal as well as a formal process.

The policy covers all situations both within the workplace and in any work-related setting outside the workplace, including for example, business trips, conferences and work-related social events.

Occasionally the council may organise social events to which staff are invited. Staff may also be invited to attend residential training courses or gatherings for staff leaving the council. Although these social events usually take place away from staff's normal workplace and outside normal working hours the council's Bullying & Harassment policy and Code of Conduct may still apply and employees should therefore be mindful of their conduct at such events and outside of work generally.

WLDC works in partnership with other authorities, organisations and also engages interim, consultant and agency staff. Should an issue of harassment/bullying arise, the complaint should be handled in conjunction with the other employer, in normal circumstances the employing organisation of the external person will be responsible for the investigation of the alleged incident(s) and the outcome will be shared with WLDC and the individual concerned.

Definitions used in this policy

The terms bullying and harassment are used interchangeably by most people, and many definitions include bullying as a form of harassment.

The term "complainant" refers to an employee who feels they are being harassed, bullied or victimised.

The term "harasser" refers to the employee who is the alleged perpetrator of the behaviour that could be construed as harassment, bullying or victimisation.

What is harassment?

Harassment at work is unlawful under the Equality Act 2010 and is defined as:

- Unwanted conduct related to a relevant protected characteristic (an area covered by discrimination legislation) which has the purpose or effect of violating an individual's dignity, or creating an intimidating, hostile, degrading, humiliating or offensive working environment for them; or
- Is reasonably considered by that person to have the effect of violating his/her dignity or of creating an intimidating, hostile, degrading, humiliating or offensive environment even if this effect was not intended by the person responsible for the conduct.

The protected characteristics under the Equality Act 2010 are:

Age	Disability
Gender reassignment	Marriage & civil partnership
Pregnancy & maternity	Race
Religion or belief	Sex
Sexual orientation	

The law also offers protection to anyone who suffers discrimination or harassment because they are perceived to possess one or more protected characteristics or because they associate with another person who possesses a protected characteristic (eg carers of a person with a disability).

Harassment is normally characterised by more than one incident of unacceptable behaviour, particularly if it reoccurs, once it has been made clear by the victim that they consider it offensive. One incident may constitute harassment, however, if it is sufficiently serious. Harassment on any grounds will not be tolerated.

Harassment can lead to disciplinary action and, where proven, may attract sanctions up to and including dismissal. In the event of any civil claim being made against the council, the perpetrator of harassment will be joined into any proceedings and may also share liability where a successful claim for damages is made.

The organisation together with any managers or supervisors who fail to take steps to prevent harassment or investigate complaints may be held liable for their unlawful actions and be required to pay damages to the victim, as will the employee who has committed the act of harassment. There is no limit to the compensation that can be awarded in employment tribunals for acts of harassment.

Examples of Harassment

These are examples, not a definitive list of types of behaviour which could be found to constitute harassment. Employees must recognise that what is acceptable to one employee may not be acceptable to another.

- **Verbal** – crude language, open hostility, offensive jokes, suggestive remarks, innuendoes, rude or vulgar comments, malicious gossip and offensive songs.
- **Non verbal** – wolf whistles, obscene gestures, sexually suggestive posters/calendars, pornographic materials (both paper based and generated on a computer, including offensive screen savers), graffiti, offensive letters, offensive emails, text messages on mobile phones and offensive objects. Making gestures that mock a person's equality characteristic.
- **Physical** – unnecessary touching, patting, pinching or brushing against another employee's body, intimidating behaviour, assault and physical coercion.
- **Coercion** – pressure for sexual favours (eg to get a job or be promoted) and pressure to participate in political, religious or trade union groups etc.
- **Isolation** or non co-operation and exclusion from social activities for reasons based on a person's equality characteristic.
- **Intrusion** – following, pestering, spying etc

- **Continued** suggestions for social activity outside the workplace after it has been made clear that such suggestions are unwelcome.

What is Bullying?

There is no legal definition of 'bullying'. It is defined by ACAS as 'Offensive, intimidating, malicious or insulting behaviour, an abuse or misuse of power through means that undermine, humiliate, denigrate or injure the recipient'.

Bullying can be a gradual wearing down process comprising a sustained form of psychological abuse that makes victim's feel demeaned and inadequate.

Bullying can occur in many ways e.g. peer to peer, manager to employee, and employee to manager. Bullying can be carried out by individuals or by groups of people.

Examples of Bullying

Workplace bullying can range from extreme forms such as violence and intimidation to less obvious actions, like deliberately ignoring someone at work. These can be split into two categories:

The obvious:

- Shouting or swearing at people in public and private
- Persistent criticism
- Ignoring or deliberately excluding people
- Persecution through threats and instilling fear
- Spreading malicious rumours
- Constantly undervaluing effort
- Dispensing disciplinary action that is totally unjustified
- Spontaneous rages, often over trivial matters

The less obvious

- Withholding information or supplying incorrect information
- Deliberately sabotaging or impeding work performance
- Constantly changing targets
- Setting individuals up to fail by imposing impossible deadlines
- Levelling unfair criticism about performance the night before an employee goes on holiday
- Removing areas of responsibility and imposing menial tasks
- Blocking applications for holiday, promotion or training.

The actions listed must be viewed in terms of the distress they cause the individual. It is the perceptions of the recipient that determine whether any action or statement can be viewed as bullying.

Recognising bullying and harassment behaviour

Managers should be aware that the types of behaviour outlined in this policy are often hard to recognise and that employees may be too frightened to report an incident. Managers should be alert to some of the possible signs, these may include:

- Sudden and unusual levels of absenteeism
- High staff turnover – especially if it occurs in a particular section or where staff work for a particular manager
- Stress symptoms – such as fatigue, anxiety, depression and panic attacks
- A change in an individual’s behaviour or performance at work

Managers should also be aware that such behaviour may be not just carried out face-to-face, it may be done in more underhand ways, such as by letter, electronically by email, by phone or work related social functions and on social networking sites.

Bullying can be carried out by groups, and there can be a bullying culture that is gradual and harmful. This can be difficult for those inside it to recognise, or to break out of.

Managers should be supportive of those who raise an issue and ensure they are no less favourably treated as a consequence. On the other hand, managers should deal with allegations sensitively when discussing the matter with the alleged “harasser” as it may be the case that the allegation may have no foundation.

What is Victimisation?

Victimisation is subjecting a person to a detriment because they have, in good faith, complained (whether formally or otherwise) that someone has been bullying or harassing them or someone else, or supported someone to make a complaint or given evidence in relation to a complaint. This would include isolating or threatening someone because they made a complaint, or giving them a heavier or more difficult workload.

Provided that an employee has acted in good faith, i.e. they genuinely believe that what they are saying is true, they have a right not to be victimised for making a complaint of bullying or harassment and the council will take appropriate action to deal with any alleged victimisation, which may include disciplinary action against anyone found to have victimised a person.

The council has a confidential reporting line for whistleblowing. An employee is also protected from victimisation or detriment if they have raised a protected disclosure under the council’s Whistleblowing Policy – available on Minerva and the council’s website.

Electronic Bullying

This is a term used to refer to bullying and harassment through electronic media, usually through instant messaging, emails, social media, or text messages. In sending emails or electronic messages employees should consider the content, language and appropriateness of such communications.

- Avoid using language which would be deemed to be offensive to others in a face-to-face setting as the impact on individuals will be much the same
- Avoid the use of provocative or inappropriate images
- Avoid forming or joining an online group that isolates or victimises fellow colleagues
- Ensure that you never use such sites to access or share illegal content

If online bullying or harassment is reported it will be dealt with in the same way as if it had taken place in a face-to-face setting.

What is the impact of bullying or harassment?

The impact of bullying or harassment includes the following:

- bullying or harassment may make someone feel anxious and humiliated
- people may feel angry and frustrated because they cannot cope
- some people may try to retaliate in some way
- others may become frightened and demotivated
- stress, loss of self-confidence and self-esteem caused by bullying or harassment can lead to job insecurity, illness, absence from work, and even resignation.
- Almost always job performance is affected and relations in the workplace suffer

Role and Responsibilities:

Failure to deal with bullying and/or harassment allegations may expose both the council and employees to a number of legal consequences. Complainants can cite both the employer and individual employees as respondents at Employment Tribunal and, if the case is upheld, both may be held liable.

Role and Responsibility of Employer

The council will:

- Accept its legal and moral responsibility to deal effectively with bullying and harassment in the workplace using this policy in conjunction with, and if appropriate, the disciplinary procedure.
- Ensure that all employees are aware of the Bullying and Harassment Policy through the induction process.
- Provide guidance and training to all employees responsible for dealing with complaints under the Bullying and Harassment Policy.
- Provide general awareness training for all employees.

Responsibility and Role of Manager

The manager is responsible for ensuring the awareness and compliance with this policy by the staff they manage.

Managers and supervisors have a specific duty to set and demonstrate standards of acceptable behaviour and to be vigilant in observing the behaviour of others. They are also responsible for taking steps to prevent inappropriate behaviour once it has been identified. Action must be taken once a manager becomes aware, even if no formal or informal complaint has been made. Inappropriate or unacceptable behaviour can be raised using performance management techniques (ie induction, probationary period, supervision, appraisal and training) as well as in 1 to 1 discussions immediately following any observed inappropriate behaviour. Where a complaint is made, managers should ensure that the procedural guidelines are followed.

Managers should –

- Be aware of the policy and what to do when a situation is brought to their attention
- Attend training organised by the council
- Treat complaints of bullying and/or harassment seriously, sensitively and confidentially.
- Ensure that the work environment is non-threatening and supportive and take steps to prevent bullying and/or harassment
- Explain and model the council's expected standards of behaviour
- Lead by example and be prepared to challenge all forms of unacceptable behaviour
- Escalate the issue if appropriate
- Consult with HR if they have any concerns, and avoid not dealing with or raising concerns

Responsibility and Role of Employee

All employees have a personal responsibility not to harass or bully other members of staff, or to condone harassment or bullying by others.

They are required to:

- Treat all colleagues with dignity and respect and be aware of how their behaviour can be perceived to affect other people.
- Be supportive of colleagues who are being bullied or harassed and bring it to the attention of their line manager, or other appropriate manager.
- Respond promptly to any feedback and advice on their behaviour, be it from a colleague or a manager.
- Seek to resolve matters informally wherever possible.
- Ensure that they understand the policy and the consequences of vexatious complaints and abuse of this policy.
- Support the council in its efforts to eradicate any such behaviour that may threaten the council's commitment to ensuring the dignity at work of all its employees.

Responsibility and Role of HR

- The HR team can offer guidance, advice and support to employees and all levels of management.
- HR will offer guidance with regard to the interpretation of this policy and best practice recommendations in dealing with incidents of bullying or harassment, including the appropriate information to record.

Responsibility and Role of Trade Union

The trade union recognised by this council will:

- Support the council in its efforts to provide a working environment free from bullying and harassment
- Help inform the workforce of this policy and encourage employees who may have a problem to use the procedures available to them
- Advise members of their rights and responsibilities under this policy and to represent members as and when appropriate

- Advise members accordingly in cases where they appear to be making malicious claims.

Responsibility and Role of Councillors

Councillors are bound by the Code of Conduct which clearly sets out standards of behaviour towards other Councillors and Officers.

If there are instances of bullying or harassment by Councillors towards Officers or other Councillors, those Councillors who are aware of the incident are encouraged to report it to the Monitoring Officer.

It is also advised that Officers, who are either the subject of bullying or harassment by Councillors, or who witness such an incident, should also report this to the HR team or the Monitoring Officer.

Formal complaints made against a Councillor will be managed in accordance with the "Arrangements for dealing with standards allegations, (against a District Councillor) under the Localism Act 2001" Procedure, available on the council's website.

Fair and Effective Management

Managers have the right to manage staff effectively, giving reasonable instructions when required and this does not constitute bullying or harassment. This includes dealing appropriately with shortcomings in performance, conduct, attendance and behaviour when fair to do so.

It is therefore important to differentiate between management and bullying and / or harassing behaviour. Within the council there is an expectation that managers fulfil their duties and responsibilities and therefore it is reasonable to expect a manager to carry out their function in a fair, firm and consistent manner.

Managers are responsible for ensuring that staff who report to them perform to an acceptable standard within a performance management framework. Legitimate, justifiable, appropriately conducted monitoring of an employee's behaviour or job performance does not therefore constitute bullying or harassment.

It is recognised that some staff may feel stressed or anxious while performance management procedures are ongoing. It is in the interests of the council that managers should be able to carry out their duties without threat of ill intended, malicious or vexatious complaints. An investigation will determine whether a manager has bullied or harassed an employee or managed them fairly, but firmly.

Initiating Investigation Without a Complaint

Issues of bullying or harassment may be identified via various sources of information other than direct complaints e.g. exit interviews (particularly in areas of high staff turnover), employee surveys or feedback. In these cases a bullying and harassment investigation may be instigated to ensure that information on possible bullying and harassment is followed up. Issues highlighted by HR will be raised with the relevant manager.

Vexatious or Malicious Complaints

Where a complaint is found to be blatantly untrue and has been brought out of spite, or for some other unacceptable motive, the complainant will be subject to the council's disciplinary procedure, as will any witnesses who are found to have deliberately misled the investigating officer or manager.

Responding to Counter Allegations

When a complaint of bullying or harassment is made, sometimes a counter complaint is also made. In these circumstances, both complaints will be investigated simultaneously by the same investigating officer, if practicable. Advice should be sought from HR in respect of how best to deal with these situations.

What happens if I am accused of harassment or bullying?

If an employee approaches you informally about your behaviour, do not dismiss the complaint out of hand because you were "only joking" or you think that he or she is being too sensitive. Remember that different people find different things acceptable and everyone has the right to decide what behaviour is acceptable to him or her, and to have his or her feelings respected by others.

You may have offended someone without intending to. If this is the case, the person concerned may be content with an explanation and an apology from you, and an assurance that you will be careful in the future not to behave in a way that you now know may cause offence. Provided that you do not repeat the behaviour which caused the offence, that may well be the end of the matter.

If you are approached about informal allegations in relation to your conduct or behaviour and mediation is proposed as an option you should carefully consider this as a helpful way forward to resolve the concerns raised. Mediation will only be viable where both parties agree to mediation.

If a formal complaint is made about your behaviour, this will be investigated and the council may bring disciplinary proceedings against you if appropriate. Complaints of bullying and / or harassment may well fall under gross misconduct, which if proved could lead to dismissal.

Procedure – where bullying or harassment behaviour is experienced

Whilst the council is firmly opposed to any behaviour that may constitute bullying or harassment, it also recognises that the employee subjected to the behaviour has a vital role to play in the prevention of this behaviour.

Bullying and harassment tends to happen over a course of time and many employees do not come forward until very late and any damage has been made worse because of the length of time. The council strongly recommends and would encourage employees not to tolerate the behaviour or be afraid to report the behaviour thus allowing it to build up.

Whenever an employee witnesses or is subject to behaviour they find unacceptable they should:

- In the first instance, if they feel able to do so, try to approach the employee concerned and explain that they find the behaviour unwelcome, explaining that it offends them or makes them feel uncomfortable, or that it interferes with their work and they wish it to stop. Often, the behaviour may have been commonly acceptable and all that is needed is the explanation that this is no longer the case.
- If this is not possible, in addition to reporting the behaviour to the manager, they could confide in another colleague so that someone else is aware of the problem and can offer support or advice in tackling the problem.
- Discreetly record all relevant incidents including dates, times and any witnesses present and the way in which the behaviour has affected the employee personally and whether it has had any impact on the work.
- Consider contacting the Employee Assistance Programme, details are available on Minerva or contact details are on posters around the council.

Confidentiality

All parties involved in an investigation are under an obligation to maintain confidentiality throughout the process. Any inappropriate sharing of information relating to the investigation could result in disciplinary action being taken.

Right to be accompanied

At all formal stages of this procedure (with the exception of agreed mediation) the employee will be given the opportunity to be accompanied by either a work colleague or their trade union representative/official employed by a trade union.

There is no right to be accompanied or represented by a solicitor or legal representative or other representative at any stage of the procedure.

It would not be reasonable for staff to insist on being accompanied by a companion whose presence would prejudice the proceedings and the council reserves the right to refuse for such a companion to accompany an employee.

Informal Stage

It is preferable for all parties concerned to try to resolve matters informally as this is likely to produce solutions which are speedy, effective and restore positive relations in the workforce.

The complainant should raise any concerns or issues informally with:

- Their manager
- The managers manager, if the immediate manager is the cause of the complaint, or:
- A member of the Human Resources team

At this stage the appropriate manager and / or member of HR will meet with the complainant to discuss the issue on a one to one basis. Appropriate action to start dealing with the complaint, such as arranging a meeting etc. should be taken within 7 working days unless the situation is so serious to warrant immediate formal action. The complainant should explain what their concerns are along with the reasons.

The manager and / or member of HR should objectively consider the merits of the complaint taking into account:

- The allegation made
- Whether they should speak to the alleged harasser to obtain their version of events
- Whether the perception of the complainant is reasonable in the circumstances i.e. could what has taken place be reasonably considered to have caused offence
- Whether the reaction of the complainant to the issue is reasonable
- Whether there may be any motives behind the allegations
- Whether there is a communication issue which may be resolved informally or by mediation

If the manager and / or member of HR consider there to be no merit in the concern the complainant should be advised of the reason(s) why.

If the manager and / or member of HR feel that the concern may be legitimate, they should discuss together the options available to resolve it. Minor issues should be resolved through normal line management.

If possible an informal discussion should then take place with both the complainant and the alleged harasser. A direct approach to the alleged harasser will make them aware that their behaviour is inappropriate and provides them the opportunity to modify it. It is a fact that some people may be unaware that their behaviour is being perceived in the way it is and bringing it to their attention is all that is needed. For example, an employee may be naturally brusque or businesslike and not appreciate that this may be taken out of context by the recipient.

Likewise, there are always two sides to an allegation and it is important to understand the alleged harasser's intentions and reasons for their behaviour when trying to understand the impact of the behaviour on the complainant and in choosing the most effective resolution to the situation.

It may also be suitable to deal with the issues by raising them at mediation meetings where appropriate and where the employees agree that this would help resolve the issues.

Depending on the behaviour complained about, ordinarily it is only when the behaviour continues after the effect on the complainant has been made clear, that the complaint can be progressed. However, an isolated incident may be sufficiently serious to mean the matter will be progressed to the formal stage immediately.

Whilst this stage is informal, notes of the discussion and action taken should be taken. HR should be informed and they will send a letter to the employee(s) confirming the discussion and necessary actions.

Should this approach fail to remedy the situation or to stop the behaviour complained of, or if an employee agrees with their manager that the situation is so serious as to warrant formal action, the formal approach should be taken.

Mediation

Mediation is a voluntary, confidential process where an independent and trained mediator helps two or more people in dispute to attempt to reach an agreement. Any agreement comes from those in dispute, not from the mediator.

Mediation is independent from any actual disputes. Therefore, participating in the mediation process will not have any impact on any additional processes should they be required.

Employees may be offered mediation and employees would ordinarily be expected to participate at any stage if it is reasonable, necessary and an effective option in the circumstances.

Mediation will be suitable for many inter personal disputes where employees would benefit from understanding their respective viewpoints. It is not intended to make employees friends, but rather to make sure that the working environment is effective.

The mediator will produce a written agreement, which will be signed by both parties and a signed copy will be shared with the Manager and a copy will also be sent to HR for record.

Any discussions taking place during mediation and the subsequent written agreement will remain confidential and “without prejudice” and may not be used by either party in any subsequent internal or external process, unless it is with the explicit consent of both parties.

If the parties cannot reach agreement through mediation then the matter will be referred back to the formal process.

Where a complaint is made whilst the employee is subject to disciplinary proceedings

Any harassment or bullying complaint which is raised during a disciplinary process and which is related to the disciplinary proceedings or the circumstances relating to the alleged misconduct will be dealt with as part of the disciplinary investigation process.

Where the harassment or bullying complaint does not relate to the disciplinary proceedings, the Investigating Officer and a member of HR will consider whether the complaint may have implications on the investigation or its outcome. Consideration may be given to whether the disciplinary investigation should be placed on hold. It will not automatically follow that the investigation will be placed on hold merely because a complaint has been made.

In the event that it is deemed appropriate to place the disciplinary investigation on hold, the complaint will be investigated under the Bullying and Harassment policy and the disciplinary investigation will reconvene upon its conclusion.

Suspension

Suspension is not a disciplinary sanction and employees should not be suspended as a matter of course. There should always be due consideration of the necessity to suspend

and this should be reviewed during the process to ensure that there is a continued need for suspension. It should be considered as a last resort and handled with tact and sensitivity.

Circumstances in which suspension may be appropriate include:

- Where the employee or other individuals are perceived to be at risk
- Gross misconduct is suspected to have occurred
- Where suspension is necessary to allow the conduct of the investigation to proceed unimpeded
- Where there is a risk of the misconduct reoccurring if the employee remained in the workplace
- This list is not exhaustive

The decision to suspend will be taken by the manager or nominated officer in consultation with a member of the HR team. The decision to suspend will always be confirmed in writing by HR and will outline the protocols, expectations and requirements of the employee during the period of suspension.

There is no appeal against the decision to suspend.

An employee who is suspended should not discuss the case with witnesses or work colleagues without permission to do so. The employee will be afforded all reasonable access to materials pertinent to the investigation where appropriate.

Contravention of this instruction without reasonable excuse will, in itself, be a potential disciplinary matter. Any request for copies of information, documentation, files etc. should be submitted to a member of the HR team.

Formal Stage

If the complainant wishes to make a formal complaint, either straightaway or because the informal procedure has failed to resolve the problem, the formal procedure should be followed.

A formal complaint should be made in writing, making it clear that it is a formal complaint under this procedure and detailing the basis upon which the alleged bullying or harassment has taken place, this should be sent to the HR team.

When a complaint is received HR will undertake a case review of the complaint and may suggest an informal resolution.

The formal stage is not appropriate to deal with cases of day to day normal management issues.

An Investigating Officer will be appointed (not from within the service) and they will be able to request advice and assistance from a member of HR where necessary during the course of the investigation. The council may, at its discretion, use an external investigator where this is deemed appropriate.

Strict confidentiality should be maintained throughout any investigation into an allegation. The importance of confidentiality must be emphasised to all parties interviewed under the investigation.

During the course of the investigation the Investigating Officer will interview the complainant, the alleged harasser and any witnesses involved. When the need to interview any employee involved arises, that employee may be accompanied by their Trade Union representative or by another employee. However, unavailability of the Trade Union Representative will not stop the interview going ahead. All parties will be advised of the nature of the complaint and will be given the opportunity to state their case.

During these meetings employees must include all facts and evidence pertinent to the complaint that they would wish to be considered. Once the investigation is complete, no other supplementary information will be allowed to be submitted by either party unless the supplementary information could not have been reasonably identified or located during the investigation.

Witnesses should be advised that their statement may be used as evidence at a later stage should the case progress to discipline procedures and that they may also be required to attend a disciplinary hearing.

Completion of investigation

When the investigation is complete, a report will be prepared by the Investigating Officer containing all the investigation information including statements and all background documents. The Investigating Officer will then make a recommendation based on the evidence of the case.

Only if the investigation is followed by disciplinary proceedings would the full report containing the original complaint and witness statements be shared with the complainant and the employee against whom the complaint is made.

May be a case to answer

If the Investigating Officer recommends that there may be a case to answer the report will be passed to the HR team so that a formal disciplinary hearing can be arranged. The disciplinary policy, from the hearing stage, should then be followed from that stage forward.

The harasser will be written to with:

- Details that a hearing will take place
- The identity of the officer hearing the case
- Full details of the complaint/allegation with any evidence attached
- Details of the potential sanction that may be issued, and
- The right to be accompanied by their trade union representative or work colleague

The harasser will be able to appeal against the decision made at the hearing, this would be confirmed in writing.

No case to answer

If the Investigating Officer decides that there is no case to answer, the complainant will be invited to a meeting with the Investigating Officer to disclose the outcome. The complainant may be accompanied by their trade union representative or a work colleague. The complainant will be provided with reasons for the decision which will be followed up in writing.

The purpose of this meeting is for the Investigating Officer to provide the complainant with reasons why it has been decided that there is no case to answer.

If the complainant disagrees with the Investigating Officer's decision, the employee will be able to appeal, this would be confirmed in writing.

Complaint Monitoring

Following the completion of the case/investigation managers should continue to monitor the situation and talk to the individuals involved informally to find out whether the conflict has been resolved or if there are renewed tensions or unhappiness. This could be carried out through one to one meetings and performance appraisals.

Policy Statement

West Lindsey District Council has a commitment to equal opportunities.

It seeks to ensure that no potential or current employee receives less favourable treatment than another on the grounds of age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

تامول عمل ا نم دي زم قباصع 676676 72410
За повече информация пръстен 01427 676676
Lisainformatsiooni ring 01427 676676
अधिकि जानकारी के लएि रगि 01427 676676
További információ gyűrű 01427 676676
Lai iegūtu vairāk informācijas gredzenu 01427 676676
Norēdami gauti daugiau informācijas žiedo 01427 676676
Aby uzyskać więcej informacji na ring 01427 676676
Pentru mai multe informații inel 01427 676676
За више информација назовите 01427 676676
رے یٹوگنا 676676 72410 رے تامول عم دی زم

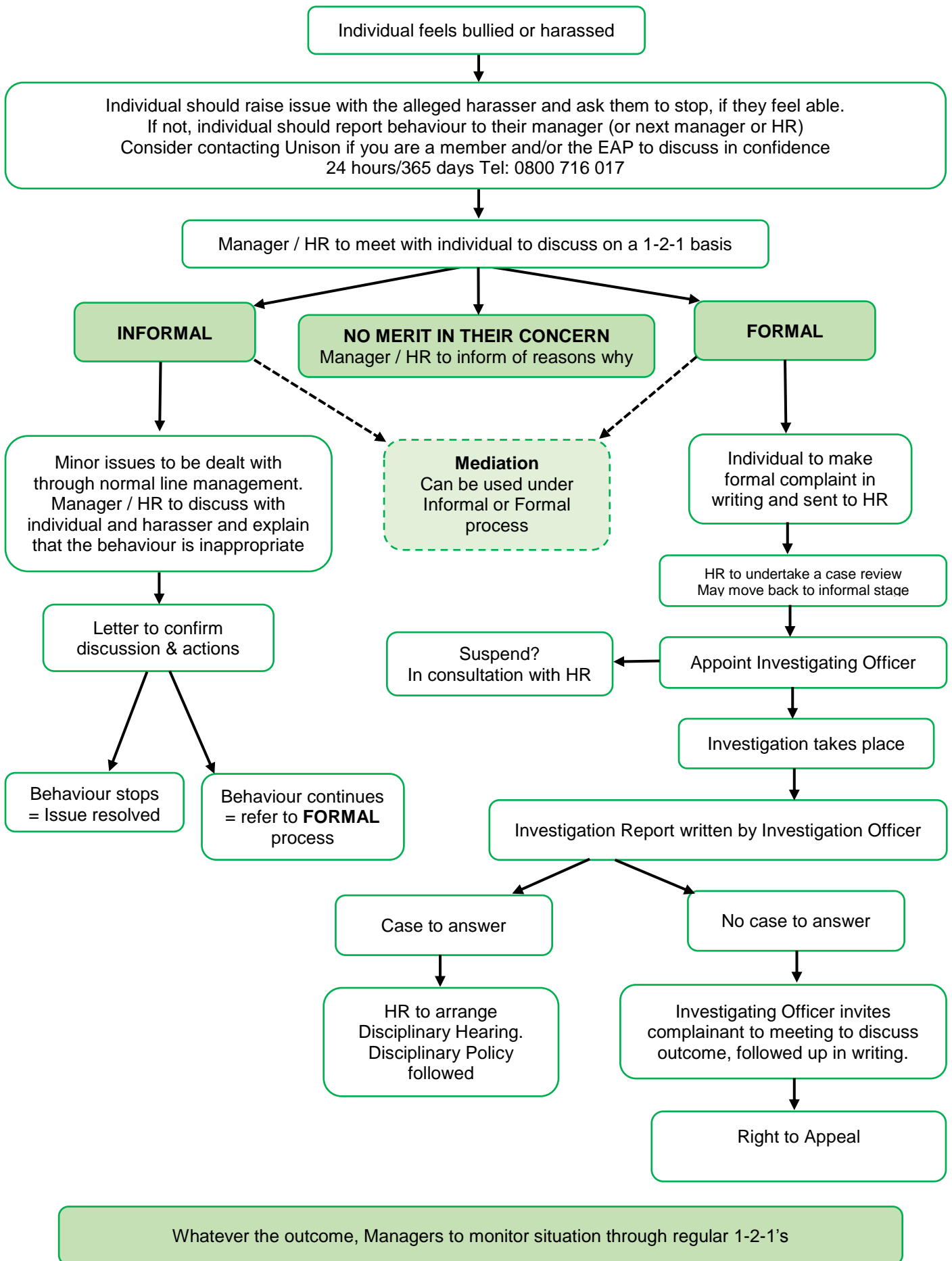
If you would like a copy of this in large, clear print, audio, Braille or in another language, please telephone
01427 676676

Guildhall, Marshall's Yard
Gainsborough, Lincolnshire DN21 2NA
Tel: 01427 676676 Fax: 01427 675170
DX 27214 Gainsborough

www.west-lindsey.gov.uk



Bullying & Harassment Procedure Flowchart





**Corporate Policy and
Resources Committee**

13 April 2017

Subject: Information Governance Policy Review (Part 2)

Report by:

Director of Resources

Contact Officer:

Steve Anderson
Information Governance
01427 676652
Steve.anderson@west-lindsey.gov.uk

Purpose / Summary:

To report on progress of the review of information governance policy documents being carried out by the Corporate Information Governance Group and to request approval from the CP&R Committee for reviewed policies to be implemented for all staff, elected members, and partners where appropriate.

RECOMMENDATION(S):

That Members approve the attached information policies for implementation to all staff, elected members, and partners where appropriate.

That delegated authority be granted to the Director of Resources to make minor housekeeping amendments to the policy in future, in consultation with the chairs of the Corporate Policy & Resources Committee and Joint Staff Consultative Committee.

IMPLICATIONS

Legal: We are required by legislation such as the Data Protection Act 1998 to implement and maintain policies on the management and protection of information.

Financial : None – [FIN/2/18](#)

Staffing : None

Equality and Diversity including Human Rights :

These new policies have no impact, adverse or otherwise, on any particular group.

Risk Assessment : None

Climate Related Risks and Opportunities : None

Title and Location of any Background Papers used in the preparation of this report:

N/A

Call in and Urgency:

Is the decision one which Rule 14.7 of the Scrutiny Procedure Rules apply?

i.e. is the report exempt from being called in due to urgency (in consultation with C&I chairman)

Yes

No

X

Key Decision:

A matter which affects two or more wards, or has significant financial implications

Yes

No

X

1. Background

In order to safeguard the Council's vital information assets and comply with the extensive legal framework around information and privacy, the Council is required to put in place an Information Security Management System (ISMS) based on recognised industry standards such as ISO/IEC 27001 (Information Security Management Systems) at the heart of its information governance activities. The Local Public Services – Data Handling Guidelines (4th Edition) recommends that local authorities structure these activities around 5 headings:

- Policy
- People
- Places
- Processes
- Procedures

Accountability for the Council's Information Assurance and ISMS rests with the Director of Resources through his role as the Senior Information Risk Owner (SIRO). He delegates responsibility for information governance to the Corporate Information Governance Group (CIGG) which he chairs. The CIGG is comprised of the information specialists from across the Council who meet approximately 6-weekly to share good practice, monitor compliance, and maintain elements of the Council's ISMS.

Comprehensive and up-to-date policies are essential to influence decisions on which security controls we need, inform the development our processes and procedures, and define training and awareness objectives for our staff, councillors and partners. Policies are usually the first thing asked by auditors when they are assessing particular aspects of our information governance arrangements.

This is the second report covering the review of the Council's information policies currently being undertaken by the CIGG and scheduled for completion by end May 2017.

The attached Policies have been reviewed and agreed by the Governance Corporate Leadership Team (GCLT) and were supported by members, unions and staff representatives at Joint Staff Consultative Committee (JSCC) meetings held on 2 Feb 2017 and 30 Mar 2017.

2. The Policy Review

The Council's information policy set is broken down as follows:

Information Management Policies

Title	Document Owner	Review Date
Data Protection Breach Policy	Emma Redwood	16/01/2015
Data Protection Policy	Emma Redwood	27/08/2015
Data Quality Policy	James O'Shaughnessy	19/02/2016
Freedom of Information and Environmental Information Policy	Emma Redwood	27/08/2015
Information Governance Policy	Steve Anderson	27/10/2018
Information Management and Protection Policy	Steve Anderson	23/06/2015
Information Sharing Policy	Steve Anderson	27/10/2018
Legal Responsibilities Policy	Steve Anderson	27/10/2018
Records Management Policy	Steve Anderson	16/01/2015

Note: Shaded policies are not due to be reviewed.

Information Security Policies

Title	Document Owner	Review Date
Information Security Policy	Cliff Dean	23/06/2015
IT Access Policy	Cliff Dean	15/08/2014
IT Infrastructure Security Policy	Cliff Dean	15/08/2014
Remote Working Policy	Cliff Dean	23/06/2015
Removable Media Policy	Cliff Dean	16/01/2015
Internet Acceptable Usage Policy	Cliff Dean	23/06/2015
Bring Your Own Device Policy	Cliff Dean	30/11/2016
Computer Telephone and Desk Use Policy	Cliff Dean	15/08/2014
Email Policy	Cliff Dean	30/11/2016
Email Policy for ActiveSync Users	Cliff Dean	30/11/2016
Information Security Incident Management Policy	Steve Anderson	01/12/2016
Mobile Device Policy	Cliff Dean	16/04/2016
PSN AUP and Personal Commitment Statement	Cliff Dean	29/08/2014

This report covers the 12 documents detailed below:

- a. Data Protection Breach Policy (Appendix 1)
- b. Freedom of Information and Environmental Information Policy (Appendix 2)
- c. Records Management Policy (Appendix 3)
- d. IT Infrastructure Security Policy (Appendix 4)
- e. Removable Media Policy (Appendix 5)
- f. Computer, Telephone, and Desk-Use Policy (Appendix 6)
- g. Email Policy (Appendix 7)
- h. Email Policy for ActiveSync Users (Appendix 8)
- i. Information Security Incident Management Policy (Appendix 9)
- j. Internet Acceptable Use Policy (Appendix 10)
- k. Mobile Device Policy (Appendix 11)
- l. Public Service Network Acceptable Use Policy (Appendix 12)

The report does not include the *Bring Your Own Device Policy* which was reviewed and left unchanged. A reassessment of the IT technical infrastructure which supports user-owned devices is being carried out and is likely to require a major update of this Policy.

3. Decisions Required

That Members approve the attached information policies for implementation to all staff, elected members, and partners where appropriate.

Delegated authority be granted to the Director of Resources to make minor housekeeping amendments to the policy in future, in consultation with the chairs of the Corporate Policy & Resources Committee and JSCC.

Appendix 1 – Data Protection Breach Policy Revisions

Policy Title: **Data Protection Breach Policy** New Version: 3.0

Revisions:

a.	ADDITION	Para 6.1	Reference to new Appendix 1 added. Details breach reporting detail in a process flow diagram
b.	ADDITION	Para 6.2	Details reporting for data incidents that do not involve personal information.
c.	AMENDMENT	Para 6.3	“Strategic Lead” replaced with “ICT Help-desk” “Out of Hours Emergency Officer” replaced with “ICT Duty Officer (ICT Manager)”
d.	AMENDMENT	Para 6.4	“Strategic Lead” replaced with “ICT Help-desk”
e.	ADDITION	Para 6.4	Inserted “Data Protection Officer”.
f.	AMENDMENT	Para 6.6	“Strategic Lead” replaced with “ICT Help-desk”
g.	AMENDMENT	Para 6.7	“Strategic Lead” replaced with “ICT Help-desk” (2 occurrences).
h.	AMENDMENT	Para 7.1	“Strategic Lead” replaced with “Team Manager” (2 occurrences).
i.	AMENDMENT	Para 8.2	“Strategic Lead” replaced with “Team Manager”.
j.	ADDITION	Para 8.2	“Data Protection Officer” added.
k.	AMENDMENT	Para 9.1	“Strategic Lead” replaced with “Team Manager”.
l.	AMENDMENT	Para 11.1	“Member and Support Services” replaced with People and Organisational Development”.
m.	AMENDMENT	Para 12	Useful Contacts updated.
n.	ADDITION	Appendix 1	New Appendix 1
o.	AMENDMENT	Appendix 2	Appendix 1 renumbered to Appendix 2

Appendix 2 – Freedom of Information and Environmental Information Policy Revisions

Policy Title: **Freedom of Information and Environmental Information Regulations Policy**

New Version: 4.0

Revisions:

a.	ADDITION	Para 3 Bullet 3	Added “Strategic Leads” to list of responsible managers.
b.	AMENDMENT	Para 3 Bullet 4	“Team Manager, Member and Support Services” replaced by “Team Manager, People and Organisational Development”.
c.	AMENDMENT	Para 3 Bullet 5	“Team Manager, Member and Support Services” replaced by “Team Manager, Customer Strategy and Services”.
d.	AMENDMENT	Para 3 Bullet 6	“Team Manager, Member and Support Services” replaced by “Team Manager, People and Organisational Development”.
e.	ADDITION	Para 3 Bullet 6	Added “... and will lead on any situations where decisions are reviewed or exemptions/exceptions are being considered.” to end of sentence.
f.	ADDITION	Para 3 Bullet 7	Added “... during their induction.” to end of sentence.
g.	AMENDMENT	Para 3 Bullet 4	“Team Manager, Member and Support Services” replaced by “Team Manager, People and Organisational Development or the Team Manager, Customer Strategy and Services”.
h.	ADDITION	Para 8	Added new para 8 which sets out a new policy for charging for Environmental Information Requests.

Appendix 3 – Records Management Policy Revisions

Policy Title: **Records Management Policy** New Version: 2.0

Revisions:

a.	AMENDMENT	Para 4	Amended to reflect latest governance structure
b.	ADDITION	Para 4	New sub-para: “Datasets stored in corporate systems must be assigned an Information Asset Owner (IAO). IAOs are responsible for all aspects of the protection, use, and retention of the data. They must authorise any request to use data for alternative purposes in line with all relevant legislation.”
c.	AMENDMENT	Para 7	Sub-para 1 amended to read: “It is essential regular housekeeping is carried out to make sure stored records are saved for the appropriate length of time in line with retention and disposal schedules. Records which form part of the corporate memory must be saved into the relevant system or shared work areas. An email mailbox is not a suitable place to store corporate records.”
d.	ADDITION	Para 8	New sub-para 4: “Where systems have the functionality to enforce retention and disposal policies they must be properly configured to do so.”

Appendix 4 – IT Infrastructure Security Policy Revisions

Policy Title: **IT Infrastructure Security Policy** New Version: 2.0

Revisions:

a.	AMENDMENT	Ex Para 10 (new para 2)	Key messages moved from Para 10 to Para 2.
b.	AMENDMENT	New Para 2	Updated to reflect latest governance structure.
c.	ADDITION	Para 6	3 new risks added: <ul style="list-style-type: none"> • Inadequate physical security controls lead to a loss of personal or sensitive information resulting in a monetary penalty and/or reputational damage. • Inadequate or inappropriate physical and technical security controls provided for IT equipment used or transported outside the Council’s physical security boundary lead to a loss of personal or sensitive information resulting in a monetary penalty and/or reputational damage. • Failure to adequately destroy data when re-using or disposing of redundant, obsolete, or defective equipment leads to a loss or disclosure of personal or sensitive information resulting in a monetary penalty and/or reputational damage.
d.	ADDITION	Para 7.1	New sentence added: “All security breaches or observed weaknesses must be reported in accordance with the Council’s Information Security Incident Management Policy.”
e.	ADDITION	Para 7.3	Reference to Mobile Device Policy added.
f.	ADDITION	Para 7.6	New sub-para 2: “Where a device is accessed using a two-factor authentication method such as BitLocker then access tokens must be stored separately from the device. They must never be kept in the same storage bag or container as the device. Furthermore, after a token or key has been used to gain access to a device then it should be removed from the device and secured.
g.	AMENDMENT	Para 10	List of references completely updated.

Appendix 5 – Removable Media Policy Revisions

Policy Title:

Removable Media Policy

New Version: 2.0

Revisions:

a.	ADDITION	Para 2 New bullet 2	“An inventory of all removable media devices supplied by the Council is to be maintained by the ICT Department.”
b.	ADDITION	Para 2 Bullet 4	2 additional sentences added: “Any exceptions to this, such as an external training provider delivering a presentation using their own media, must be first approved by the ICT Department and devices must be scanned for viruses and malware. Access to approved externally-provided devices must be set to read-only .”
c.	AMENDMENT	Para 2 Bullet 8	Amended to read “Removable media devices that are no longer required, or have become damaged, must be returned to the ICT Department and disposed of securely to avoid data leakage.”
d.	AMENDMENT	Para 7	Para amended to remove ambiguity: “It is the Council’s policy to discourage the use of removable media as far as reasonably practicable. Where there is no practicable alternative, such as working remotely with no secure network connection, then removable media may be used but only when a properly risk-assessed business case is provided and agreed by the relevant team manager. There are significant risks associated with the use of removable media and, therefore, clear business benefits that outweigh the risks must be demonstrated before approval will be given.”
e.	ADDITION	Para 7.1	New sentences added: “Exceptions to this, such as an external training provider delivering a presentation using their own media, must be first approved by the ICT Department and devices must be scanned for viruses and malware. Access to approved externally-provided devices must be set to read-only.” An inventory of all removable media devices supplied by the Council network is to be maintained by the ICT Department and each device must be logged out and back in.”
f.	AMENDMENT	Para 7.3	Para amended to read: “It is the duty of all users to immediately report any actual or suspected breaches in information security in accordance with the Council’s Information Security Incident Management Policy by

			<p>completing a Report an Information Governance Incident on the Council's Intranet.</p> <p>It is the duty of all councillors to report any actual or suspected breaches in information security to the Monitoring Officer or the Director of Resources."</p>
g.	AMENDMENT	Para 7.4	"Assistant Chief Executive" replaced by "Director of Resources".
h.	ADDITION	Para 7.5	Added to end of sentence: "... and return them to the ICT Department."
i.	AMENDMENT	Para 7.6	Final 2 Sentences moved to beginning of para:
j.	AMENDMENT	Para 7.7 Bullet 8	Para amended to read: "Information held on a removable media device must be kept to a minimum, and no more case files / sets of information than required for the approved purpose are to be held on a device at any time."
k.	DELETION	Para 7.7	Deleted from final sub-para: "or a Corporate Information Governance Group representative."
l.	ADDITION	Para 8	Inserted into para: "the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000"
m.	AMENDMENT	Para 8	Job titles updated.
o.	DELETION	Para 10	Deleted in Toto
p.	ADDITION	New para 10	Reference documents updated.

Appendix 6 – Computer, Telephone, and Desk-Use Policy Revisions

Policy Title: **Computer, Telephone, and Desk-Use Policy**

New Version: 3.0

Revisions:

a.	AMENDMENT	Para 2	Key Messages moved to beginning of document. Paras renumbered accordingly.
b.	AMENDMENT	General	Security classifications amended to reflect new Government security classifications
c.	ADDITION	Para 6	10 new risks associated with use of computers, telephones and desks added which this policy aims to mitigate.
d.	AMENDMENT	Para 7.3	Practicalities of operating within a clear desk policy clarified

Appendix 7 – Email Policy Revisions

Policy Title: **Email Policy**

New Version: 4.0

Revisions:

a.	AMENDMENT	Para 1	Following text added to Policy Statement: “using a variety of training methods during on-boarding, the induction process, and throughout their employment or term of office”.
b.	AMENDMENT	General	Job titles updated to reflect current organisational structure.
c.	ADDITION	Para 6.2 (sub-para 4)	New sentence: “An email could also be construed as a contract or legally-binding agreement.”.
d.	AMENDMENT	Para 6.4	“Users are provided with a limited mailbox size (50,000KB), ...” replaced with “The Council will impose limits, when necessary, ...”.

Appendix 8 – Email Policy for ActiveSync Users Revisions

Policy Title: **Email Policy for ActiveSync Users** New Version: 2.0

Revisions:

a.	AMENDMENT	Para 7.1 Para 7.2 Para 7.3 Para 7.7	Amended to reflect the new Government Security Classifications.
b.	ADDITION	Para 7.1 Para 7.2 Para 7.3 Para 7.7	Reference to “other Government-approved email service” added in preparation for expected retirement of the GCSx mail service.
c.	AMENDMENT	General	Amendments to reflect current organisational structure.
d.	DELETION	Para 7.6	List of redundant security classifications deleted.
e.	DELETION	Para 9	Deleted in toto.
f.	ADDITION	Para10	“Bring Your Own Device Policy” added to list of references.

Appendix 9 – Information Security Incident Management Policy Revisions

Policy Title: **Information Security Incident Management Policy**
New Version: 3.0

Revisions:

a.	ADDITION	Intro	“How to Report an Information Security Incident” instruction panel added.
b.	ADDITION	Para 3	Council building tenants added to Policy Scope.
c.	ADDITION	Appendix 1	“Loss of Mobile Phone/Tablet added to list of example incidents
d.	AMENDMENT	Appendix 3	Incident Management Process Flow amendment

Appendix 10 – Internet Acceptable Use Policy Revisions

Policy Title: **Internet Acceptable Use Policy** New Version: 3.0

Revisions:

a.	ADDITION	Para 4	Text from Para 5 added: “The Policy should be applied at all times whenever using the Council-provided Internet facility. This includes access via any access device including a desktop computer or Council-approved smartphone device and when using any of the Council’s approved remote/home working channels.”.
b.	DELETION	Para 5	Para 5 moved and combined with Para 4. Para 5 deleted in toto. Paras renumbered.
c.	AMENDMENT	Para 5	Risk updated to read: “Uncontrolled access to the Internet from the corporate network could lead to loss of productivity, increased exposure to malware, spyware, phishing attacks and illegal or criminal activity resulting in user access to information systems and facilities being lost, legal action being taken against the Council as a result of misuse of the Internet or the Council failing to comply with the requirements for connecting to government secure networks.
d.	DELETION	Para 6.5 (formally 7.5)	Table of website categories blocked by web filter software deleted in toto. (No longer relevant)
e.	ADDITION	Para 6.6 (formally 7.6)	“Information Security Incident Management Policy” added to list of related policies.
f.	AMENDMENT	Para 7	“Team Manager, People and Organisational Development” replaced with “your manager”.

Appendix 11 – Mobile Device Policy Revisions

Policy Title: **Mobile Device Policy**

New Version: 2.0

Revisions:

a.	ADDITION	Para 4 Bullet 3	New sentence, "Information must not be stored solely on device desktops".
b.	ADDITION	Para 4 Bullet 4	Reference added to "Information Management and Protection Policy"
c.	AMENDMENT	Para 5	Amended to include reference to Enterprise Architecture principles.
d.	AMENDMENT	Para 5	Amended to reflect current organisation structure.
e.	ADDITION	Para 7 New bullet point 4	"Access tokens should be removed from the device immediately after logon and secured out of sight. Under no circumstances must they be stored with the device."
f.	AMENDMENT	Para 7 bullet point 6	Amended to include references to "local folders" and "desktop".
g.	ADDITION	Para 10	New sentence, "Third parties are required to agree and sign the Council's Third Party Connection Policy."
h.	AMENDMENT	Appendix 2	Clarified meaning of "personal work" and included "usage is logged and monitored".
i.	ADDITION	Appendix 4 Appendix 5	Added reference to "Bring Your Own Device Policy".

Appendix 12 – Public Service Network Acceptable Use Policy and Personal Commitment Statement Revisions

Policy Title: **Public Service Network Acceptable-Use Policy**

New Version: 2.0

a. Revisions:

a.	AMENDMENT	Para 1 bullet 1	“must” amended to “should” (relaxation of Government Policy on requirements for Baseline Personnel Security Standard Checks)
b.	ADDITION	Para 1	New sub-para – “Any Council staff who have administrative privileges (for example, users who are able to reconfigure the network or system administrators) MUST have been verified against the Baseline Personnel Security Standard (BPSS).”
c.	AMENDMENT	Para 5, List item 11	Para amended to add reference to the Information Management and Protection Policy
d.	AMENDMENT	General	Job titles etc, updated to reflect current organisation structure.
e.	AMENDMENT	Para 10	List of reference documents updated.

Data Protection Breach Policy

JSCC Approved :
CP&R Approved:

Document Control

Version Number	
Approved by	Corporate Policy and Resources Committee
Date approved	
Review Date	
Authorised by	Director of Resources
Contact Officer	Monitoring Officer

Contents

Contents	2
1. Policy Statement.....	3
2. Purpose	3
3. Scope	3
4. Legal Context.....	3
5. Types of Breach.....	3
6. Immediate Containment/Recovery.....	4
7. Investigation.....	5
8. Notification	5
9. Review and Evaluation	6
10. Related Documents.....	7
11. Implementation	7
12. Useful Contacts.....	7
Appendix 1 – Data Protection Breach Process Diagram.....	8
Appendix 2 - Data Protection Breach Notification Form.....	9

1. Policy Statement

1.1. West Lindsey District Council holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible.

2. Purpose

2.1. This policy sets out the procedure to be followed by all West Lindsey District Council staff if a data protection breach takes place.

3. Scope

3.1. This policy applies to all personal and sensitive data held by West Lindsey District Council.

3.2. Some typical examples of personal identifiable information include:-

- **Personal Data** – eg name; address; telephone number; date of birth; NI number; bank account details
- **Sensitive Personal Data** – eg information specifically relating to race or ethnicity; political opinions; religious beliefs, or beliefs of a similar nature; membership of a trade union or non-membership; physical or mental health or condition; sexual life; commission or alleged commission or an offence.

3.3. The principles of securing information (in accordance with Principle 7 of the Data Protection Act), can be found in the Council's Information Security Policy.

4. Legal Context

4.1. The Data Protection Act 1998 makes provision for the regulation of the processing (use) of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

4.2. Principle 7 of the Data Protection Act 1998 states that organisations which process personal data must take "appropriate technical and organisation measures against the unauthorised or unlawful processing of personal data and against accidental loss of destruction of, or damage to, personal data".

5. Types of Breach

5.1. Data protection breaches could be caused by a number of factors. Some examples are:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment Failure
- Human Error
- Unforeseen circumstances such as fire or flood
- Hacking
- 'Blagging' offences where information is obtained by deception.

6. Immediate Containment/Recovery

- 6.1. The following process is shown diagrammatically at Appendix 1.
- 6.2. A person who discovers/receives a report of an incident involving the confidentiality, integrity, or availability of Council data but which **does not** involve personal information must log an Information Governance Incident on Minerva. This will be investigated in line with the Information Security Incident Management Policy.
- 6.3. A person who discovers/receives a report of an incident involving the confidentiality, integrity, or availability of Council data **which involves personal information** must inform the ICT Helpdesk immediately. If the incident (breach) occurs or is discovered outside normal working hours, then the ICT Duty Officer (ICT Manager) must be contacted.
- 6.4. ICT Help-desk staff (or ICT Duty Officer) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, and to alert the relevant team manager or the Out of Hours Duty Officer.
- 6.5. The ICT Help-desk staff should contact the Data Protection Officer and the Information Governance Officer as soon as possible. The Information Governance Officer will provide advice and ensure that an Information Governance Incident is logged and maintained in accordance with the Information Security Incident Management Policy.
- 6.6. The ICT Help-desk staff in consultation with the Data Protection Officer must also consider whether the police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.
- 6.7. The ICT Help-desk staff must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:
- a. Attempting to recover lost equipment.
 - b. Contacting the Council's Customer Services Centre, Benefits or other relevant Council Departments, so that they are prepared for any potentially inappropriate enquiries 'phishing' for further information on the individual concerned. Consideration should be given to a global

email. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual making the enquiry back. Whatever the outcome of the call, it should be reported immediately to the ICT Help-desk.

- c. Contact the Communications Team so that they can be prepared to handle any press enquiries.
- d. The use of back-ups to restore lost/damaged/stolen data.
- e. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
- f. If the data breach includes any entry codes or passwords, then these codes must be changed immediately, and the relevant agencies and members of staff informed.
- g. Following an assessment of the level of risk associated with the incident a decision will be taken as to who will undertake an investigation into the incident.

7. Investigation

- 7.1. In most cases, the next stage would be for the relevant team manager to fully investigate the breach. The team manager should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation.
- 7.2. The investigation should consider the type of data, its sensitivity, what protections are in place (eg encryption), what has happened to the data, whether the data could be put to any illegal or inappropriate use, how many people are affected, what type of people have been affected (the public, suppliers etc) and whether there are wider consequences to the breach.
- 7.3. A clear record should be made of the nature of the breach and the actions taken to mitigate it.
- 7.4. The investigation should be completed urgently and wherever possible within 24 hours of the breach being discovered/reported. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

8. Notification

- 8.1. Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an investigation has taken place.
- 8.2. The team manager should, after seeking advice from the Data Protection Officer and the Information Governance Officer, decide whether anyone

should be notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) should be notified using the form at Appendix 2 of this document. Every incident should be considered on a case by case basis. The following points will help you decide whether and how to notify:

- Are there any legal/contractual requirements to notify?
- Will notification help prevent the unauthorised or unlawful use of personal data?
- Could notification help the individual – could they act on the information to mitigate risks?
- If a large number of people are affected, or there are very serious consequences, you should notify the ICO. The ICO should only be notified if personal data is involved. There is guidance available from the ICO on when and how to notify them, which can be obtained at:

http://www.ico.org.uk/for_organisations/data_protection/the_guide/principle_7

- Consider the dangers of over-notifying. Not every incident warrants notification and over-notification may cause disproportionate enquiries and work.
- The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach.
- When notifying individuals, give specific and clear advice on what they can do to protect themselves and what you are willing to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the Council's Complaints Procedure).

9. Review and Evaluation

- 9.1. Once the initial aftermath of the breach is over, the team manager should fully review both the causes of the breach and the effectiveness of the response to it. A report should be written and sent to the next available CLT meeting for discussion.
- 9.2. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources for advice and guidance.
- 9.3. This policy may need to be reviewed after a breach or after legislative changes, new case law or new guidance. Consideration should be given to reviewing this policy on an annual basis.

10. Related Documents

- Data Protection Policy
- Information Security Policy
- Information Security Incident Management Policy

11. Implementation

11.1. This policy takes effect immediately. All managers should ensure that staff are aware of this policy and its requirements. If staff have any queries in relation to the policy, they should discuss this with their line manager, the Information Governance Officer or the People and Organisational Development Team Manager.

12. Useful Contacts

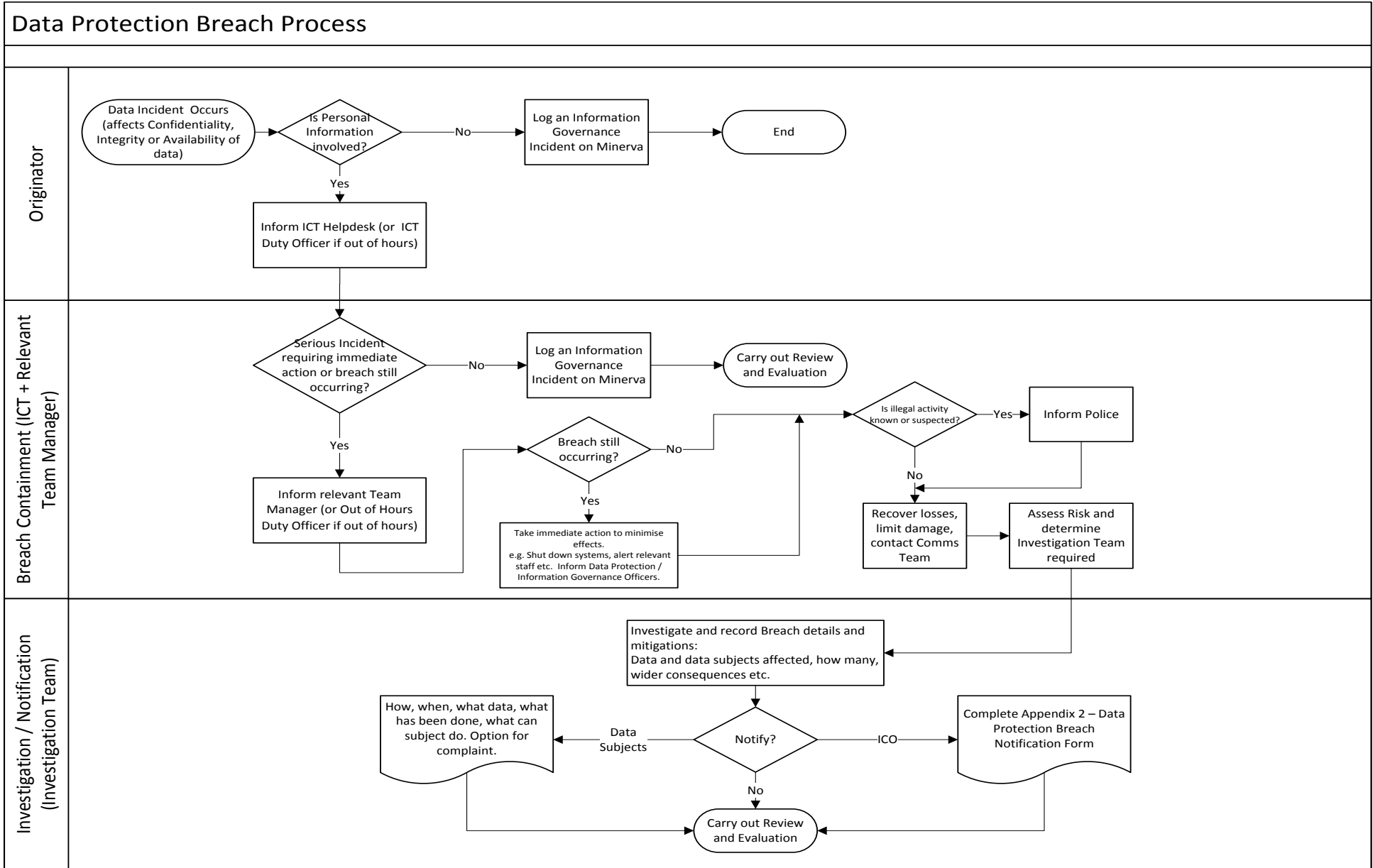
ICT Help-desk	01427 675165
ICT Manager – ICT Duty Officer (Cliff Dean)	07583033062
Ian Knowles (Senior Information Risk Owner)	01427 675183
Alan Robinson (Data Protection Officer)	01427 676509
Emma Redwood (TM – People and Organisational Development)	01427 676591
Steve Anderson (Information Governance Officer)	01427 676652

Alternative formats (ie hard copy, large print or Braille) of this procedure are available upon request.

Appendix 1 – Data Protection Breach Process Diagram

Data Protection Breach Process

Page 88



Appendix 2 - Data Protection Breach Notification Form

This form is to be used when data controllers wish to report a breach of the Data Protection Act to the ICO. It should not take more than 15 minutes to complete.

If you are unsure whether it is appropriate to report an incident, you should read the following guidance before completing the form: [Notification of Data Security Breaches to the Information Commissioner's Office](#).

Please provide as much information as possible and ensure that all mandatory (*) fields are completed. If you don't know the answer, or you are waiting on completion of an internal investigation, please tell us. In addition to completing the form below, we welcome other relevant supporting information, eg incident reports.

In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.

1. Organisation details

- (a) * What is the name of your organisation – is it the data controller in respect of this breach?
- (b) Please provide the data controller's registration number. [Search the online Data Protection Public Register](#).
- (c) * Who should we contact if we require further details concerning the incident? (Name and job title, email address, contact telephone number and postal address)

2. Details of the data protection breach

- (a) * Please describe the incident in as much detail as possible.
- (b) * When did the incident happen?
- (c) * How did the incident happen?
- (d) If there has been a delay in reporting the incident to the ICO please explain your reasons for this.

- (e) What measures did the organisation have in place to prevent an incident of this nature occurring?
- (f) Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.

3. Personal data placed at risk

- (a) * What personal data has been placed at risk? Please specify if any financial or sensitive personal data has been affected and provide details of the extent.
- (b) * How many individuals have been affected?
- (c) * Are the affected individuals aware that the incident has occurred?
- (d) * What are the potential consequences and adverse effects on those individuals?
- (e) Have any affected individuals complained to the organisation about the incident?

4. Containment and recovery

- (a) * Has the organisation taken any action to minimise/mitigate the effect on the affected individuals? If so, please provide details.
- (b) * Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.
- (c) What steps has your organisation taken to prevent a recurrence of this incident?

5. Training and guidance

- (a) As the data controller, does the organisation provide its staff with training on the requirements of the Data Protection Act? If so, please provide any extracts relevant to this incident here.
- (b) Please confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?
- (c) As the data controller, does the organisation provide any detailed guidance to staff on the handling of personal data in relation to the incident you are reporting? If so, please provide any extracts relevant to this incident here.

6. Previous contact with the ICO

- (a) * Have you reported any previous incidents to the ICO in the last two years?
- (b) If the answer to the above question is yes, please provide: brief details, the date on which the matter was reported and, where known, the ICO reference number.

7. Miscellaneous

- (a) Have you notified any other (overseas) data protection authorities about this incident? If so, please provide details.
- (b) Have you informed the Police about this incident? If so, please provide further details and specify the Force concerned.
- (c) Have you informed any other regulatory bodies about this incident? If so, please provide details.
- (d) Has there been any media coverage of the incident? If so, please provide details of this.

Sending this form

Send your completed form to casework@ico.org.uk, with 'DPA breach notification form' in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Please note that we cannot guarantee security of forms or any attachments sent by email.

What happens next?

When we receive this form, we will contact you within seven calendar days to provide:

- a case reference number; and
- information about our next steps

If you need any help in completing this form, please contact our helpline on **0303 123 1113** or **01625 545745** (operates 9am to 5pm Monday to Friday)

Freedom of Information and Environmental Information Policy

JSCC Approved :
CP&R Approved:

Document Control

Organisation	West Lindsey District Council
Title	Freedom of Information and Environmental Information Policy
Filename	
Owner	
Subject	Information Policy Document
Protective Marking	OFFICIAL
Review date	06/10/2016

Revision History

Revision Date	Revised By	Previous Version	Description of Revision
3/11/2011	Steve Anderson	Draft v0.2	Amendments requested by JSCC meeting held on 2/11/2011: Para 3 – Clarification of Corporate Information Officer's department. Paras 5.1 and 8 – website links replaced with friendly URLs.
16/2/2012	Steve Anderson	Draft v0.3	Formally adopted by Policy & Resources Committee
20/8/2013	Anne Rossington	V1.0	Change of job title at paragraphs 3 and 4
27/08/2014	Carolyn Lancaster	V1.1	Review – no amendments req'd
28/10/2014	Anne Rossington	V1.2	Amendments made – Section 3 Responsibilities – monitoring and reporting now go through the Progress and Delivery report, and no longer the Wider Management Team.
06/10/2015	Carolyn Lancaster	V2.0	Changed Service Managers to Team Managers in Para 3.

Contents

1. Policy Statement.....	3
2. Scope	3
3. Responsibilities.....	3
4. Available guidance.....	4
5. The Council's Publication Scheme	4
6. Specific requests for information.....	4
7. Charges for Freedom of Information Requests.....	5
8. Charges for Environmental Information Regulation Requests	5
9. Complaints.....	7
10. Review of policy	7

1. Policy Statement

- 1.1 West Lindsey District Council (the Council) takes its responsibilities for the management of the requirements of the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR) seriously.
- 1.2 This Policy outlines our approach to responding to requests for information made under the FOIA and the EIR.
- 1.3 It provides a framework to make sure that we fully support and consistently apply the principles of Freedom of Information, and meet the standards set out in the Lord Chancellor's Code of Practice on satisfying public authorities' obligations under the FOIA and the EIR.
- 1.4 The Policy aims to promote greater openness and to build public trust by providing access to information. We believe that access to information about decisions we take can help local people to influence local service provision. This will be balanced against the need to protect the confidentiality of, for instance, personal and commercially sensitive information.

2. Scope

- 2.1 This Policy applies to all employees, elected members, contractors, agents and representatives and temporary staff working for the Council.
- 2.2 The purpose of this Policy is to make sure that the Council complies with the terms of the FOIA and the EIR.
- 2.3 This Policy does not cover Subject Access Requests (requests for access to personal information). These are exempt from the FOIA under section 40 and are processed in line with the Data Protection Act 1998.

3. Responsibilities

- The Council recognises there is corporate responsibility to give the public a general right of access to all information held by the Council.
- The senior officer with overall responsibility for the Council's compliance with legislation, and therefore this policy, is the Chief Executive.
- Directors, Strategic Leads, and Team Managers are responsible for promoting openness and accountability in their teams and services.
- The Team Manager, People and Organisational Development is responsible for drawing up guidance on freedom of information and

promoting compliance with this Policy to allow easy, appropriate and timely retrieval of information.

- Team Manager, Customer Strategy and Services is responsible for monitoring and reporting through the Progress and Delivery report, on responses to requests for information.
- The Team Manager, People and Organisational Development will provide an advisory service to the remainder of the Council and will lead on any situations where decisions are reviewed or exemptions/exceptions are being considered.
- Line managers must make sure that all staff are aware of the requirements of the legislation and that all new staff receive an introductory briefing on the access to information procedures during their induction.
- All staff must recognise that all recorded information may be given to the public and that in every case the law requires that there will be full and unconditional disclosure unless one of the legal exemptions/exceptions applies.

4. Available guidance

- 4.1 Guidance on the procedures necessary to comply with this Policy is available for Council staff from Team Manager, People and Organisational Development or the Team Manager, Customer Strategy and Services, or on the Information pages on the Council's Intranet.

5. The Council's Publication Scheme

- 5.1 The Council's Publication Scheme is available on the website at <http://www.west-lindsey.gov.uk/your-council/how-the-council-works/information-and-information-governance/> or in hard copy.

- 5.2 The Publication Scheme specifies:

- what information the Council will make routinely available to the public;
- how it will do so; and
- whether information will be made available free of charge or on payment of a fee.

6. Specific requests for information

- 6.1 Information not already made available in the Council's Publication Scheme is accessible through a specific request for information. In this regard the FOIA establishes two related rights:

- the right to be told whether information exists; and
 - the right to receive the information (subject to exemptions or exceptions).
- 6.2 These rights can be exercised by anyone worldwide. Requests for access to information not listed in the publication scheme will be processed through the Council's access to information procedures.
- 6.3 Requestors will be entitled to all the information unless one of the legal exemptions/exceptions applies. However, only those specific pieces of information to which the exemption applies will be withheld.
- 6.4 Where the Council has decided that an exemption/exception applies it will, if appropriate, consider the prejudice test and/or the public interest test and may in some circumstances withhold the requested information.
- 6.5 The Council aims to respond to all requests within 20 working days although further reasonable details can be requested to identify and find the information. If a fee is required, the Council will issue a fees notice and the applicant has 3 months in which to pay before their request is considered as being withdrawn.

7. Charges for Freedom of Information Requests

- 7.1 Unless otherwise specified information made available through the Council's Publication Scheme will be free of charge.
- 7.2 The Council reserves the right to charge a fee for dealing with a specific request for information not listed in the publication scheme in line with the legislation.

8. Charges for Environmental Information Regulation Requests

What can be charged?

- 8.1 There are two types of activity under EIR that public authorities can charge for:
1. The cost of staff time spent locating, retrieving and extracting the information;
 2. The costs incurred when printing or copying the information and sending to the applicant.
- 8.2 However, the EIRs do allow the Council to make a charge to recover the costs of locating the information and collating it in order to make it available for inspection. A charge made for locating and collating information to be inspected must be reasonable. If the information is

held in a system that allows for straightforward public access it is unlikely that a charge is reasonable. If a requestor asks for inspection of material that would require a significant cost to prepare for inspection, the EIR allows the authority to make a charge.

What cannot be charged for?

8.3 There are costs the Council cannot charge for:

1. The costs of maintaining a register of information or a database;
2. Overhead costs (i.e. wider staff overheads);
3. Staff time spent reviewing and redacting information (although there are cases where staff time in this instance can be taken into account when considering if a request is Vexatious/Manifestly Unreasonable due to excessive burden on staff resource and time);
4. Charge applicants for inspecting the information or accessing public registers or lists of environmental information; and
5. For allowing access to the information in situ.

8.4 In addition, the ICO is clear that requestors should not be unfairly penalised in cases where the authority has failed to keep records in a reasonably accessible state. Therefore where the Council's systems prevent easy access to information purely because of records management issues, staff should fully consider whether it is appropriate to charge.

Schedule of Charges

8.5 Public authorities must have a published schedule of charges in order to be able to charge applicants for environmental information. Currently the Council uses the following rate:

Minimum charge of £70 (0% VAT)

<https://www.west-lindsey.gov.uk/my-council/contacts-facts-and-figures/council-spending/budget-book/>

Charging Threshold

8.6 This threshold is based upon the approximated time taken to locate, retrieve, extract and summarise the information required. This charge also covers any disbursement costs.

Manifestly Unreasonable

8.7 Where it is estimated that complying with a request will exceed 18 hours, the Council will consider whether the request is in fact Manifestly Unreasonable under Regulation 12(4) (b) of the Environmental Information Regulation Act 2004 and will use existing procedures for

doing so, including applying the Public Interest Test and providing advice and assistance to the requestor in order to narrow down the scope of their request. The 18 hour timeframe is that used under the FOIA to determine if a request exceeds an appropriate limit.

Issuing a Charge

8.8 The decision to issue a charge will be made promptly and within 3 working days of the receipt of the request wherever possible, in order to ensure that deadlines for responding to requests within the 20 working days limit are met. A response will be sent to the requestor, which informs the requestor that a fee is payable and how to make payment.

Advance Payment

8.9 In all cases where a fee is charged, payment will be required in advance of disclosure.

8.10 Requestors will have 60 days for payment to reach the council. Where payment is not received, it will be assumed that the information is no longer required and the request terminated.

8.11 Payment can be made by phone by calling 01427 676676 and selecting the option for 'All other enquiries'. The requestor must advise that payment is in relation to an EIR request, quoting the EIR reference number. The payment will then be assigned under the relevant Ledger Code by the Council.

Review of Costs

8.12 Costs will be reviewed annually to endeavour to keep costs reasonable.

9. Complaints

An individual has the right to complain about the response they have received regarding their request for information. Details of the council's Data Protection and Freedom of Information Complaints Procedure can be found at <http://www.west-lindsey.gov.uk/your-council/have-your-say/comments-compliments-and-complaints/> .

10. Review of policy

10.1 This policy shall be reviewed annually.

Records Management Policy

Document Control

Organisation	West Lindsey District Council
Title	Records Management Policy
Author	Steve Anderson
Date	16 Jan 2014
Review date	16 Jan 2015

Contents

1. What is Records Management?.....	3
2. Objectives.....	3
3. Legislation	3
4. Roles and responsibilities	4
5. Accuracy of personal records and data	4
6. Access to records (Statutory public access)	4
6.1. Subject Access Requests	4
6.2. Freedom of Information.....	5
6.3. Environmental Information Regulations	5
6.4. Standards for the storage of paper records.....	5
7. Standards for managing electronic records and email.....	5
8. Retention and disposal schedules	6
9. Offsite Storage Procedure and Guidance	6
10. Corporate Records Destruction Procedure.....	6

1. What is Records Management?

Records management is the practice of maintaining records from the time they are created up to their eventual disposal. This may include classifying, storing, securing, and destruction (or in some cases, archival preservation) of records.

A record can be on paper, a physical object or digital records, for example, customer records, birth certificates, office documents, prosecution evidence, electronic systems and e-mail. Records management is primarily concerned with retaining records produced from the Council's business activities.

Records Management is governed by a number of laws and regulations, several of which concern Data Protection and Freedom of Information.

2. Objectives

West Lindsey District Council ("the Council") is committed to improve the way in which it creates, maintains, and destroys information and records.

Records will be managed in appropriate management systems and organised accordingly; for example alphabetically, numerically, in date order, etc. Reference numbers and/or version control must be applied. This will assist with identifying records which need to be accessed in the future, and for storing of records prior to destruction.

Retention and disposal schedules will be followed to make sure that appropriate retention periods are maintained prior to destruction of records so the Council complies with relevant legislation and regulations.

Mandatory training is provided for employees and Elected Members on the importance of managing records effectively.

Policies, procedure and guidance must be used in conjunction with the Council's retention and disposal schedules.

Audits will be carried out to monitor compliance with policy, procedure and guidance for safe management of records.

3. Legislation

The Council is required by law to comply with all relevant legislation or guidance. All employees (including temporary employees), Elected Members, partners and external contractors must comply with the relevant legislation when acting on behalf of West Lindsey District Council.

The Council will comply with the following legislation and guidance, and any other legislation as appropriate:

- Data Protection Act 1998
- The Freedom of Information Act 2000
- Public Records Act 1958
- Re-use of Public Sector Information Regulations 2005

- Employment legislation
- Health and safety legislation

4. Roles and responsibilities

Development of records management procedures and practices are the responsibility of the Corporate Information Governance Group (CIGG) who report to the Director of Resources (the Council's Senior Information Risk Owner (SIRO)).

All employees and Elected Members of the authority are responsible for the records they hold on behalf of the Council. They must follow this Policy and all procedures, guidance, and the retention and disposal schedules approved by the Governance Corporate Leadership Team (GCLT).

Datasets stored in corporate systems must be assigned an Information Asset Owner (IAO). IAOs are responsible for all aspects of the protection, use, and retention of the data. They must authorise any request to use data for alternative purposes in line with all relevant legislation.

All records created by Council employees and elected members will remain the property of the Council.

The creation, maintenance and destruction of records are the responsibility of the department providing the service. Each department must manage records in accordance with this policy and all associated policies and procedures. It is essential records are stored securely and the location of files is up to date at all times.

5. Accuracy of personal records and data

The Council must make sure all information is processed in accordance with the Data Protection Act. The Council's Data Protection Policy explains how employees are expected to comply with the Act when creating and maintaining records on behalf of the Council.

All records must be accurate, up to date and not excessive. Any corrections, amendments or additions to a record are to be made in accordance with departmental procedures and a record of changes retained for audit purposes.

6. Access to records (Statutory public access)

6.1. Subject Access Requests

The Data Protection Act 1998 (Subject Access) gives individuals the right to access their personal information held by the Council. Policy, procedure and guidance can be found on the Council's Intranet and <http://www.west-lindsey.gov.uk/>

6.2. Freedom of Information

The Freedom of Information Act gives the people a right to know what decisions are taken on their behalf by the Council on how services are run. The Council has published a publication scheme which shows what information can already be accessed. Any information which is not part of the Publication Scheme can be requested under the Freedom of Information Act. There may be exceptions where statutory exemptions apply. Further guidance and contact information can be found on the Intranet and <http://www.west-lindsey.gov.uk/>

6.3. Environmental Information Regulations

The Government have issued regulations to local Government which make it easy for people to access information about the state of the elements of the environment (air, atmosphere, water, soil, landscape, natural sites and ecology, biological diversity, and genetically modified organisms). Some information related to this is contained within the Council's Publication Scheme. Further guidance and contact information can be found on the Intranet and <http://www.west-lindsey.gov.uk/>

6.4. Standards for the storage of paper records

The Council must make sure records are protected from damaging elements such as water, light, temperature, humidity, fire and infestation.

The security of the information must also be protected by keeping storage units and rooms locked when not in use. Access to keys must be restricted to the responsible service area employees.

Locations such as basements are not suitable for long term storage so alternative arrangements must be made.

Records must be managed in line with the Council's retention and disposal schedules and destruction and offsite storage procedures which are available on the Intranet.

7. Standards for managing electronic records and email

It is essential regular housekeeping is carried out to make sure stored records are saved for the appropriate length of time in line with retention and disposal schedules. Records which form part of the corporate memory must be saved into the relevant system or shared work areas. An email mailbox is not a suitable place to store corporate records.

The Information Security Policy has further information on appropriate management of electronic records and email and is available on the Intranet.

8. Retention and disposal schedules

The Council's retention and disposal schedules identify the types of records held and length of time each document or electronic record is retained, and when it should be destroyed. In some cases, records are retained permanently.

Departments are consulted on the types of records held and agreement reached on the appropriate length of time set for retention of those records. Requests can be made to change retention periods but there must be a valid business reason and agreement with Information Governance. Some retention periods are governed by statutory legislation so it is important retention periods are applied correctly when deciding how long to keep or destroy a record.

All records have different retention periods, for example the destruction date may be from last involvement (closed record/last action entry) or from date of birth. This must be checked on the corporate retention and disposal schedules.

Where systems have the functionality to enforce retention and disposal policies they must be properly configured to do so.

The retention and disposal schedules can be found on the Intranet.

9. Offsite Storage Procedure and Guidance

The Council is required to keep records for specified periods of time after involvements have ended. The length of time for keeping closed records varies dependent upon the nature of the involvement the Council had with the customer.

The retention period for each type of record is specified in the Council's retention and disposal schedules.

The Offsite storage procedure and guidance contains guidance in relation to the processes for preparing records prior to sending offsite and for retrieving closed records.

10. Corporate Records Destruction Procedure

The Council has a statutory duty under the Data Protection Act to make sure records relating to living individuals are not kept for an excessive amount of time. Where records are outside of the retention period they must be destroyed unless there is a valid reason for retaining them. If the responsible department has a business need to retain information after the destruction date set the Information Governance team must be notified and an agreement reached to change. The records destruction procedure is available on the Intranet.

IT Infrastructure Security Policy

Document Control

Organisation	West Lindsey District Council
Title	IT Infrastructure Security Policy
Author	S M Anderson
Owner	ICT Manager
Subject	IT Policy
Review date	15/8/2015

Revision History

Revision Date	Revised By	Previous Version	Description of Revision
15/8/2013	S M Anderson	V1.0	Reviewed for PSN Compliance.

Contents

Contents	2
1 Policy Statement	3
2 Key Messages.....	3
3 Purpose.....	3
4 Scope	4
5 Definition	4
6 Risks	4
7 Applying the Policy	5
7.1 Secure Areas	5
7.2 Non-Electronic Information Security	6
7.3 Equipment Security	6
7.4 Cabling Security	7
7.5 Equipment Maintenance.....	7
7.6 Security of Equipment off Premises	8
7.7 Secure Disposal or Re-use of Equipment	8
7.8 Delivery and Receipt of Equipment into the Council	9
7.9 Regular Audit	9
8 Policy Compliance.....	9
9 Review and Revision.....	9
10 References	9

1 Policy Statement

There shall be no unauthorised access to either physical or electronic information within the custody of West Lindsey District Council (“the Council”).

Protection shall be provided for:

- Sensitive paper records.
- IT equipment used to access electronic data.
- IT equipment used to access the Council network.

2 Key Messages

- OFFICIAL information and equipment used to store and process this information must be **stored** securely.
- Only staff or visitors who can be confirmed as having been verified to the Baseline Personnel Security Standard (BPSS) are to be permitted unescorted access to the data centre or IT equipment rooms.
- Keys to all secure areas housing IT equipment and lockable IT cabinets are held centrally by IT department, as appropriate. Keys are not stored near these secure areas or lockable cabinets.
- All general computer equipment must be located in suitable physical locations.
- Desktop PCs, laptops and tablets should not have data stored on the local hard drive.
- Non-electronic information must be assigned an owner and a classification. OFFICIAL information must have appropriate information security controls in place to protect it.
- Staff should be aware of their responsibilities in regard to the Data Protection Act. The Team Manager, People and Organisational Development can provide advice if required.
- Equipment that is to be reused or disposed of must have all of its data and software erased / destroyed.
- All security breaches or observed weaknesses must be reported in accordance with the Council’s Information Security Incident Management Policy.
- If in any doubt call ICT on ext. 165 and log a helpdesk call.

3 Purpose

The purpose of this Policy is to establish standards in regard to the physical and environmental security of the Council’s information, in line with section A9 of ISO/IEC/27001.

Access the Council’s information equipment and information must be controlled to assure the protection of the personal, confidential and OFFICIAL information that the Council holds and uses. Control of access is also required to comply with legislative requirements, information security best practice, and security

frameworks such as PCI-DSS security standards regulating credit and debit card transactions and access to the Public Service Network (PSN),

This protection may be as simple as a lock on a filing cabinet or as complex as the security systems in place to protect the Council's IT data centre. The protection required needs to be appropriate to the level of information held and the consequential risks of unauthorised access. No service should allow the protection provided for their teams and locations to fall below that required for the level of information held.

4 Scope

All West Lindsey District Council Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council with access to the Council's equipment and information (electronic and paper records) are responsible for ensuring the safety and security of the Council's equipment and the information that they use or manipulate.

5 Definition

This Policy applies to all users of the Council's owned or leased / hired facilities and equipment. It defines what paper and electronic information belonging to the Council should be protected and offers guidance on how such protection can be achieved. The Policy also describes employee roles and the contribution staff make to the safe and secure use of information within the custody of the Council.

The Policy should be applied whenever a user accesses Council information or information equipment. It applies to all locations where information within the custody of the Council or information processing equipment is stored, including remote sites.

6 Risks

The Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This Policy aims to mitigate the following risks:

- Inadequate physical security controls lead to a loss of personal or sensitive information resulting in a monetary penalty and/or reputational damage.
- Inadequate or inappropriate physical and technical security controls provided for IT equipment used or transported outside the Council's physical security boundary lead to a loss of personal or sensitive information resulting in a monetary penalty and/or reputational damage.
- Failure to adequately destroy data when re-using or disposing of redundant, obsolete, or defective equipment leads to a loss or disclosure

of personal or sensitive information resulting in a monetary penalty and/or reputational damage.

- Non-reporting of information security incidents.
- Loss of direct control of user access to information systems and facilities.

Non-compliance with this Policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

7 Applying the Policy

7.1 Secure Areas

All information produced by the Council is OFFICIAL and **must** be stored appropriately. A risk assessment should identify the **appropriate** level of protection required for the information being stored.

Physical security must begin with the building itself and an assessment of perimeter vulnerability must be conducted. The building must have **appropriate** control mechanisms in place for the type of information and equipment that is stored there. These could include, but are not restricted to, the following:

- Alarms fitted and activated outside working hours.
- Window and door locks.
- Window bars on lower floor levels.
- Access control mechanisms fitted to all accessible doors (where codes are utilised they should be regularly changed and known only to those people authorised to access the area/building).
- CCTV cameras.
- Staffed reception area.
- Protection against damage - e.g. fire, flood, vandalism.

As an example, access to secure areas such as the data centre and IT equipment rooms must be adequately controlled and physical access to buildings should be restricted to authorised persons.

Only staff or visitors who can be confirmed as having been verified to the Baseline Personnel Security Standard (BPSS) are to be permitted unescorted access to the data centre or IT equipment rooms.

Staff working in secure areas should challenge anyone not wearing a badge or equivalent identification tag. Each department must ensure that doors and windows are properly secured.

Identification and access tools/passes (e.g. badges, keys, entry codes etc.) must only be held by officers authorised to access those areas and should not be loaned/provided to anyone else.

Visitors to secure areas are required to sign in and out with arrival and departure times and are required to wear an identification badge. A Council IT employee **must** monitor all visitors accessing secure IT areas and who cannot be confirmed as having been verified against the BPSS, **at all times**.

Keys to all secure areas housing IT equipment and lockable IT cabinets are held centrally by the IT department, as appropriate. Keys are not stored near these secure areas or lockable cabinets.

In all cases where security processes are in place, instructions must be issued to address the event of a security breach. Where breaches do occur, or a member of staff leaves outside normal termination circumstances, all identification and access tools/passes (e.g. badges, keys etc.) should be recovered from the staff member and any door/access codes should be changed immediately. Please also refer to the IT Access Policy and the Human Resources Information Security Standards (TBA). All security breaches or observed weaknesses must be reported in accordance with the Council's Information Security Incident Management Policy.

7.2 Non-Electronic Information Security

Paper based (or similar non-electronic) information must be assigned an owner and a classification as stated in the Information Management and Protection Policy. All Government information is classified as OFFICIAL and appropriate information security controls to protect it must be put in place. A risk assessment should identify the appropriate level of protection required for the information being stored. Paper in an open office must be protected by the controls for the building (please refer to section 6.1) and via appropriate measures that could include, but are not restricted to, the following:

- Filing cabinets that are locked with the keys stored away from the cabinet.
- Locked safes.
- Stored in a Secure Area protected by access controls.

7.3 Equipment Security

All general computer equipment must be located in suitable physical locations that:

- Limit the risks from environmental hazards – e.g. heat, fire, smoke, water, dust and vibration.
- Limit the risk of theft – e.g. **if necessary** items such as laptops should be physically attached to the desk using Kensington locks (or an authorised alternative).
- Allow workstations handling sensitive data to be positioned so as to eliminate the risk of the data being seen by unauthorised people.

Desktop PCs, laptops and tablets should not have data stored on the local hard drive. Data should be stored on the network file servers where appropriate.

This ensures that information lost, stolen or damaged via unauthorised access can be restored with its integrity maintained. Information concerning network drives and the appropriate place to store Council information can be found in the ICT guidance material.

All servers and associated network equipment must be sited in a physically secure environment. Business critical systems should be protected by an Un-interrupted Power Supply (UPS) to reduce the operating system and data corruption risk from power failures. The equipment must not be moved or modified by anyone without authorisation from the IT Department.

All items of equipment must be recorded on an inventory. The ICT Team Leader maintains the ICT Inventory and ensures that it is updated as soon as assets are received or disposed of.

All equipment must be security marked and have a unique asset number allocated to it. This asset number should be recorded in the Council's Asset Register and the IT Department inventory.

For portable computer devices which are used away from Council property please refer to the Remote Working Policy and the Mobile Device Policy.

7.4 Cabling Security

Cables that carry data or support key information services must be protected from interception or damage. Where practical, power cables should be separated from network cables to prevent interference (this does not apply to Power over Ethernet (PoE) powered devices such as Voice over Internet Protocol (VoIP) telephones. Network cables should be protected by conduit and where possible avoid routes through public areas.

7.5 Equipment Maintenance

The IT Department, all Departmental ICT representatives (if appropriate) and 3rd party suppliers must make sure that all of the Council's ICT equipment is maintained in accordance with the manufacturer's instructions and with any documented internal procedures to ensure it remains in working order. Staff involved with maintenance should where appropriate:

- Retain all copies of manufacturer's instructions.
- Identify recommended service intervals and specifications.
- Enable a call-out process in event of failure.
- Ensure only authorised technicians complete any work on the equipment.
- Record details of all remedial work carried out.
- Identify any insurance requirements.
- Record details of faults incurred and actions required.

A service history record of equipment should be maintained so that when equipment becomes older decisions can be made regarding the appropriate time for it to be replaced.

Equipment maintenance must be in accordance with the manufacturer's instructions. This must be documented and available for support staff to use when arranging repairs.

7.6 Security of Equipment off Premises

The use of equipment off-site must be formally approved by the user's Team Manager. Equipment taken away from Council premises is the responsibility of the user and should:

- Be logged in and out, where applicable.
- Not be left unattended.
- Concealed whilst transported.
- Not be left open to theft or damage whether in the office, during transit or at home.
- Where possible, be disguised (e.g. laptops should be carried in less formal bags).
- Be encrypted.
- Be password protected.
- Be adequately insured.

Where a device is accessed using a two-factor authentication method such as BitLocker then access tokens must be stored separately from the device. They must never be kept in the same storage bag or container as the device. Furthermore, after a token or key has been used to gain access to a device then it should be removed from the device and secured.

Further information can be found in the Mobile Device Policy, Removable Media Policy and Remote Working Policy.

Users should ensure, where necessary and required, that insurance cover is extended to cover equipment which is used off site. Users should also ensure that they are aware of and follow the requirements of the insurance policy. Any losses / damage must be reported to the IT Department and the Finance Section.

Staff should be aware of their responsibilities in regard to Data Protection and be conversant with the Data Protection Act (please refer to the Legal Responsibilities Policy).

7.7 Secure Disposal or Re-use of Equipment

Equipment that is to be reused or disposed of must have all of its data and software erased / destroyed. If the equipment is to be passed onto another organisation (e.g. returned under a leasing agreement) the data removal must be achieved by using professional data removing software tools. Equipment must be returned to IT for data removal.

Software media or services must be destroyed to avoid the possibility of inappropriate usage that could break the terms and conditions of the licences held.

7.8 Delivery and Receipt of Equipment into the Council

In order to confirm accuracy and condition of deliveries and to prevent subsequent loss or theft of stored equipment, the following must be applied:

- Equipment deliveries must be signed for by an authorised individual using an auditable formal process. This process should confirm that the delivered items correspond fully to the list on the delivery note. Actual assets received must be recorded.
- Loading areas and holding facilities should be adequately secured against unauthorised access and all access should be auditable.
- Subsequent removal of equipment should be via a formal, auditable process.

7.9 Regular Audit

Internal Audit is responsible for auditing information security arrangements regularly to provide an independent appraisal and recommending security improvements where necessary.

8 Policy Compliance

If any user is found to have breached this Policy, they may be subject to the Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this Policy or how it may apply to you, seek advice from the IT Department.

9 Review and Revision

This Policy will be reviewed as it is deemed appropriate, but no less frequently than every 24 months.

Policy review will be undertaken by The ICT Manager supported by the Corporate Information Governance Group (CIGG).

10 References

The following Council Policy documents are directly relevant to this Policy, and are referenced within this document:

- IT Access Policy.
- Information Management and Protection Policy.

- Human Resources Information Security Standards (TBA).
- Remote Working Policy.
- Removable Media Policy.
- Mobile Device Policy
- Legal Responsibilities Policy.
- Information Security Incident Management Policy.

The following Council Policy documents are indirectly relevant to this Policy:

- PSN Acceptable Usage Policy and Personal Commitment Statement.
- Computer, Telephone and Desk Use Policy.
- Communications and Operation Management Policy (TBA).

Removable Media Policy

Document Control

Organisation	West Lindsey District Council
Title	Removable Media Policy
Author	Steve Anderson
Date	16 Jan 2014
Review date	16 Jan 2015

Revision History

Revision Date	Reviser	Version	Description of Revision
26/11/2013	Steve Anderson	Draft Version 0.2	Para 5 Definition amended to add Smartphones and Tablet Computers (JSCC Chairman's Brief – 25/11/2013)
11/12/2013	Steve Anderson	Draft Version 0.3	Para 5 Definition – Media Card Readers amended to Media Cards (JSCC – 10/12/2013)

Contents

1	Policy Statement	4
2	Key Messages	4
3	Purpose	4
4	Scope	5
5	Definition	5
6	Risks	5
7	Applying the Policy	6
7.1	Procurement of Removable Media	6
7.2	Security of Data	6
7.3	Incident Management	7
7.4	Third Party Access to Council Information	7
7.5	Preventing Information Security Incidents	7
7.6	Disposing of Removable Media Devices	7
7.7	User Responsibility	8
8	Policy Compliance	9
9	Review and Revision	9
10	References	9

1 Policy Statement

West Lindsey District Council (“the Council”) will control the use of removable media devices to store and transfer information by all users who have access to information, information systems and IT equipment for the purposes of conducting official Council business.

2 Key Messages

The key messages within this policy are summarised below:-

- It is the Council’s policy to prohibit the use of all removable media devices. Exceptions to this will only be approved if there is a valid business case for using a device.
- An inventory of all removable media devices supplied by the Council is to be maintained by the ICT Department.
- All removable media devices supplied by the Council are to be encrypted using approved encryption software by the ICT Department.
- Any removable media device that has not been supplied by the Council **should not** be used. Any exceptions to this, such as an external training provider delivering a presentation using their own media, must be first approved by the ICT Department and devices must be scanned for viruses and malware. Access to approved externally-provided devices must be set to **read-only**.
- All data stored on removable media devices **must** only be on encrypted devices.
- Damaged or faulty removable media devices must not be used.
- Special care **must** be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.
- Removable media devices that are no longer required, or have become damaged, must be returned to the ICT Department and disposed of securely to avoid data leakage.

3 Purpose

This document states the Removable Media policy for the Council. The Policy establishes the principles and working practices that are to be adopted by all users in order for data to be safely stored and transferred on removable media.

This Policy aims to ensure that the use of removable media devices is controlled in order to:

- Enable the correct data to be made available where it is required.
- Maintain the integrity of the data.
- Prevent unintended or deliberate consequences to the stability of the Council’s computer network.
- Avoid contravention of any legislation, policies or good practice requirements.
- Build confidence and trust in the data that is being shared between systems.
- Maintain high standards of care in ensuring the security of OFFICIAL information.
- Prohibit the disclosure of information as may be necessary by law.

4 Scope

This Policy applies to all Councillors; Committees; Departments; Partners; Employees of the Council; contractual third parties and agents of the Council who have access to Council information, information systems or IT equipment and intend to store any information on removable media devices.

5 Definition

This Policy should be adhered to at all times, but specifically whenever any user intends to store information used by the Council to conduct official business on removable media devices.

Removable media devices include, but are not restricted to the following:

- CDs
- DVDs
- Optical Disks
- External Hard Drives
- USB Memory Sticks (also known as pen drives or flash drives)
- Media Cards
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards)
- Smartphones
- Tablet Computers
- MP3 Players
- Digital Cameras
- Backup Cassettes
- Audio Tapes (including Dictaphones and Answering Machines)

6 Risks

The Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business. Information is used throughout the Council and sometimes shared with external organisations and applicants. Securing personal and sensitive personal data is of paramount importance – particularly in relation to the Council's need to protect data in line with the requirements of the Data Protection Act 1998.

Any loss of the ability to access information or interference with its integrity could have a significant effect on the efficient operation of the Council. It is therefore essential for the continued operation of the Council that the confidentiality, integrity and availability of all information recording systems are maintained at a level, which is appropriate to the Council's needs.

This Policy aims to mitigate the following risks:

- Disclosure of information as a consequence of loss, theft or careless use of removable media devices.

- Contamination of Council networks or equipment through the introduction of viruses through the transfer of data from one form of IT equipment to another.
- Potential sanctions against the Council or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the Council or individuals as a result of information loss or misuse.
- Damage to the Council's reputation as a result of information loss or misuse.

Non-compliance with this Policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

7 Applying the Policy

It is the Council's policy to discourage the use of removable media as far as reasonably practicable. Where there is no practicable alternative, such as working remotely with no secure network connection, then removable media may be used but only when a properly risk-assessed business case is provided by the relevant team manager. There are significant risks associated with the use of removable media and, therefore, clear business benefits that outweigh the risks must be demonstrated before approval will be given.

Should access to, and use of, removable media devices be approved the following sections apply and must be adhered to at all times.

7.1 Procurement of Removable Media

All USB memory sticks and external hard drive devices must only be purchased through the ICT Department. Non-Council owned removable media devices of any type should not be used to store any information used to conduct official Council business, and should not be used with any Council owned or leased IT equipment. Exceptions to this, such as an external training provider delivering a presentation using their own media, must be first approved by the ICT Department and devices must be scanned for viruses and malware. Access to approved externally-provided devices **must be** set to read-only.

An inventory of all removable media devices supplied by the Council is to be maintained by the ICT Department and each device must be logged out and back in.

7.2 Security of Data

Data that is only held in one place and in one format is at much higher risk of being unavailable or corrupted through loss, destruction or malfunction of equipment, than data which is frequently backed up. Therefore removable media should not be the only place where data obtained for Council purposes is held. Copies of any data stored on removable media must also remain on the source system or network until the data is successfully transferred back to the network or system. Data stored on removable media must only be done so temporarily and removed at the earliest opportunity. Data should not be permanently held on a removable media device.

In order to minimise physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment.

Each user is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way whilst in their care or under their control.

All data stored on removable media, must be stored on encrypted removable media devices.

7.3 Incident Management

It is the duty of all users to immediately report any actual or suspected breaches in information security in accordance with the Council's Information Security Incident Management Policy by completing a **Report an Information Governance Incident** on the Council's Intranet.

It is the duty of all councillors to report any actual or suspected breaches in information security to the Monitoring Officer or the Director of Resources.

7.4 Third Party Access to Council Information

No third party (external contractors, partners, agents, the public, or non-employee parties) may extract information from the Council's network information stores or IT equipment and place on a removable media device without explicit agreement by the Director of Resources or the ICT Manager.

Should third parties be allowed access to Council information then all the considerations of this Policy apply to their storing and transferring of the data.

7.5 Preventing Information Security Incidents

Damaged or faulty removable media devices must not be used. It is the duty of all users to stop using removable media when it is damaged and return them to the ICT Department.

Virus and malware checking software approved by the Council's IT Department must be operational on both the machine from which the data is taken and the machine on to which the data is to be loaded. The data must be scanned before the media is loaded on to the receiving machine.

Whilst in transit or storage the data held must be on an encrypted device to reduce risk to the Council, other organisations or individuals from the data being lost whilst in transit or storage.

7.6 Disposing of Removable Media Devices

Removable media devices that are no longer required, or have become damaged, must be returned to the ICT Department. Damaged devices must be disposed of securely to avoid data leakage. Any previous contents of any reusable media must be erased. This must be a thorough removal of all data from the media to avoid potential data leakage using specialist software and tools.

For advice or assistance on how to thoroughly remove all data, including deleted files, from removable media contact the ICT Department.

7.7 User Responsibility

All considerations of this Policy must be adhered to at all times when using all types of removable media devices. However, special attention must be paid to the following when using USB memory sticks (also known as pen drives or flash drives), recordable CDs, DVDs and diskettes:

- Any removable media device used in connection with Council equipment or the network or to hold information used to conduct official Council business **must** only be purchased and installed by the ICT Department. Any removable media device that has not been supplied and logged out by the ICT Department **must not** be used.
- All data stored on removable media devices **must** only be stored on encrypted devices supplied through the ICT Department.
- Virus and malware checking software **must** be used when the removable media device is connected to a machine.
- Only data that is authorised and necessary to be transferred should be saved on to the removable media device. Data that has been deleted can still be retrieved.
- Removable media devices **must not** to be used for archiving or storing records as an alternative to other storage equipment.
- Special care **must** be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.
- A record of the information placed onto any removable media device **must** be kept by the user and be available to the relevant team manager, the ICT Department and the Corporate Information Governance Group (CIGG) in the event of any actual or suspected breach in information security.
- Information held on a removable media device must be kept to a minimum, and no more case files / sets of information than required for the approved purpose are to be held on a device at any time.
- All information should be removed from the removable media device and placed onto the Council's network as soon as possible.
- Memory sticks used to provide the encryption keys required to unlock tablet computers are to be removed from the tablet immediately after boot. Encryption keys must be kept separate from the tablet to prevent unauthorised access to the corporate network and data.

For advice or assistance on how to securely use removable media devices, or for further advice or clarification on any part of this policy, please contact the ICT Department.

8 Policy Compliance

Whilst respecting the privacy of authorised users, the Council maintains its legal right, in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of removable media by authorised users to ensure adherence to this Policy. Any such interception or monitoring will be carried out in accordance with the provisions of this legislation. Users should be aware that deletion of items from removable media does not necessarily result in permanent deletion.

In addition to routine monitoring and audits, where a manager suspects that the removable media is being abused or misused by a user, they should inform their line manager, who will, if deemed appropriate, contact the Director of Resources and/or Team Manager People and Organisational Development to determine whether an investigation is appropriate. Should an investigation be authorised, designated staff in the ICT Department, or Internal Audit may assist or carry out this task.

In addition the Council will also comply with any legitimate requests for information from authorised bodies under the Regulation of Investigatory Powers or other applicable legislation.

If any user is found to have breached this Policy, they may be subject to the Council's disciplinary procedure. If a criminal offence is considered to have been committed, further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from your team manager or the ICT Department.

9 Review and Revision

This Policy will be reviewed by the Council as it is deemed appropriate, but no less frequently than every 12 months.

10 References

The Council has a suite of Information Security policy documents that are directly or indirectly relevant to this policy. These are:-

- Information Security Policy
- Data Protection Policy
- Remote Working Policy
- Information Security Incident Management Policy
- Legal Responsibilities Policy

In addition, users should also be familiar with the following Council policy:-

- Disciplinary Policy

It is the user's responsibility to ensure their awareness of and compliance with all of these policies. Further information can be obtained from your manager, the ICT Department, or from the Council's Intranet.



Computer, Telephone, and Desk-Use Policy

Document Control

Organisation	West Lindsey District Council
Title	Computer, Telephone and Desk Use Policy
Author	J Anderson
Filename	
Owner	ICT Team Leader
Subject	IT Policy
Protective Marking	Not Protectively Marked
Review date	15/8/2014

Revision History

Revision Date	Revised By	Previous Version	Description of Revision
15/8/2013	S M Anderson	V1.0	Reviewed for PSN Compliance – Lists of relevant policy documents updated
14/10/2014	S M Anderson	V1.1	Annual Review – Amended to include new Government Classification Markings

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date

Contents

1. Policy Statement	4
2. Key Messages	4
3. Purpose	4
4. Scope	4
5. Definition	5
6. Risks	5
7. Applying the Policy	6
7.1 Computer Resources Misuse	6
7.2 Telephone	6
7.3 Clear Desk	6
7.4 Legislation	7
8. Policy Compliance	8
9. Review and Revision	8
10. References	8
Appendix 1 – Code of Practice Relating to Private Telephone Calls	9

1. Policy Statement

West Lindsey District Council (“the Council”) will make sure that every user is aware of, and understands, the acceptable use of the Council’s computer and telephony resources and the need to operate within a “clear desk” environment.

2. Key Messages

- Users must adhere to the Council’s Computer, Telephone and Desk Use Policy at all times.
- Users of the Council’s telephony facilities must follow the Code of Practice Relating to Private Telephone Calls (Appendix 1 of this document).
- Users must not leave sensitive information in clear view on an unattended desk.
- Users must leave a clean, clear desk at the end of the day.
- Council OFFICIAL-SENSITIVE information must be stored in a facility (e.g. lockable safe or cabinet) suitable for this classification level.

3. Purpose

Modern day business operations and advances in technology have necessitated the wide spread use of computer facilities into most offices within the Council and, with the introduction of portable computers, away from the Council’s premises.

As such, there is considerable scope for the misuse of computer resources for fraudulent or illegal purposes, for pursuing personal interests or for amusement/entertainment. The Council also handles large amounts of OFFICIAL information. The security of this information is of paramount importance. Making sure that a clear desk policy operates across the Council can help prevent the security of this information from being breached.

The misuse of the Council’s computer and telephony resources is considered to be potential gross misconduct and may render the individual(s) concerned liable to disciplinary action including dismissal.

The purpose of this document is to establish guidelines as to what constitutes “computer and telephony resources”, what is considered to be “misuse” and how users should operate within a clear desk environment.

4. Scope

This document applies to all Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council who have access to information systems or information used for Council purposes.

This Policy should be read in conjunction with the following policies:-

Information Management and Protection Policy.

Information Security Policy.

IT Access Policy.

Email Policy.

Internet Acceptable Usage Policy.

Social Media Policy.
Software Policy (TBA).
PSN Acceptable Usage Policy and Personal Commitment Statement.
Legal Responsibilities Policy (TBA).
Removable Media Policy.
Human Resources Information Security Standards (TBA).
Information Security Incident Management Policy.
IT Infrastructure Policy.
Communications and Operation Management Policy (TBA).
Remote Working Policy.

5. Definition

This Policy should be applied whenever users who access information systems or information utilise the Council's computer and telephony resources.

Computer and telephony resources include, but are not restricted to, the following:

- Mainframe computers.
- Departmental computers.
- Personal computers.
- Portable laptop computers.
- Tablet computers
- Terminals.
- Printers.
- Network equipment.
- Telecommunications facilities, including mobile phones.
- Smartphones.

6. Risks

The Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This Policy aims to mitigate the following risks:

- The non-reporting of information security incidents.
- Inadequate destruction of data.
- The loss of direct control of user access to information systems and facilities etc.

New Risks:

- Inadvertently or intentionally downloading malware.
- Falling victim to social engineering.
- Committing or aiding fraud.
- Creating legal liabilities via illicit activity or non-compliance with regulations or copyright.
- Gaining unauthorised access to critical information.
- Leaking unauthorised access to critical information.
- Inappropriate use of social media.

- Accessing inappropriate content.
- Downloading content for personal use (cost and bandwidth issues).
- Timewasting.

Non-compliance with this Policy could have a significant effect on the reputation and the efficient operation of the Council and may result in financial loss and being unable to provide necessary services to our customers.

7. Applying the Policy

7.1 Computer Resources Misuse

No exhaustive list can be prepared defining all possible forms of misuse of computer resources. The individual circumstances of each case will need to be taken into account. However, some examples are outlined below:

- Use of computer resources for the purposes of fraud, theft or dishonesty.
- Storing/loading/executing of software for a purpose which is not work related.
- Storing/loading/executing of software which has not been acquired through approved Council procurement procedures, or for which the council does not hold a valid program licence, or which has not been the subject of formal virus checking procedures.
- Storing/processing/printing of data for a purpose which is not work related.

7.2 Telephone

The Council has a Code of Practice (see Appendix 1) relating to telephone use. This concerns the use of Council-owned static and mobile telephones for private telephone calls and must be followed at all times.

Misuse of the Council's telephone services is also considered to be potential gross misconduct and may render the individual(s) concerned liable to disciplinary action.

7.3 Clear Desk

The Council has a clear desk policy in place to make sure that all information is held securely at all times. It also supports the Council's flexible working arrangements.

Sensitive material must not be left in clear view on unattended desks.

At the end of each day, every desk must be cleared of all documents that contain any Council OFFICIAL information, or any information relating to clients or citizens.

Trays containing work should be stored in a locked cabinet or drawer overnight, and there should be nothing left on desks at the end of the working day.

Council OFFICIAL-SENSITIVE information must be stored in a facility (e.g. lockable safe or cabinet) commensurate with this classification level.

Nothing should be left lying on printers, photocopiers or fax machines at the end of the day. Consideration should be given to the location of printers which are used for overnight printing. If OFFICIAL information is printed overnight then the printer is to be located in a secure location.

Users of IT facilities are responsible for safeguarding data by making sure that equipment is not left logged-on when unattended, and that portable equipment in their custody is not exposed to opportunistic theft.

Computer screens must be locked to prevent unauthorised access when unattended. Screens must lock automatically after a 5 minute period of inactivity in order to protect information. A screen saver with password protection enabled must be installed on all PCs and laptops. Attempts to tamper with this security feature will be investigated and could lead to disciplinary action.

Floor space under furniture and around the office should remain free from obstructions at all times to facilitate the cleaning and maintenance of the building.

Checks of each area will be made regularly by team managers and any items that are found on the floor (apart from footrests and bins) will be removed.

As part of good housekeeping, boxes, folders etc. should not be stored on top of furniture, cabinets, window ledges etc.

The clear desk policy is not intended to hinder your day to day working. In an ideal world, we would all work with a clear desk.

7.4 Legislation

Users should understand the relevant legislation relating to Information Security and Data Protection, and should be aware of their responsibilities under this legislation. The following statutory legislation governs aspects of the Council's information security arrangements. This list is not exhaustive:

- The Computer Misuse Act 1990.
- The Official Secrets Act 1989.
- The Data Protection Act 1998.
- The Freedom of Information Act 2000.
- The Environmental Information Regulations 2004.
- The Human Rights Act 1998.
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (amended in 2004, 2011, 2015, and 2016)
- The Electronic Communications Act 2000.
- The Regulation of Investigatory Powers Act 2000.
- The Copyright Designs and Patents Act 1988.
- The Re-use of Public Sector Information Regulations 2015.

Individuals can be held personally and legally responsible for breaching the provisions of the above Acts.

8. Policy Compliance

If any user is found to have breached this Policy, they will be subject to the Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from People and Organisational Development.

9. Review and Revision

This Policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by ICT Team Leader supported by the Corporate Information Governance Group.

10. References

The following Council Policy documents are directly relevant to this Policy, and are referenced within this document:

- IT Access Policy

The following Council Policy documents are indirectly relevant to this Policy:

- Information Management and Protection Policy.
- Information Security Policy.
- Email Policy.
- Internet Acceptable Usage Policy.
- Social Media Policy.
- Software Policy (TBA).
- Public Service Network Acceptable Usage Policy and Personal Commitment Statement.
- Legal Responsibilities Policy (TBA).
- Removable Media Policy.
- Human Resources Information Security Standards (TBA).
- Information Security Incident Management Policy.
- IT Infrastructure Policy.
- Communications and Operation Management Policy (TBA).
- Remote Working Policy.

Appendix 1 – Code of Practice Relating to Private Telephone Calls

This Code of Practice applies to the use of Council-owned static and mobile telephones for private telephone calls.

Whenever possible, private calls should be made on an employee's personal device. However, the Council acknowledges that employees may occasionally need to make calls of a personal nature using a Council-owned device whilst at work. This Code of Practice outlines reasonable steps that all employees are expected to take to make sure that the provision of service is not compromised and there is no financial loss.

Where possible, private calls should be made outside standard hours of service provision, i.e. before 9pm, after 5pm, or during an employee's lunch break.

Private calls during these hours should be kept to a minimum, so as not to prevent business calls getting through.

Each employee should keep a record of the private calls they make. The Council may carry out monitoring to ensure private use is not excessive.

There may be times when unforeseen working commitments may require the rearranging of personal engagements. The Council recognises that such calls are necessary in order for employees to effectively perform their duties, and should not be treated as private. However, the Council stresses that such calls are normally exceptional, and expect employees to recognise when such calls are required.

Email Policy

Document Control

Organisation	West Lindsey District Council
Title	Email Policy
Author	S M Anderson
Filename	
Owner	
Subject	IT Policy
Protective Marking	OFFICIAL
Review date	

Revision History

Revision Date	Revised By	Previous Version	Description of Revision
20/1/2011	Steve Anderson	Draft V0.1	Para 6 and 11 amended to reflect that use of WLDC email address for all WLDC business is recommended rather than mandated.
3/2/2011	Steve Anderson	Draft V0.2	Plain English guidelines applied.
7/4/2011	Steve Anderson	Draft V0.3	Adopted by O&R Committee
6/2/2014	Steve Anderson	Version 1.0	Amended to reflect new organisation structure. Minor corrections and updates.
3/6/2014	Steve Anderson	Version 1.1	Reviewed by Corporate Information Governance Group. Minor corrections and reorganisation of the document. Approved by CMT.
27/6/2016	Steve Anderson	Version 2.0	Revised to include latest Government Classification Scheme, updated roles and responsibilities and minor typographical amendments.

Contents

Contents	3
1. Policy Statement	4
2. Purpose	4
3. Key Messages	4
4. Scope	4
5. Risks	5
6. Applying the Policy	5
6.1 Email as Records	5
6.2 Email as a Form of Communication	6
6.3 Junk Mail	8
6.4 Mail Box Size	8
6.5 Monitoring of Email Usage	8
6.6 Classification of Messages	9
6.7 Security	11
6.8 Confidentiality	11
6.9 Negligent Virus Transmission	12
7. Policy Compliance	12
8. Policy Governance	12
9. Review and Revision	13
10. References	13

1. Policy Statement

West Lindsey District Council will make sure all users are aware of the acceptable use of Council email facilities using a variety of training methods during on-boarding, the induction process, and throughout their employment or term of office.

2. Purpose

The aim of this Policy is to direct all users of Council email facilities by:

- providing guidance on expected working practice;
- highlighting issues affecting the use of email;
- informing users about the acceptable use of ICT facilities in relation to emails;
- describing the standards that users must maintain;
- stating the actions that may be taken to monitor the effectiveness of this Policy; and
- warning users about the consequences of inappropriate use of the email service.

The Policy establishes a framework within which users of Council email facilities can apply self-regulation to their use of email as a communication and recording tool.

3. Key Messages

- All emails that are used to conduct or support official Council business should be sent using a “@west-lindsey.gov.uk” address.
- All emails sent via the Government Connect Secure Extranet (GCSx) must be sent using a “@west-lindsey.gcsx.gov.uk” address.
- Non-work email accounts **should not** be used to conduct or support official Council business.
- Councillors and users must make sure that any emails containing sensitive information are sent from an official Council email address.
- All official external e-mail must carry the official Council disclaimer (see section 7.1).
- Under no circumstances should users email material (either internally or externally), which is defamatory, obscene, or does not comply with the Council’s Equal Opportunities policy.
- Where GCSx email is available to connect the sender and receiver of the email message, this **must be used** for all external email use and must be used for communicating OFFICIAL-SENSITIVE, confidential or material containing person identifiable information (PII).
- Automatic forwarding of email must be considered carefully to prevent OFFICIAL-SENSITIVE, confidential or material containing person identifiable information (PII) material being forwarded inappropriately.

4. Scope

This Policy covers all email systems and facilities that are provided by the Council for conducting and supporting official business activity through the Council’s network infrastructure and all stand alone and portable computer devices.

This Policy applies to all councillors, committees, departments, partners, employees of the Council, contractual third parties, and agents of the Council who have been designated as authorised users of corporate email facilities.

The use of email facilities will be permitted only to staff that have been specifically designated as authorised users for that purpose, received proper training and have confirmed in writing that they accept and agree to abide by the terms of this Policy.

The Policy also applies where appropriate to the internal Microsoft exchange e-mail facility which may be accessed by staff who are not authorised Internet and external e-mail users.

The use of Council email facilities by staff who have not been authorised for that purpose will be regarded as a disciplinary offence.

All email prepared and sent from West Lindsey District Council email addresses or mailboxes, and any non-work email sent using Council Information and Communication Technology (ICT) facilities is subject to this Policy.

5. Risks

The Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This Policy aims to mitigate the following risk:

Non-compliance with this Policy could have a significant effect on the efficient operation of the Council and may result in financial loss or reputation and an inability to provide necessary services to our customers.

6. Applying the Policy

6.1 Email as Records

All emails that are used to conduct or support official Council business **should** be sent using a “@west-lindsey.gov.uk” address. All emails sent over the Public Service Network (PSN) via the Government Connect Secure Extranet (GCSx) secure email service **must** be of the format “@west-lindsey.gcsx.gov.uk”.

Non-work email accounts **should not** be used to conduct or support official Council business. However, councillors and users **must** make sure that any emails containing **sensitive** information are sent from an official Council email address. Also, any emails containing OFFICIAL-SENSITIVE or material containing person identifiable information (PII) **must** be sent from a GCSx email address or other Council-approved secure email service (please also refer to section 7.7). All emails that represent aspects of Council business or Council administrative arrangements are the property of the Council and not of any individual employee.

Emails held on Council equipment are considered to be part of the corporate record and email also gives a record of staff activities.

The legal status of an email message is similar to any other form of written communication. So any e-mail message sent from a facility provided to conduct or support official Council business should be considered to be an official communication from the Council. To make sure that the Council is adequately protected from misuse of e-mail, the following controls will be exercised.

- It is a condition of acceptance of this Policy that users comply with the instructions given during the email training sessions.
- All official external e-mail sent via the Internet must carry the following disclaimer:

“This e-mail message has been scanned for Viruses and Content.

**** DISCLAIMER **** The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination or other use, or taking of any action in reliance upon this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from your computer. Any correspondence with the sender will be subject to automatic monitoring.”*

- All email sent via the Government Connect Secure Extranet (GCSx) must carry the following disclaimer:

“This transmission is intended for the named addressee(s) only and may contain sensitive or protectively marked material up to OFFICIAL-SENSITIVE and should be handled accordingly. Unless you are the named addressee (or authorised to receive it for the addressee) you may not copy or use it, or disclose it to anyone else. If you have received this transmission in error please notify the sender immediately. All GCSX traffic may be subject to recording and/or monitoring in accordance with relevant legislation.”

Users should be aware that deletion of e-mail from individual accounts does not necessarily result in permanent deletion from the council’s ICT systems.

Emails and attachments can be an important part of the Council’s corporate record and users should note that they may need to be disclosed under the Data Protection Act 1998 or the Freedom of Information Act 2000. Consequently, the email system should not be used to permanently store corporate records. Emails that can be classed as a record should be properly copied out and filed in the relevant corporate system.

Further information about this can be obtained from the Data Protection Officer, Team Manager, People and Organisational Development, Team Manager Customer Strategy and Services, or the Information Governance Officer.

6.2 Email as a Form of Communication

Email is designed to be an open and transparent method of communicating. However, it cannot be guaranteed that the message will be received or read, or that the content will be understood in the way that the sender of the email intended. The person sending an email is responsible for deciding whether email is the most suitable method for conveying time

critical; OFFICIAL-SENSITIVE, confidential or material containing person identifiable information (PII); or for communicating in particular circumstances.

All emails sent to conduct or support official Council business must comply with corporate communications standards. Refer to West Lindsey's Emailogic Reference Manual (available on the Council Intranet) for the standards which must be applied to email communications.

Councillors **should** make sure that any emails containing sensitive information are sent from an official Council email. Any emails containing OFFICIAL-SENSITIVE, or material containing person identifiable information (PII) **must** be sent from a GCSx email address or other Council-approved secure email service.

Email must not be considered to be any less formal than memo's or letters that are sent out from a particular service or the Council. An email could also be construed as a contract or legally-binding agreement. When sending external email, care should be taken not to contain any material which would reflect poorly on the Council's reputation or its relationship with customers, clients or business partners.

Under no circumstances should users email material (either internally or externally), which is, for example, defamatory, obscene, or does not comply with the Council's Equal Opportunities Policy, or which could reasonably be expected to be considered inappropriate. Any user who is not clear about whether material is appropriate should consult their team manager before starting any associated activity or process.

ICT facilities provided by the Council for email should not be used for:

- sending unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organisations;
- the unauthorised sending to a third party of OFFICIAL-SENSITIVE, confidential or material containing person identifiable information (PII) material concerning the activities of the Council;
- sending material that infringes the copyright of another person, including intellectual property rights;
- activities that unreasonably waste staff effort or use network resources, or activities that unreasonably serve to deny the service to other users;
- activities that corrupt or destroy other users' data;
- activities that disrupt the work of other users;
- the creation or sending of any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material;
- the creation or sending of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;
- the creation or sending of material that is abusive or threatening to others, or serves to harass or bully others;
- the creation or sending of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs;
- the creation or sending of defamatory material;

- the creation or sending of material that includes false claims of a deceptive nature;
- so-called 'flaming' - ie the use of impolite terms or language, including offensive or condescending terms;
- activities that violate the privacy of other users;
- unfairly criticising individuals, including copy distribution to other individuals;
- publishing to others the text of messages written on a one-to-one basis, without the prior express consent of the author;
- the creation or sending of anonymous messages - ie without clear identification of the sender; or
- the creation or sending of material which brings the Council into disrepute.

6.3 Junk Mail

There may be times where a user will receive unsolicited mass junk email or spam. Users are advised to delete such messages without reading them. Do not reply to or forward the email. Even trying to remove the email address from the distribution list can confirm the existence of the address following a speculative e-mail.

Before giving your e-mail address to a third party, such as a website, consider carefully the possible consequences of that address being passed (possibly sold on) to an unknown third party, and whether the potential problems which may result outweigh the benefits.

Chain letter e-mails (those that ask you to forward the message to one or more extra recipients who are unknown to the original sender) **must not** be forwarded using Council systems or facilities.

6.4 Mail Box Size

To make sure that the email system is available and performing well, users should avoid sending unnecessary messages. In particular, the use of the "global list" of e-mail addressees is discouraged.

The Council will impose limits, when necessary, to reduce problems associated with server capacity. Email users should manage their email accounts to stay within these limits and make sure that items are filed or deleted as appropriate to avoid any deterioration in systems and to comply with the Records Management Policy.

Email messages can be used to carry other files or messages either embedded in the message or attached to the message. If it is necessary to provide a file to another person, then a reference to where the file exists should be sent rather than a copy of the file. This is to avoid excessive use of the system and avoids filling to capacity another person's mailbox. If a copy of a file must be sent then it should not exceed (3 MB) in size.

6.5 Monitoring of Email Usage

All users should be aware that email usage is logged and recorded centrally. The monitoring of email (outgoing and incoming) traffic can be undertaken to enable the Council to:

- plan and manage its resources effectively;
- make sure that users act only in accordance with policies and procedures;

- make sure that standards are maintained;
- prevent and detect any crime; and
- investigate any unauthorised use.

Monitoring of content will only be carried out by staff specifically authorised for that purpose. These arrangements will be applied to all users and may include checking the contents of email messages for:

- establishing the existence of facts relevant to the business, client, supplier and related matters;
- ascertaining or demonstrating standards which ought to be achieved by those using the facilities;
- preventing or detecting crime;
- investigating or detecting unauthorised use of email facilities;
- ensuring effective operation of email facilities; and
- determining if communications are relevant to the business.

Where a manager suspects that the email facilities are being abused by a user, they should contact the Team Manager, People and Organisational or ICT Team Leader. Designated staff in ICT can investigate and provide evidence and audit trails of access to systems. ICT will also comply with any legitimate requests from authorised bodies under the Regulation of Investigatory Powers legislation for this information.

Access to another employee's email (other than that by specifically authorised staff) is strictly forbidden unless the employee has given their consent, or their email needs to be accessed and the Team Manager, People and Organisational Development has given authorisation for specific work purposes whilst they are absent. If this is the case, a written request to the People and Organisational Development team from the employee's team manager is required. Accessing another employee's email must be absolutely necessary and must be carried out with regard to the rights and freedoms of the employee.

6.6 Classification of Messages

When creating an email, the information contained within it must be assessed and classified by the owner according to the content, when appropriate. It is advisable that all emails are protectively marked in accordance with the Government Classification Scheme. The marking classification will indicate how the email, and the information contained within it, should be protected and who should be allowed access to it.

The Government Classification Scheme is set out in the Information Management and Protection Policy and has 4 principles:

Principle One: ALL information that HMG needs to collect, store, process, generate or share to deliver services and conduct government business has intrinsic value and requires an appropriate degree of protection.

Principle Two: EVERYONE who works with government (including staff, contractors and service providers) has a duty of confidentiality and a responsibility to safeguard any HMG information or data that they access, irrespective of whether it is marked or not, and must be provided with appropriate training.

Principle Three: Access to sensitive information must ONLY be granted on the basis of a genuine “need to know” and an appropriate personnel security control.

Principle Four: Assets received from or exchanged with external partners MUST be protected in accordance with any relevant legislative or regulatory requirements, including any international agreements and obligations.

The Scheme requires that all information to be protectively marked using one of 3 classifications. The way the document is handled, published, moved and stored will depend on this scheme.

The classifications are:

- OFFICIAL
- SECRET (not relevant to local government)
- TOP SECRET (not relevant to local government)

ALL routine public sector business, operations and services should be treated as OFFICIAL - many departments and agencies will operate exclusively at this level. This includes a wide range of information, of differing value and sensitivity, which needs to be defended against the threat profile described below, and to comply with legal, regulatory and international obligations. This includes:

- The day to day business of government, service delivery and public finances.
- Routine international relations and diplomatic activities.
- Public safety, criminal justice and enforcement activities.
- Many aspects of defence, security and resilience.
- Commercial interests, including information provided in confidence and intellectual property.
- Personal information that is required to be protected under the Data Protection Act (1998) or other legislation (e.g. benefits records).

The typical threat profile for the OFFICIAL classification is broadly similar to that faced by a large UK private company with valuable information and services. It anticipates the need to defend UK Government data or services against compromise by attackers with bounded capabilities and resources. This may include (but is not limited to) hactivists, single-issue pressure groups, investigative journalists, competent individual hackers and the majority of criminal individuals and groups.

Baseline Security Outcomes:

- ALL Her Majesty’s Government (HMG) information must be handled with care to prevent loss or inappropriate access, and deter deliberate compromise or opportunist attack.
- Staff must be trained to understand that they are personally responsible for securely handling any information that is entrusted to them in line with local business processes.
- Baseline security controls reflect commercial good practice.

Protective Markings:

There is no requirement to explicitly mark routine OFFICIAL information. Baseline security measures should be enforced through local business processes.

A limited subset of OFFICIAL information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the “OFFICIAL” classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the “need to know”. In such cases where there is a clear and justifiable requirement to reinforce the “need to know”, assets should be conspicuously marked: ‘OFFICIAL–SENSITIVE’.

Information up to OFFICIAL-SENSITIVE can be sent via GCSx and must be marked appropriately using guidance above.

6.7 Security

Emails sent between west-lindsey.gov.uk addresses are held within the same network and are deemed to be secure. However, emails sent outside this closed network travel over the public communications network and are liable to interception or loss. There is a risk that copies of the email are left within the public communications system. Therefore, OFFICIAL-SENSITIVE, or material containing person identifiable information (PII) must not be sent via email outside a closed network, unless via the GCSx email or it is encrypted using an approved encryption method.

Where GCSx email is available to connect the sender and receiver of the email message, this **must be used** for all external email use and must be used for communicating OFFICIAL-SENSITIVE, or material containing person identifiable information (PII).

All Council employees that require access to GCSx email are required to read, understand and sign the Public Service Network Acceptable Usage Policy and Personal Commitment Statement.

6.8 Confidentiality

All staff are under a general requirement to maintain the confidentiality of information. There are also particular responsibilities under Data Protection legislation to maintain the confidentiality of personal data. If any member of staff is unsure of whether they should pass on information, they should talk to the Data Protection Officer or their manager.

Staff must make every effort to make sure that the confidentiality of email is properly maintained. Staff should be aware that a message is not deleted from the system until all recipients of the message and of any forwarded or attached copies have deleted their copies. Also, confidentiality cannot be assured when messages are sent over outside networks, such as the Internet, because of the insecure nature of most of these networks and the number of people to whom the messages can be freely circulated without the knowledge of the Council.

Care should be taken when addressing all emails, but particularly where they include OFFICIAL-SENSITIVE, or material containing person identifiable information (PII), to prevent accidental transmission to unintended recipients. Particular care should be taken if

the email client software auto-completes an email address as the user begins typing a name.

Automatic forwarding of email (for example when the intended recipient is on leave) must be considered carefully to prevent OFFICIAL-SENSITIVE, or material containing person identifiable information (PII) being forwarded inappropriately. Rules can be implemented to include or exclude certain mail based on the sender or subject. If you need help with this, please contact ICT in the first instance.

The automatic forwarding of a GCSx email to a lower classification email address (i.e. a standard .gov.uk email) contradicts national guidelines and is therefore not acceptable.

6.9 Negligent Virus Transmission

Computer viruses are easily transmitted via email and internet downloads. Full use must therefore be made of the council's anti-virus software. If any user has concerns about possible virus transmission, they must report the concern to ICT Team on Ext. 165.

In particular, users must:

- not send by email any file attachments which they know to be infected with a virus;
- not download data or programs of any nature from unknown sources;
- make sure that an effective anti-virus system is operating on any computer which they use to access council facilities;
- not forward virus warnings other than to the ICT Team; and
- report any suspected files to the ICT Team.

The Council will make sure that email is virus checked at the network boundary and at the host, and where appropriate will use two functionally independent virus checkers.

If a computer virus is sent to another organisation, the Council could be held liable if there has been negligence in allowing the virus to be sent. Users must therefore comply with all information security policies and guidance.

7. Policy Compliance

If any user is found to have breached this Policy, they may be subject to the Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this Policy or how it may apply to you, seek advice from People and Organisational Development team.

8. Policy Governance

The following table identifies who within the council is Accountable, Responsible, Informed or Consulted with regards to this Policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.

- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Corporate Information Governance Group (CIGG), Information Governance Officer (IGO)
Accountable	Section 151 Officer (Senior Information Risk Owner (SIRO))
Consulted	JSCC, EOWG
Informed	Councillors, committees, departments, partners, employees of the council, contractual third parties and agents of the council

9. Review and Revision

This Policy will be reviewed as it is deemed appropriate, but no less frequently than every 24 months.

The policy review will be undertaken by Corporate Information Governance Group (CIGG).

10. References

The following West Lindsey District Council policy documents are directly relevant to this Policy, and are referenced within this document:

- Equal Opportunity Policy
- Information Management and Protection Policy
- Public Service Network Acceptable Usage Policy and Personal Commitment Statement.
- Information Security Policy
- Emailogic Reference Manual
- Records Management Policy

The following West Lindsey District Council policy documents are indirectly relevant to this Policy:

- IT Access Policy
- Internet Acceptable Usage Policy.
- Legal Responsibilities Policy.
- Computer, Telephone and Desk Use Policy.
- Removable Media Policy.
- Information Security Incident Management Policy.
- IT Infrastructure Policy.

Email Policy for ActiveSync Users

Document Control

Organisation	West Lindsey District Council
Title	Email Policy For Users Of Mobile Devices Equipped With Microsoft Exchange ActiveSync
Author	S M Anderson
Filename	
Owner	
Subject	IT Policy
Protective Marking	
Review date	

Revision History

Revision Date	Revised By	Previous Version	Description of Revision

Contents

1	Policy Statement.....	4
2	Key Messages	4
3	Purpose	4
4	Scope	5
5	Definition.....	5
6	Risks.....	5
7	Applying the Policy	5
	7.1 Email as Records.....	5
	7.2 Email as a Form of Communication	6
	7.3 Junk Mail	7
	7.4 Mail Box Size	8
	7.5 Monitoring of Email Usage	8
	7.6 Classification of Messages	9
	7.7 Security	9
	7.8 Confidentiality.....	9
	7.9 Negligent Virus Transmission.....	10
8	Policy Compliance	10
9	Review and Revision	10
10	References.....	10
11	Signatures.....	12
	11.1 Personal Commitment Statement.....	12

1 Policy Statement

West Lindsey District Council (“the Council”) will make sure that all users are aware of the acceptable use of Council email facilities.

2 Key Messages

- Access to the Council’s Microsoft Exchange ActiveSync allows users of mobile devices such as iPad, iPhone, Android, Windows phone, to synchronise their West Lindsey District Council mailbox to their device. The service is not compatible Notebooks and PCs running Microsoft Windows.
- The Microsoft Exchange ActiveSync service is provided to users on the understanding that each user is responsible for paying the data costs associated with synchronising their Council mailbox over the mobile network.
- All users must agree to allow their device to be remotely secured and managed. Passwords will be required to meet the Council’s password policy for complexity and frequency of change.
- The Council strongly recommends that all emails used to conduct or support official Council business should be sent using a “@west-lindsey.gov.uk” address.
- Non-work email accounts **should not** be used to conduct or support official Council business.
- Users must make sure that any emails containing personal, sensitive personal, or confidential information, are sent from an official Council email address.
- All official external e-mail must carry the official Council disclaimer (see section 7.1).
- Under no circumstances should the Council’s email service be used to email material (either internally or externally), which is defamatory, obscene, or does not comply with the Council’s Equal Opportunities policy.
- Automatic forwarding of email to other email accounts must be considered carefully to prevent sensitive or confidential material being forwarded inappropriately.

3 Purpose

The aim of this Policy is to direct all users using Council email facilities by:

- providing guidance on expected working practice;
- highlighting issues affecting the use of email;
- informing users about the acceptable use of ICT facilities in relation to emails;
- describing the standards that users must maintain;
- stating the actions that may be taken to monitor the effectiveness of this Policy; and
- warning users about the consequences of inappropriate use of the email service.

The Policy establishes a framework within which users of Council email facilities can apply self-regulation to their use of email as a communication and recording tool.

4 Scope

This Policy covers all email systems and facilities that are provided by the Council for conducting and supporting official business activity through the Council's network infrastructure and all stand alone and portable computer devices.

The Policy applies to all users who have been authorised to use the Council's Microsoft Exchange ActiveSync service.

Use of the Council's Microsoft Exchange ActiveSync service will be permitted only to those who have been specifically designated as authorised users for that purpose, received proper training, and have confirmed in writing that they accept and agree to abide by the terms of this Policy.

5 Definition

All email prepared and sent from West Lindsey District Council email addresses or mailboxes, and any non-work email sent using Council Information and Communication Technology (ICT) facilities is subject to this Policy.

6 Risks

The Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This Policy aims to mitigate the following risk:

Non-compliance with this Policy could have a significant effect on the efficient operation of the Council and may result in financial loss or reputation and an inability to provide necessary services to our customers.

7 Applying the Policy

7.1 Email as Records

All emails that are used to conduct or support official Council business **should** be sent using a "@west-lindsey.gov.uk" address.

Non-work email accounts **should not** be used to conduct or support official Council business. However, users **must** make sure that any emails containing **sensitive** information are sent from an official Council email address. Also, any emails containing OFFICIAL-SENSITIVE information **must** be sent from a GCSx email address or other government-approved secure email service (please also refer to section 7.7). All emails that represent aspects of Council business or Council administrative arrangements are the property of the Council and not of any individual.

Emails held on Council equipment are considered to be part of the corporate record and email also gives a record of users' activities.

The legal status of an email message is similar to any other form of written communication. So any e-mail message sent from a facility provided to conduct or support official Council business should be considered to be an official communication from the Council. To make sure that the Council is adequately protected from misuse of e-mail, the following controls will be exercised.

It is a condition of acceptance of this Policy that users comply with the instructions given during the email training sessions.

All official external e-mail sent via the Internet must carry the following disclaimer:

“This e-mail message has been scanned for Viruses and Content.

**** DISCLAIMER *** The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination or other use, or taking of any action in reliance upon this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from your computer. Any correspondence with the sender will be subject to automatic monitoring.”*

Users should be aware that deletion of e-mail from individual accounts does not necessarily result in permanent deletion from the council’s ICT systems.

Users should also note that email and attachments may need to be disclosed under the Data Protection Act 1998 or the Freedom of Information Act 2000. Further information about this can be obtained from the Data Protection Officer or the Team Manager, People and Organisational Development.

7.2 Email as a Form of Communication

Email is designed to be an open and transparent method of communicating. However, it cannot be guaranteed that the message will be received or read, or that the content will be understood in the way that the sender of the email intended. The person sending an email is responsible for deciding whether email is the most suitable method for conveying time critical; sensitive or confidential information; or for communicating in particular circumstances.

Users **must** make sure that any emails containing sensitive information relating to Council business are sent from an official Council email. Any emails containing OFFICIAL-SENSITIVE information **must** be sent from a GCSx email address or other government-approved secure email service.

Email must not be considered to be any less formal than memo’s or letters that are sent out from a particular service or the Council. When sending external email, care should be taken not to contain any material which would reflect poorly on the Council’s reputation or its relationship with customers, clients or business partners.

Under no circumstances should users email material (either internally or externally), which is, for example, defamatory, obscene, or does not comply with the Council’s Equal Opportunities Policy, or which could reasonably be expected to be considered

inappropriate. Any user who is not clear about whether material is appropriate should consult their team manager before starting any associated activity or process.

ICT facilities provided by the Council for email should not be used for:

- sending unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organisations;
- the unauthorised sending to a third party of sensitive or confidential material concerning the activities of the Council;
- sending material that infringes the copyright of another person, including intellectual property rights;
- activities that unreasonably waste staff effort or use network resources, or activities that unreasonably serve to deny the service to other users;
- activities that corrupt or destroy other users' data;
- activities that disrupt the work of other users;
- the creation or sending of any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material;
- the creation or sending of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;
- the creation or sending of material that is abusive or threatening to others, or serves to harass or bully others;
- the creation or sending of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs;
- the creation or sending of defamatory material;
- the creation or sending of material that includes false claims of a deceptive nature;
- so-called 'flaming' - ie the use of impolite terms or language, including offensive or condescending terms;
- activities that violate the privacy of other users;
- unfairly criticising individuals, including copy distribution to other individuals;
- publishing to others the text of messages written on a one-to-one basis, without the prior express consent of the author;
- the creation or sending of anonymous messages - ie without clear identification of the sender; or
- the creation or sending of material which brings the Council into disrepute.

7.3 Junk Mail

There may be times where a user will receive unsolicited mass junk email or spam. Users are advised to delete such messages without reading them. Do not reply to or forward the email. Even trying to remove the email address from the distribution list can confirm the existence of the address following a speculative e-mail.

Before giving your e-mail address to a third party, such as a website, consider carefully the possible consequences of that address being passed (possibly sold on) to an unknown third party, and whether the benefits outweigh the potential problems.

Chain letter e-mails (those that ask you to forward the message to one or more extra recipients who are unknown to the original sender) **must not** be forwarded using Council systems or facilities.

7.4 Mail Box Size

To make sure that the email system is available and performing well, users should avoid sending unnecessary messages. In particular, the use of the “global list” of e-mail addresses is discouraged.

Users are provided with a limited mail box size (50,000KB), to reduce problems associated with server capacity. Email users should manage their email accounts to stay within the limit and make sure that items are filed or deleted as appropriate to avoid any deterioration in systems.

Email messages can be used to carry other files or messages either embedded in the message or attached to the message. If it is necessary to provide a file to another person, then a reference to where the file exists should be sent rather than a copy of the file. This is to avoid excessive use of the system and avoids filling to capacity another person’s mailbox. If a copy of a file must be sent then it should not exceed (3 MB) in size.

7.5 Monitoring of Email Usage

All users should be aware that email usage is monitored and recorded centrally. The monitoring of email (outgoing and incoming) traffic is undertaken so that the Council can:

- plan and manage its resources effectively;
- make sure that users act only in accordance with policies and procedures;
- make sure that standards are maintained;
- prevent and detect any crime; and
- investigate any unauthorised use.

Monitoring of content will only be carried out by staff specifically authorised for that purpose in accordance with Communications and Operation Management Policy (TBA). These arrangements will be applied to all users and may include checking the contents of email messages for:

- establishing the existence of facts relevant to the business, client, supplier and related matters;
- ascertaining or demonstrating standards which ought to be achieved by those using the facilities;
- preventing or detecting crime;
- investigating or detecting unauthorised use of email facilities;
- ensuring effective operation of email facilities; and
- determining if communications are relevant to the business.

Where it is suspected that the email facilities are being abused, users should contact the ICT Manager or ICT Team Leader. Designated staff in ICT can investigate and provide evidence and audit trails of access to systems. ICT will also comply with any legitimate

requests from authorised bodies under the Regulation of Investigatory Powers legislation for this information.

Access to another users email (other than that by specifically authorised staff) is strictly forbidden unless the user has given their consent, or their email needs to be accessed and the Director of Resources or Team Manager, People and Organisational Development has given authorisation for specific work purposes whilst they are absent. If this is the case, a written request to People and Organisational Development is required. This must be absolutely necessary and has to be carried out with regard to the rights and freedoms of the individual.

7.6 Classification of Messages

When creating an email, the information contained within it must be assessed and classified by the owner according to the content, when appropriate. It is advisable that all emails are protectively marked in accordance with the Council's Protective Marking Policy (see the Information Management and Protection Policy). The marking classification will decide how the email, and the information contained within it, should be protected and who should be allowed access to it.

7.7 Security

Emails sent between west-lindsey.gov.uk addresses are held within the same network and are deemed to be secure. However, emails sent outside this closed network travel over the public communications network and are liable to interception or loss. There is a risk that copies of the email are left within the public communications system. Therefore, OFFICIAL-SENSITIVE material must not be sent via email outside a closed network, unless via the GCSx or other government-approved secure email service.

7.8 Confidentiality

All elected members and staff are under a general requirement to maintain the confidentiality of information. There are also particular responsibilities under Data Protection legislation to maintain the confidentiality of personal data. If a user is unsure whether they should pass on information, they should seek advice.

Users must make every effort to make sure that the confidentiality of email is properly maintained. Users should be aware that a message is not deleted from the system until all recipients of the message and of any forwarded or attached copies have deleted their copies. Also, confidentiality cannot be assured when messages are sent over outside networks, such as the Internet, because of the insecure nature of most of these networks and the number of people to whom the messages can be freely circulated without the knowledge of the Council.

Care should be taken when addressing all emails, but particularly where they include sensitive information, to prevent accidental transmission to unintended recipients. Particular care should be taken if the email client software auto-completes an email address as the user begins typing a name.

Automatic forwarding of email (for example when the intended recipient is on leave) must be considered carefully to prevent sensitive material being forwarded inappropriately. Rules can be implemented to include or exclude certain mail based on the sender or subject. If you need help with this, please contact ICT in the first instance.

7.9 Negligent Virus Transmission

Computer viruses are easily transmitted via email and internet downloads. Full use must therefore be made of anti-virus software where possible. If a user has concerns about possible virus transmission, they must report the concern to ICT Team.

In particular, users must:

- not send by email any file attachments which they know to be infected with a virus;
- not download data or programs of any nature from unknown sources;
- make sure that, where possible, an effective anti-virus system is operating on any device which they use to access Council email;
- not forward virus warnings other than to the ICT Team on request; and
- must report any suspected files to the ICT Team.

The Council will make sure that email is virus checked at the network boundary and at the host, and where appropriate will use two functionally independent virus checkers.

If a computer virus is sent to another organisation, the Council could be held liable if there has been negligence in allowing the virus to be sent.

8 Policy Compliance

If any user is found to have breached this Policy, they may be subject to the Council's relevant disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the ICT Department or the Information Governance Officer.

9 Review and Revision

This Policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

The policy review will be undertaken by the Corporate Information Governance Group (CIGG).

10 References

The following West Lindsey District Council policy documents are directly relevant to this Policy, and are referenced within this document:

- Communications and Operation Management Policy (TBA)

- Equal Opportunity Policy
- Information Management and Protection Policy
- PSN Acceptable Usage Policy and Personal Commitment Statement.
- Emailogic Reference Manual
- Bring Your Own Device Policy

The following West Lindsey District Council policy documents are indirectly relevant to this Policy:

- IT Access Policy
- Internet Acceptable Usage Policy.
- Legal Responsibilities Policy.
- Computer, Telephone and Desk Use Policy.
- Removable Media Policy.
- Human Resources Information Security Standards.
- Information Security Incident Management Policy.
- IT Infrastructure Policy.

11 Signatures

Name of User:	
Position:	
Department:	
Access Request Approved by: (Line Manager)	
Access Request Approved by: (People and Organisational Development)	
Username Allocated (IT Department)	
Email Address Allocated: (IT Department)	@west-lindsey.gov.uk
User Access Request Processed: (IT Department)	

11.1 Personal Commitment Statement

I,, accept that I have been granted access to my West Lindsey mailbox from a mobile device. I understand and accept the rights that have been granted, I understand the business reasons for these access rights, and I understand that breach of them, and specifically any attempt to access services or assets that I am not authorised to access, may lead to disciplinary action and specific sanctions. I also accept and will abide by this Policy, that I will be responsible for all costs associated with the operation of my mobile device, and that I will permit my device to be remotely managed and secured by the West Lindsey District Council IT Department. I understand that failure to comply with this agreement, or the commission of any information security breaches, may lead to withdrawal of this service and the invocation of the Council’s disciplinary policy.

Signature of User:

Dated

A copy of this agreement is to be retained by the User and the People and Organisational Development Team Manager.

Information Security Incident Management Policy

Document Control

Organisation	West Lindsey District Council
Title	Information Security Incident Management Policy and Procedure
Author	Steve Anderson
Owner	
Subject	IT Policy
Protective Marking	OFFICIAL
Review date	

Revision History

Revision Date	Revisor	Previous Version	Description of Revision
1 Apr 2009	S M Anderson	Draft 0.1	Issued
2 Nov 2010	S M Anderson	Draft 1.0	Minor amendments following review by ICT.
13 Jan 2011	S M Anderson	Draft 1.1	Issued
27 Jun 2013	S M Anderson	1.0	Process diagram amended to include reporting to EMWARP, named persons updated, risks reworded.
23/6/2014	S M Anderson	2.0	Reviewed by Corporate Information Governance Group. Minor document reorganisation. Approved by CMT.
23/6/2016	S M Anderson	2.1	Document reorganised to the latest policy template standard and revised to include separate procedures for ICT Incidents and IG Incidents.

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Director of Resources (SIRO)	Ian Knowles	

1. Overview.....	4
2. Purpose	4
3. Scope	4
4. Policy	4
a. Procedures for Incident Handling.....	5
5. Policy Compliance	5
a. Compliance Measurement	6
b. Non-Compliance	6
6. Related Standards, Policies and Processes	6
7. Definitions and Terms.....	7
Appendix 1 – Examples of Information Security Incidents	8
ICT Incidents	8
Information Governance Incidents	8
Appendix 2 – Information Governance Incident Management Process	9
1. Reporting an Incident.....	9
2. Escalation Criteria	10
3. Data Breach Reporting.....	10
4. Roles and Responsibilities	10
5. Learning from Information Security Incidents	11
Appendix 3 - Information Governance Incident Management Process Flow.....	12

HOW TO REPORT AN INFORMATION SECURITY INCIDENT

Please report any actual, suspected or potential breach of information security promptly as follows:

ICT related incidents

- Log a call on the ICT Helpdesk system
- If you don't have access to the Helpdesk system or the system is unavailable please contact the ICT Team on extension 165.

Information Governance related incidents:

- Complete an Information Governance Incident Form on Minerva (<http://minerva.sharelincs.net/pages/incident-management.aspx>)
- If Minerva is unavailable please contact a member of the Incident Response Team via the ICT Helpdesk on extension 165.

1. Overview

West Lindsey District Council (the “Council”) will make sure that it reacts appropriately to any actual or suspected security incidents or weaknesses relating to information and information systems within the custody of the Council.

2. Purpose

The purpose of this Policy is to provide management direction for meeting the above overview.

3. Scope

This document applies to all Councillors, Committees, Departments, Partners, Employees of the Council, Tenants, contractual third parties and agents of the Council who use West Lindsey District Council’s IT facilities and equipment, or have access to, or custody of, customer information or West Lindsey District Council information.

This Policy will be communicated to managers at a suitable Service Leadership Team (SLT) workshop and to Councillors and staff by using the Council’s Learning Platform. Managers who are responsible for managing third party contracts and agents must ensure that adherence to this Policy is specified in the relevant contract.

4. Policy

The Policy covers:

- a. The reporting and management of ICT-specific incidents such as virus infections, denials of service, hacking and ICT equipment.

- b. The reporting and management of Information Governance (IG) incidents. These are physical and human-related security incidents and weaknesses which could compromise the Confidentiality, Integrity and Availability of the Council's information.

Examples of the types of incident covered by this Policy are listed at Appendix 1. The Council has a clear incident reporting mechanism in place which details the procedures for identifying, reporting and recording security incidents. By continually communicating to Councillors, Committees, Departments, Partners, Employees of the Council, Tenants, contractual third parties and agents of the Council, the importance of recognising, reporting and managing incidents, the Council can continue to improve its information-related processes and procedures and the training and guidance it provides to users.

All Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council are required to report all incidents – including potential or suspected incidents, as soon as possible via the Council's Incident Reporting procedures outlined at Appendices 2 and 3.

a. Procedures for Incident Handling

Events and weaknesses need to be reported at the earliest possible stage as they need to be assessed by the Incident Response Team (IRT). This enables the IRT to identify when a series of events or weaknesses have escalated to become an incident. It is vital for the ICT Department to gain as much information as possible from the business users to identify if an incident is occurring. Please do not attempt to confirm any suspected ICT weaknesses. Testing weaknesses might be interpreted as a potential misuse of the system and could also cause damage to the information system or service.

i. ICT-Related Incidents

The majority of ICT-related incidents (such as malware attacks, denials of service etc.) will be identified by ICT staff during normal daily maintenance and monitoring activities. Some, such as virus alerts, suspicious emails, etc. could be identified by staff. All ICT-related incidents, however, must be logged on the ICT Helpdesk System and managed in accordance with the ICT Incident Management Process (refer to ICT Team procedures for full details).

ii. Information Governance Incidents

Most IG Incidents will be identified or observed by staff during their normal work activity

Appendix 2 details the IG Incident Management Process and sets out the requirements and method of reporting IG incidents and the roles and responsibilities for managing them.

5. Policy Compliance

All users **must** understand and use this Policy and are responsible for assuring the safety and security of the Council's systems and information that they use or manipulate.

a. Compliance Measurement

Compliance with this Policy will be measured by recording the number of incidents reported.

b. Non-Compliance

Non-compliance with this Policy could have a significant effect on the reputation and the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

If any user is found to have breached this Policy, they may be subject to the Council's disciplinary procedure. If a criminal offence is considered to have been committed action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this Policy or how it may apply to you, seek advice from your Corporate Information Governance Group (CIGG) representative, the Information Governance Officer, or the ICT Dept.

6. Related Standards, Policies and Processes

The following Council policy documents are directly relevant to this Policy:

- Data Protection Policy
- Data Protection Breach Policy
- Email Policy.
- Internet Acceptable Use Policy.
- PSN Acceptable Usage Policy and Personal Commitment Statement.
- Computer, Telephone and Desk Use Policy.
- Removable Media Policy.
- Remote Working Policy.
- IT Access Policy.
- IT Infrastructure Policy.

7. Definitions and Terms

Information Security Incident	<p>An adverse event that has caused or has the potential to cause damage to an organisation's information assets, reputation and/or personnel. Incident management is concerned with managing the effects of intrusion, compromise and misuse of information and information resources, and ensuring the continuity of critical information systems and processes.</p> <p>Examples of common information security incidents are given in Appendix 1.</p>
Information	<p>The definition of information includes, but is not confined to, paper and electronic documents and records, email, voicemail, still and moving images and sound recordings, the spoken word, data stored on computers or tapes, transmitted across networks, printed out or written on paper, carried on portable devices, sent by post, courier or fax, posted onto intranet or internet sites or communicated using social media.</p>
Confidential Information	<p>The definition of confidential information can be summarised as:</p> <ul style="list-style-type: none">▪ Any personal information that would cause damage or distress to individuals if disclosed without their consent.▪ Any other Information that would prejudice the Authority's or another party's interests if it were disclosed without authorisation.

Appendix 1 – Examples of Information Security Incidents

ICT Incidents

Examples of ICT Incidents are given below. It should be noted that this list is not exhaustive.

- Virus/Malware infection or warning
- Loss of Device/Bitlocker Key
- Non-compliance with ICT Policies/Procedures
- System Malfunction (Hardware/Software)
- Unauthorised/Uncontrolled System Changes
- Loss of Mobile Phone/Tablet

Information Governance Incidents

Examples of the most common Information Governance Incidents are listed below. It should be noted that this list is not exhaustive.

- Information disclosed in error (verbally, in writing, or electronically – i.e. sending a sensitive e-mail to 'all staff' by mistake).
- Information lost in transit (hard copy or electronic format)
- Lost or stolen paperwork
- Non-secure disposal – hardware (i.e. failing to securely wipe hard-drive)
- Non-secure disposal – paperwork (i.e. sensitive information disposed of in standard waste bin)
- Disclosure of passwords (i.e. writing down passwords – giving password to another person)
- Tailgating (allowing another person to enter without checking identity)
- Access doors left open
- Confidential paperwork left out (not in secure storage)
- Lost or Found ID Badges
- Lost or Found Door Access fobs
- Indication or suspicion of unauthorised access to building (damage to door locks or windows – caught on CCTV)
- Indication or suspicion of unauthorised access to IT system

Appendix 2 – Information Governance Incident Management Process

1. Reporting an Incident

1. A security incident is observed or reported.
2. Officer completes an Information Governance Incident Form on Minerva (<http://minerva.sharelincs.net/pages/incident-management.aspx>).
3. A SharePoint workflow automatically creates a list item, sets the Incident Status to “Open”.
4. A SharePoint workflow calculates a level of response required based on the following matrix:

		Impact		
		High	Medium	Low
Urgency	High	Level 3	Level 3	Level 2
	Medium	Level 3	Level 2	Level 1
	Low	Level 2	Level 1	Level 0
	Confidential or Personal Data involved	Level 3		

Level 3 (Confidential or Personal Info involved) - 8 hour response and Senior Information Risk Owner (SIRO) involvement required.

Level 3 – 24 hour response required and senior management signoff.

Level 2 – 48 hour response required and team manager signoff.

Level 1 - 72 hour response required and investigating officer signoff

Level 0 – For routine incidents or incidents resolved at source. CIGG monitoring and signoff.

5. SharePoint workflow generates an email and sends it to the Incident Response Team (IRT) IGIncidents@west-lindsey.gov.uk.
6. IRT assess the incident, take mitigating actions if appropriate, assign the investigating officer(s) based on the type of incident and responsible function, and forward the incident email to them.
7. Investigating officer(s) investigate the incident, take or propose mitigating actions to prevent the incident becoming worse, and recommend the actions needed to resolve it. If the incident involves loss or compromise of personal information the investigating officer(s) must refer to the Data Protection Breach Policy for guidance on breach reporting.
8. Once all actions have been recorded in the form the investigating officer sets the Incident Status to “Complete”.

9. The Corporate Information Governance Group (CIGG) meets approximately 6 weekly and is responsible for reviewing all “Open” and “Completed” incidents. The CIGG members are also responsible for confirming that all actions have been taken and that any awareness messages are cascaded to their respective teams. Incidents approved for closure are listed in the CIGG meeting minutes.
10. The Information Governance Officer sets the Incident Status for incidents approved for closure by the CIGG to “Closed”.
11. Incident is resolved.

2. Escalation Criteria

The IRT will monitor open incidents and decide, in consultation with the Investigating Officer, if a case needs to be escalated. A case can be escalated if a response has not been received by the target date or if the Investigating Officer cannot resolve the incident without senior management support.

3. Data Breach Reporting

Incidents involving the loss or compromise of personal information covered by the Data Protection Act must be investigated in accordance with the Council’s Data Protection Breach Policy. Serious incidents involving large quantities of data or which affect a large number of people must be reported to the Information Commissioner’s Office (ICO). Guidance on when to report incidents is given in the Data Protection Breach Policy.

Any incident involving the loss or compromise of personal information being shared with partners or being processed on behalf of partners must be reported to those partners in accordance with any contracts or data sharing agreements in place.

4. Roles and Responsibilities

The Incident Response Team

The Incident Response Team (IRT) is responsible for reacting to incidents or weaknesses as soon as they are reported or identified and for ensuring that they are quickly assigned to the appropriate officer or officers for investigation and resolution. The IRT comprises:

- ICT Team (Level 2 & 3 Officers). This ensures that senior ICT staff have oversight of both IG and ICT incidents.
- Information Governance Officer (IGO)

The IRT members will receive notification of an incident by email and will assess the incident and assign it to the appropriate officer according to the type of incident and the team responsible for the function.

For instance, the IRT would assign an incident involving a lost ID badge to a Human Resources Officer.

Investigating Officers

Investigating officers are responsible for ensuring that incidents are properly investigated and their effects minimised within set targets.

Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) (Director of Resources) is responsible to the Chief Executive for ensuring all information risks are recognised and managed in the Council organisation through its information risk policy and assessment process. The SIRO must be informed of any serious information security incident and especially any incident involving confidential or personal information.

Corporate Information Governance Group

The Corporate Information Governance Group (CIGG) is a consultation group and has a pivotal and central role in making sure that Information Governance is effectively managed across the organisation. The group comprises the information specialists from across all service areas and will review all incidents and will ensure that the lessons learned from these are cascaded to teams and included in procedures and awareness training.

Information Governance Officer

The Information Governance Officer (IGO) is a permanent role responsible to the SIRO for the day to day administration and enforcement of the Council's Information Governance Policy. The IGO is a member of the IRT and monitors and advises where appropriate on incident management and administers the IG Incident Reporting System.

5. Learning from Information Security Incidents

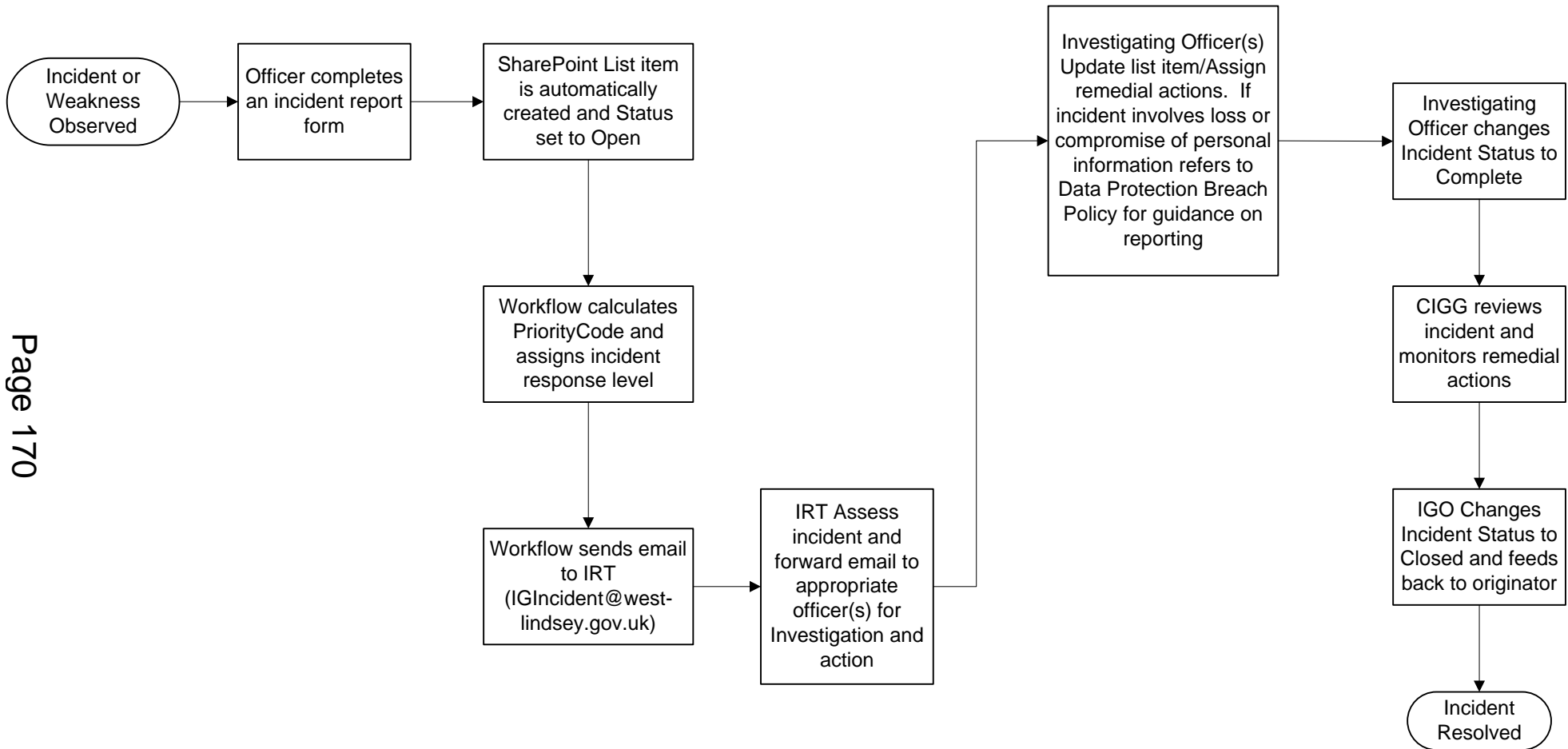
To learn from incidents and improve the response process incidents must be recorded and a Post Incident Review conducted. This is the responsibility of the Corporate Information Governance Group (CIGG) which is chaired by the SIRO. The following details must be retained:

- Types of incidents.
- Volumes of incidents and malfunctions.
- Costs incurred during the incidents.

The information must be collated and reviewed on a regular basis by the ICT Department and any patterns or trends identified. Any changes to the process made as a result of the Post Incident Review must be formally noted.

The information, where appropriate, should be shared with the East Midlands Warning, Advice and Reporting Point (WARP) to aid the alert process for the region.

Appendix 3 - Information Governance Incident Management Process Flow



Internet Acceptable Use Policy

Document Control

Organisation	West Lindsey District Council
Title	Internet Acceptable Usage Policy
Author	S M Anderson
Owner	ICT Manager
Subject	IT Policy
Review date	23 Jun 2015

Revision History

Revision Date	Revisor	Previous Version	Description of Revision
17/2/2011	Steve Anderson	Draft V0.1	Plain English guidelines applied
10/3/2011	Steve Anderson	Draft V0.2	Para 6.3. Requirement to not have personal items ordered over the Internet delivered to a Council address removed.
18/3/2011	Steve Anderson	Draft V0.3	Para 4 amended to include Internet access from any Council-approved smartphone device.
7/4/2011	Steve Anderson	Draft V0.4	Adopted by O&R Committee
6/2/2014	Steve Anderson	Version 1.0	Ref to old Use of Computers Policy removed.
23/6/2014	Steve Anderson	Version 1.1	Reviewed by Corporate Information Governance Group. Minor updates and corrections added. Approved by CMT.

Contents

1	Policy Statement.....	4
2	Key Messages	4
3	Purpose	4
4	Scope	4
5	Risks.....	4
6	Applying the Policy	5
6.1	What is the Purpose of Providing the Internet Service?.....	5
6.2	What You Should Use Your Council Internet Account For.....	5
6.3	Personal Use of the Council’s Internet Service.....	5
6.4	Internet Account Management, Security and Monitoring	6
6.5	Things You Must Not Do.....	6
6.6	Your Responsibilities	7
6.7	Line Manager’s Responsibilities	7
6.8	Who Should I Ask if I Have Any Questions?	7
7	Policy Compliance	7
8	Review and Revision	8
9	References	8
	Appendix 1 – Agreement	9

1 Policy Statement

West Lindsey District Council (“the Council”) will make sure all users of Council-provided Internet facilities are aware of the dangers and acceptable use of these facilities.

2 Key Messages

- You must familiarise yourself with the detail, essence and spirit of this Policy before using the Council’s Internet facility.
- At the discretion of your team manager, and provided it does not interfere with your work, the Council allows personal use of the Internet in your own time (for example during your lunch-break and before and after work hours).
- You are responsible for the security provided by your network account. Only you should know your log-on id (username) and you should be the only person who uses your account.
- You **must not** create, download, upload, display or access knowingly, sites that contain pornography or other “unsuitable” material that might be deemed illegal, obscene or offensive.
- You must assess any risks associated with your Internet usage and make sure that the Internet is the most appropriate mechanism to use.
- You must not use any material obtained from the Internet in a manner which might infringe the owner’s copyright.

3 Purpose

This Policy document explains how you should use your Council Internet facility. It outlines your personal responsibilities and what you must and must not do.

The Internet facility is made available for the business purposes of the Council. A certain amount of personal use is allowed in accordance with the statements contained within this Policy.

The Council recognises that it is impossible to define precise rules covering all available Internet activities. Users must respect the spirit of the Policy to make sure their use of the facility is productive.

4 Scope

This Internet Acceptable Usage Policy applies to, but is not limited to, all councillors, committees, departments, partners, employees of the Council, contractual third parties and agents of the Council who access the Council’s Internet service and Information and Communication Technology (ICT) equipment.

The Policy should be applied at all times whenever using the Council-provided Internet facility. This includes access via any access device including a desktop computer or Council-approved smartphone device and when using any of the Council’s approved remote/home working channels.

5 Risks

The Council recognises that there are risks associated with users accessing and handling information when carrying out official Council business.

This Policy aims to mitigate the following risk:

- Uncontrolled access to the Internet from the corporate network could lead to loss of productivity, increased exposure to malware, spyware, phishing attacks and illegal or criminal activity resulting in user access to information systems and facilities being lost, legal action being taken against the Council as a result of misuse of the Internet or the Council failing to comply with the requirements for connecting to government secure networks.

6 Applying the Policy

6.1 What is the Purpose of Providing the Internet Service?

The Internet service is primarily provided to give Council employees and councillors:

- access to information that is relevant to fulfilling the Council's business obligations;
- the capability to post updates to Council owned and/or maintained web sites; and
- an electronic commerce facility.

6.2 What You Should Use Your Council Internet Account For

Your Council Internet account should be used in accordance with this Policy to access anything in carrying out your work including:

- access to and/or provision of information;
- research; and
- electronic commerce (e.g. buying equipment for the Council).

6.3 Personal Use of the Council's Internet Service

At the discretion of your line manager, and provided it does not interfere with your work, the Council permits personal use of the Internet in your own time (for example during your lunch-break and before or after working hours).

The Council is not, however, responsible for any personal transactions you enter into - for example in respect of the quality, delivery or loss of items ordered. You must accept responsibility for, and keep the Council protected against, any claims, damages, losses or the like which might arise from your transaction. For example, in relation to payment for the items or any personal injury or damage to property they might cause.

If you purchase personal goods or services via the Council's Internet service you are responsible for making sure that the information you provide shows that the transaction is being entered into by you personally and not on behalf of the Council.

If you are in any doubt about how you may make personal use of the Council's Internet service you are advised not to do so.

All personal usage must be in accordance with this Policy. Your computer and any data held on it are the property of the Council. It may be accessed at any time by the Council to make sure that all its statutory, regulatory and internal policy requirements are being complied with.

6.4 Internet Account Management, Security and Monitoring

The Council will provide access to the Internet through your network account which comprises a secure logon-id (username) and a two-factor authentication method. The Council's ICT Department is responsible for the technical management of this account.

You are responsible for the security provided by your network account. Only you should know your log-on id and you should be the only person who uses your account.

The provision of Internet access is owned by the Council and all access is recorded, logged and interrogated for the purposes of:

- monitoring total usage to make sure business use is not impacted by lack of capacity; and
- monitoring and recording all access for reports that can be produced for line managers and auditors on request.

6.5 Things You Must Not Do

Except where it is strictly and necessarily required for your work, for example ICT audit activity or other investigation, you must not use your Internet account to:

- create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive;
- subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files;
- subscribe to, enter or utilise real time chat facilities such as chat rooms, text messenger or pager programs;
- subscribe to, enter or use online gaming or betting sites;
- subscribe to or enter "money making" sites or enter or use "money making" programs;
- run a private business;
- download any software that does not comply with the Council's Software Policy (To Be Issued); or
- use any material obtained from the Internet in a manner which might infringe the owner's copyright.

The above list gives examples of "*unsuitable*" usage but is neither exclusive nor exhaustive. "*Unsuitable*" material would include data, images, audio files or video files the transmission of which is illegal under British law, and, material that is against the rules, essence and spirit of this and other Council policies.

6.6 Your Responsibilities

It is your responsibility to:

- familiarise yourself with the detail, essence and spirit of this Policy before using the Internet facility provided for your work;
- assess any risks associated with Internet usage to make sure that the Internet is the most appropriate mechanism to use;
- understand that you may only use the Council's Internet facility within the terms described in this Policy;
- Report any security incidents or weaknesses in accordance with the Information Security Incident Management Policy; and
- read and abide by the following related policies:
 - Email Policy
 - Software Policy (TBA).
 - IT Access Policy.
 - Remote Working Policy.
 - Information Security Incident Management Policy.
 - Legal Responsibilities Policy.

6.7 Line Manager's Responsibilities

Line managers are responsible for making sure that their staff's Internet use:

- in work time is relevant to and appropriate to the Council's business and within the context of the users responsibilities; and
- in their own time is subject to the rules contained within this document.

6.8 Who Should I Ask if I Have Any Questions?

In the first instance you should refer questions about this Policy to your manager who can refer you to the Information Governance Officer if appropriate. Councillors should refer questions to the Monitoring Officer or the Team Manager, People and Organisational Development.

You should refer technical queries about the Council's Internet service to the ICT Helpdesk on Ext. 165.

7 Policy Compliance

Non-compliance with this Policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

Any user found to have breached this Policy may be subject to the Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this Policy or how it may apply to you, seek advice from your manager.

8 Review and Revision

This Policy will be reviewed as appropriate, but no less frequently than every 12 months.

The policy review will be carried out by the ICT Manager supported by the Corporate Information Governance Group (CIGG).

9 References

The following Council Policy documents are directly relevant to this Policy, and are referenced within this document:

- Email Policy.
- Software Policy (TBA).
- IT Access Policy.
- Remote Working Policy.
- Information Security Incident Management Policy.
- Legal Responsibilities Policy.

The following Council Policy documents are indirectly relevant to this Policy;

- PSN Acceptable Usage Policy and Personal Commitment Statement.
- Computer, Telephone and Desk Use Policy.
- Mobile Device Policy.
- Information Management and Protection Policy.
- Human Resources Information Security Standards (TBA).
- IT Infrastructure Security Policy.
- Communications and Operation Management Policy (TBA).

Appendix 1 – Agreement

Acceptable Usage Policy

Each user must read, understand and sign to verify they have read and accepted this Policy. The Policy must be signed annually.

- I understand and agree to comply with the Internet Acceptable Usage Policy of my organisation.

Signature of User:

A copy of this agreement is to be retained by the User and People and Organisational Development.

Document Date:	
Name of User:	
Position:	
Department:	

Mobile Device Policy

Version Number	Version 2.0
Approved by	Policy and Resources Committee
Date approved	16 Apr 2015
Review Date	16 Apr 2016
Authorised by	Director of Resources
Contact Officer	Information Governance Officer

Revision History

Revision Date	Revisor	Previous Version	Description of Revision
Draft Version 0.2	24/2/2015	Draft Version 0.1	Minor typographical amendments and references to members added to appendices 4 and 5 following JSCC Chairs Brief.
Version 1.0	16/4/2015		Approved and adopted by P&R Committee

Contents

1	Introduction	4
2	Scope	4
3	Purpose	5
4	Security of Information	5
5	Access	6
6	Procurement	7
7	Use of Laptops.....	7
8	Use of Mobile Phones, iPads, and Tablets (Council-Owned)	8
9	Disposing of Mobile Computing Devices	9
10	Third Party Access to Council Information.....	10
11	Training	10
12	Policy Compliance and Audit.....	10
13	Policy Governance	11
14	Equality Impact Assessment	12
15	Policy Review and Maintenance.....	12
	Appendix 1 - Policy Overview and Key Messages	13
	Appendix 2 – Council-Owned Laptop/Tablet (Category 1)	15
	Appendix 3 – Managed Mobile Phone/iPads (Category 2).....	16
	Appendix 4 – Personal Mobile Phone (Part Managed) (Category 3).....	17
	Appendix 5 – Unmanaged Personal Remote Desktop (Category 4)	18

1 Introduction

Information is an asset. Like any other business asset it has a value and must be protected. The systems that enable us to store, process and communicate this information must also be protected in order to safeguard information assets.

We use the collective term ‘information systems’ for our information and the systems we use to store, process and communicate that information. The practice of protecting our information systems is known as ‘information security’ and is one of the key themes of the Council’s Information Governance Framework.

This Policy is part of a set of information governance policies and procedures that supports the delivery of the Information Governance Framework. It should be read in conjunction with these associated policies and in particular the Information Security Policy.

West Lindsey District Council (“the Council”) recognises that there are risks associated with users accessing and handling information in order to conduct official business. Information is used throughout the Council and sometimes shared with external organisations and applicants. Mobile computing devices have become indispensable tools for enhancing collaboration and productivity by making it easier to work when away from the office. However, these high-capacity devices are easily lost or stolen, presenting major risks of information loss. They can also infect PCs and networks by transferring malware and viruses. Portable computing devices can carry information far from Council premises and thereby expose them to different and potentially increased risks.

Non-compliance with this Policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers. The impact of resultant damage to the Council’s reputation should not be underestimated.

2 Scope

This Policy applies to everyone who has access to the Council’s information, information assets or IT equipment. These people are referred to ‘users’ in this Policy. This may include, but is not limited to employees of the Council, members of the Council, temporary workers, partners and contractual third parties.

All those who use or have access to Council information must understand and adopt this Policy and are responsible for ensuring the security of the Council’s information systems and the information that they use or handle.

For the purposes of this Policy, mobile computing devices which may be granted access to the corporate network fall into one of four categories. These are:

1. Council-owned Laptop/Tablet
2. Managed Mobile Phones/iPads
3. Personal Mobile Phones (part-managed)

4. Unmanaged Personal RDP access

Specific details for each category is given in the appendices to this document.

3 Purpose

This Policy establishes the principles and working practices that are to be adopted by all users in order for information to be safely stored and transferred on mobile computing devices. It aims to ensure that these devices are used securely in order to:

- Maintain the security and **confidentiality** of the Council's information assets when they are accessed by users from mobile devices;
- Maintain the **integrity** and **availability** of information in order to guarantee access to accurate information whenever it is required;
- Prohibit the disclosure of information as may be necessary by law and maintain high standards of care in ensuring the security of protectively marked information;
- Prevent disclosure of protectively marked information as a consequence of loss, theft or careless use of media and mobile computing devices;
- Avoid contravention of any legislation, policies or good practice requirements, potential sanctions against the Council or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse, or potential legal action against the Council or individuals as a result of information loss or misuse;
- Prevent reputational damage as a result of information loss or misuse;
- Prevent unintended or deliberate consequences to the stability of the Council's computer network by contamination of Council networks or equipment through the introduction of viruses or other malware through the transfer of information from one form of IT equipment to another;
- Build confidence and trust in the information that is being shared between systems;
- Enable wide and simple access to Council information by all those who are authorised to use it;
- Improve service delivery by giving staff and customers secure access to the information they need.

4 Security of Information

Information that is only held in one place and in one format is at much higher risk of being unavailable or corrupted through loss, destruction or malfunction of equipment than information which is frequently backed up. Therefore mobile devices (and removable media) should not be the only places where information obtained for Council purposes is held.

Copies of any information stored on mobile devices (or removable media) must also remain on the source system or networked computer until the information is successfully transferred to another networked computer or system.

In order to minimise the potential for a security breach the following security measures must be applied to all mobile computing devices:

- In order to minimise physical risk, loss, theft or electrical corruption, all mobile computing (and any removable media) must be stored in an appropriately secure and safe environment.
- All OFFICIAL information held on mobile computing devices must be encrypted where possible.
- Information must not be held on mobile computing devices for longer than necessary and should be securely deleted once it is no longer required. Information must not be stored solely on device desktops.
- Whilst in transit or storage the information held on any mobile devices must be given appropriate security according to the type of information and its sensitivity in line with the Council's Protective Marking Policy (see Information Management and Protection Policy).
- Users must make sure that access/authentication tokens, usernames, passwords and other authentication information should be kept secure and in a separate location to the mobile computing device.
- Users should be aware that the Council will deploy software to monitor the use of and the transfer of Council information to and from all Council-owned and personal-owned IT equipment. It will prohibit the use of devices that have not been recorded on the Corporate IT Asset Register. Management reports will be generated and used to support internal and external audit.
- Damaged, faulty or infected devices should not be used.
- Up-to date virus and malware checking software should be operational on both the machine from which the information is taken and the machine on to which the data is to be loaded. In order to implement this, it is necessary to regularly connect laptops and tablets to the corporate network.
- If whilst using mobile devices the checking software indicates there is a problem, use of the device must be stopped immediately and Corporate ICT Services informed so it can be recorded as a security incident in accordance with the Information Security Incident Management Policy.
- Users **must** ensure they comply with the Council's Information Security Policy and Protective Marking Policy.

5 Access

All information processing within the Council is guided by its adopted Enterprise Architecture Data Principles. Accordingly, it is the Council's policy to limit the use of

mobile computing to only devices which fall into Category 1 – Council-owned Laptop/Tablet for processing and storing confidential, personal, and otherwise controlled information. There are large risks associated with the use of mobile computing devices and therefore clear business benefits that outweigh the risks must be demonstrated before approval is given for other device categories. The use of mobile computing devices in categories 2, 3, and 4 for the processing and storage of protected information will only be approved if a valid business case is supplied. Connection of user-owned devices to the Council's network will only be approved if a business case meets the requirements of the Council's Bring Your Own Device Policy.

Approval for access to, and use of, mobile computing devices must be given by the user's Team Manager or a Strategic Lead or a Director.

Should access to, and use of, mobile computing devices be approved the following sections apply and must be followed at all times.

6 Procurement

Any mobile computing device used in connection with Council equipment or the network or to hold information used to conduct official Council business and any associated peripheral equipment and software **must** only be procured through Corporate ICT Services in accordance with agreed procurement methods as per the Contract Procedure Rules and Financial Procedure Rules and Approved Code of Practice (ACoP) No. 25 – Software Acquisition and Deployment.

All ICT hardware devices used to access the Council network should be recorded on the Corporate IT Asset Register.

Non-Council owned removable media devices **must not** be used to store any information used to conduct official Council business, and **must not** be used with any Council-owned or leased IT equipment unless authorised by Corporate ICT Services. For more information on the use of removable media devices refer to the Removable Media Policy, part of the Information Governance Framework

7 Use of Laptops

All Council computer systems are subject to information security risks, but the portability of laptops makes them particularly vulnerable to damage, loss or theft, either for their re-sale value or the information they contain. Furthermore, the fact that they are often used outside Council premises increases the risks from personnel outside the Council.

In order to minimise the potential risks, users must apply the following security controls:

- The physical security of laptops is the personal responsibility of users who must take all reasonable precautions and be sensible and stay alert to the risks.
- Users must keep laptops within their possession within sight whenever possible. They should never be left visibly unattended. Extra care should be taken in public places such as airports, railway stations or restaurants. It takes thieves just a fraction of a second to steal an unattended laptop.
- Where possible, laptops should be locked out of sight and must never be left visibly unattended in a vehicle. If absolutely necessary, they should be locked out of sight in the boot but it is generally much safer for the user to take them with them.
- Access tokens should be removed from the device immediately after logon and secured out of sight. Under no circumstances must they be stored with the device.
- Laptops should be carried and stored in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage. An ordinary-looking briefcase is also less likely to attract thieves than an obvious laptop bag. If a laptop is lost or stolen, the Police should be notified immediately and the Corporate ICT Service Desk informed as soon as practicable in accordance with the Council's Information Security Incident Management Policy.
- Information should not be stored on local hard drives (this includes all local folders and the Desktop (which is just another local folder) unless there is no alternative.
- Information identified by the Information Asset Owner as needing a level of protection (i.e. personal or confidential information) should not be stored on the hard drive unless it is encrypted.
- Data encryption will be applied to all laptop hard drives owned by the Council.

8 Use of Mobile Phones, iPads, and Tablets (Council-Owned)

All Council computer systems are subject to information security risks, but the portability of mobile phones, iPads, and tablet computers makes them particularly vulnerable to damage, loss or theft, either for their re-sale value or the information they contain. Furthermore, the fact that they are often used outside Council premises increases the risks from personnel outside the Council.

In order to minimise the potential risks, users must understand and apply the following security controls:

- Personal devices (i.e. non-Council-owned) shall not be connected to a laptop, tablet, or desktop for any other purpose than re-charging the device.

- No information identified by the Information Asset Owner as needing a level of protection (i.e. personal or confidential information) shall be stored on a mobile phone, iPad, or tablet computer unless it is encrypted and the device is locked with a PIN code.
- It is the user's responsibility that sensitive information, including that contained in emails, shall not be held on a mobile phone, iPad, or tablet computer for longer than is necessary.
- All spam, chain and other junk emails are subject to the Council's email policy.
- The downloading of unauthorised software onto a Council-owned mobile phone, iPad, or tablet computer is prohibited. The ICT Department will publish a list of authorised software and "apps" on the Intranet for download.
- Employees shall report any suspected virus or malware to the Corporate ICT Service Desk immediately.
- Internet access via a Council-owned mobile phone, iPad, or tablet computer is subject to the Council's Internet Acceptable Use Policy.
- Employees shall take all appropriate precautions to protect the mobile device from loss, theft or damage. These precautions include, but are not limited to:
 - The device shall not be left unattended in public view in a vehicle;
 - The device shall not be left unattended in a public place;
 - The keypad shall be locked at all times when the device is not in use;
 - All mobile phones, iPads, or tablet computers shall be password protected in accordance with Council policy;
 - It should be noted that if a user loses or has a mobile phone, iPad, or tablet computer stolen on which they have stored unencrypted personal data owned by the Council, they may be liable to prosecution under the Data Protection Act 1998.

9 Disposing of Mobile Computing Devices

Mobile computing (and removable) devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage. Any previous contents must be thoroughly erased using specialist software and tools where necessary in line with the IT Equipment Disposal Policy.

The Corporate IT Asset Register must be updated accordingly.

For advice or assistance on how to thoroughly remove all data, including deleted files, from mobile devices (or removable media) contact the ICT Service Desk.

10 Third Party Access to Council Information

No third party (external contractors, partners, agents, the public, or non-employee parties) may receive data or extract information from the Council's network, information stores, or IT equipment without explicit agreement from the Information Asset Owner.

Should third parties be allowed access to Council information then all the considerations of this Policy apply to their storing and transferring information.

Third party access to Council information should be supported with contract clauses and either a Data Sharing Agreement, Data Processing Agreement, Confidentiality Letter, or Non-disclosure agreement. Third parties are required to agree and sign the Council's Third Party Connection Policy.

Where mobile (or removable media) devices are to be used by third parties, for example when providing training, these should be made available prior to being required in order that they can be checked for malware on a stand-alone PC prior to being connected to the network.

11 Training

Training is an important part of the Council's mobile deployment. For each device category, training will be given as detailed in the relevant appendix.

The aim of the training is to show users how to work from remote locations, operate the systems, safe guard data/equipment and how to report incidents if something goes wrong.

A user policy will set out the key dos and don'ts in relation to mobile working. Staff and members will be required to agree and sign this policy before remote access is given.

12 Policy Compliance and Audit

Failure to observe the standards set out in this Policy may be regarded as serious and any breach may render an employee liable to action under the Council's disciplinary procedure, which may include dismissal. The disciplinary procedure is part of the Local Conditions of Employment. The Members' Code of Conduct covers any breach of this Policy by elected members.

Non-compliance with this Policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers. The Council will audit its information

governance procedures and where practical and proportional, Corporate ICT Services will monitor users' access to information for the purpose of detecting breaches of this Policy and/or other Council policies and procedures.

All external mobile access is audited and penetration-tested as part of the Council's annual Public Service Network (PSN) audit. This penetration test provides assurance that the security measures adopted by the Council are robust and makes sure there are no untreated security voids or vulnerabilities.

Occasionally there may be situations where exceptions to this Policy are required, as full adherence may not be practical, could delay business critical initiatives or could increase costs. These will need to be risk assessed on a case by case basis. Where there are justifiable reasons why a particular policy requirement cannot be implemented, a policy exemption may be requested from the Senior Information Risk Owner (SIRO) via the Corporate Information Governance Group (CIGG). Exemptions may be granted to an individual, a team/group or a service area and may be for a temporary period or on a permanent basis, but subject to review.

It is the duty of all users to report, as soon as practicably possible, any actual or suspected breaches in information security in accordance with the Information Security Incident Management Policy and procedures. Any user who does not understand the implications of this Policy or how it may apply to them, should seek advice from their team manager and/or the Information Governance Officer.

13 Policy Governance

The following table identifies who within the Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

Responsible – the person(s) responsible for developing and implementing the policy.

Accountable – the person who has ultimate accountability and Council for the policy.

Consulted – the person(s) or groups to be consulted prior to final policy implementation or amendment.

Informed – the person(s) or groups to be informed after policy implementation or amendment.

West Lindsey District Council	
Responsible	Information Governance Officer
Accountable	Senior Information Risk Owner (SIRO) – Director of Resources
Consulted	Corporate Information Governance Group (CIGG), Governance Corporate Leadership Team (GCLT), Joint Staff Consultative Committee (JSCC), Policy and Resources Committee.
Informed	All users and persons with management or oversight responsibility for users.

14 Equality Impact Assessment

Equality and diversity issues have been considered in respect of this Policy and it has been assessed that a full Equality Impact Assessment is not required as there will be no adverse impact on any particular group.

15 Policy Review and Maintenance

This Policy will be reviewed annually, or as appropriate and in response to changes to legislation or Council policies, technology, increased risks and new vulnerabilities or in response to security incidents.

Appendix 1 - Policy Overview and Key Messages

Policy Overview:

This Policy establishes the principles and working practices that are to be adopted by all users in order for information to be safely stored and transferred on mobile computing devices.

Key Messages:

In order to minimise the potential for a security breach the following security measures must be applied to all mobile computing devices:

- The Council will provide mobile computing devices wherever there is a valid business case for their use.
- The use of mobile computing devices for the processing and storage of information will only be approved if a valid business case for its use is developed. Areas processing personal or confidential information will require tight processes of control.
- Only IT equipment procured through formal and agreed processes should be used.
- All OFFICIAL information stored on mobile computing devices **must** be encrypted where possible.
- In order to minimise physical risk, loss, theft or electrical corruption, all mobile computing must be stored in an appropriately secure and safe environment.
- Information must not be held on mobile computing devices for longer than necessary and should be securely deleted once it is no longer required.
- Whilst in transit or storage the information held on any mobile computing device must be given appropriate security according to the type of information and its sensitivity in line with the Council's Protective Marking Policy (see Information Management and Protection Policy).
- All mobile phones, iPads, and tablets shall be password protected in accordance with Council policy.
- If a user loses or has a mobile phone, iPad, or tablet stolen on which they have stored unencrypted personal data owned by the Council, they may be liable to prosecution under the Data Protection Act 1998.
- Users must ensure that access/authentication tokens, usernames, passwords and other authentication information should be kept secure and in a separate location to the mobile computing device.

- Users should be aware that the Council will deploy software to monitor the use of mobile computing devices and the transfer of information to and from all devices and Council-owned IT equipment. The software will prohibit the use of devices that have not been recorded on the Corporate IT Asset Register.
- Management reports will be generated and used to support internal and external audit.
- Damaged, faulty or infected devices should not be used.

Appendix 2 – Council-Owned Laptop/Tablet (Category 1)

Description

A managed Laptop/Tablet is a device that has been purchased by the Council to facilitate Council business. Personal work (other than that permitted by the Council and set out in acceptable usage policies) is not allowed on these devices. This device is managed by the SHAREDLINCS.NET. IT Department and settings are centrally managed using group policy and usage is logged and monitored. The devices are built to a documented standard build.

Approx. number of Devices: 230

O/S: Windows 8.1 Pro

Device Approval Process

Laptops/Tablets are automatically issued to staff that have a role that requires their use.

Removal or use of these devices outside the confines of the main Council building must be authorised by the user's team manager.

Training

Training will include:

- How to use the device
- How to store the device
- Potential Issues
- Lost or stolen procedure
- Sign appropriate UA Policy

Appendix 3 – Managed Mobile Phone/iPads (Category 2)

Description

A managed mobile phone/iPad is a device that has been purchased by the Council to facilitate Council business. The phones are typically windows 8.1 devices and both phones and iPads are managed using the authorities on premise Mobile Device Management (MDM) solution. Currently, only access to non-secure emails is allowed.

Approx. number of devices: 120

O/S Phone: Windows 8.1

O/S iPad: IOS 7

Device Approval Process

Phone/iPad are automatically issued to staff that have a role that requires their use.

Training

Training will include:

- How to use the device
- How to store the device
- Network Types
- Potential Issues
- Lost or stolen procedure
- Sign appropriate UA Policy

Appendix 4 – Personal Mobile Phone (Part Managed) (Category 3)

Description

These are devices personally owned by staff or members. In accordance with the Council's Bring Your Own Device Policy, the Council provides access to non-secure emails only and offers no financial incentives. Management of these devices extends to email functionality using Exchange 2013 ActiveSync policies. If the employee or the member leaves the Council all evidence of the email access can be removed with or without the employee's or member's permission. After this process the phone is left with no access or historical Council emails, contacts or calendar entries.

Approx. number of device: 25
O/S: Windows 8.1, Android and IOS

Device Approval Process

The use of personal devices to undertake Council work must be authorised by team managers.

Training

Training will include:

- How to use the device
- How to store the device
- Network Types
- Potential Issues
- Lost or stolen procedure
- Sign appropriate UA Policy

Appendix 5 – Unmanaged Personal Remote Desktop (Category 4)

Description

Access to Remote Desktop servers may be authorised to staff and members from their home Microsoft Windows device in accordance with the Bring Your Own Device Policy. Typically this would be a PC. These devices are not managed and do not have any direct link into the Council's network. This method of access uses an RDP via a SSL gateway which challenges every user for a username, password and an OTP before gaining access to NON SECURE systems.

Approx. number of users: 100

O/S: Windows Vista – 8.1

Training

- How to setup your home PC/Laptop
- Setting up users 2-Factor
- What can be accessed and what cant
- Local system requirements – AV, Updates and Firewall
- Sign appropriate UA Policy



**Public Service Network Acceptable Use Policy and
Personal Commitment Statement**

Document Control

Organisation	West Lindsey District Council
Title	Public Service Network Acceptable Usage Policy and Personal Commitment Statement
Author	Steve Anderson
Subject	IT Security Policy
Protective Marking	OFFICIAL
Review date	

Revision History

Revision Date	Revisor	Previous Version	Description of Revision
29/03/2010	Steve Anderson	Final Copy – v1.0	Organisational Development Services Manager title revised to Business Improvement Manager
5/4/2011	Steve Anderson	V1.1	Annual review carried out. References to newly issued documents updated. Some minor plain english changes incorporated.
29/8/2013	Steve Anderson	V1.2	Annual review carried out – Document Approvals and Distribution updated. Policy statement updated to reflect current requirements – Corporate risks updated – department names and job titles updated.
14/10/2014	Steve Anderson	V1.3	Annual review carried out – document updated to replace references to GCSx with PSN

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date

Contents

1	Policy Statement	4
2	Scope	4
3	Definition	4
4	Risks	4
5	PSN Acceptable Usage Policy	5
6	PSN Personal Commitment Statement	8
7	Policy Compliance	9
8	Policy Governance	9
9	Review and Revision	9
10	References	10

1 Policy Statement

It is West Lindsey District Council's ("the Council") policy that all users of the Public Service Network (PSN) understand and comply with corporate commitments and information security measures associated with the PSN.

The PSN is a secure Government network and allows secure interactions between connected Local Authorities and organisations that sit on the pan-government secure network infrastructure.

Some Council staff will need to have access to the facilities operated on this network to allow them to carry out their business and may include staff having access to a secure email facility. **Before** access to the PSN can be given to **anyone**, they:

- **should** have been verified against the HMG Baseline Personnel Security Standard (BPSS);
- **must** have completed the council's Information Governance and any associated training; and
- **must** have read and understood this Acceptable Usage Policy (AUP) and signed the Personal Commitment Statement.

Any Council staff who have **administrative** privileges (for example, users who are able to reconfigure the network or system administrators) **MUST** have been verified against the Baseline Personnel Security Standard (BPSS).

All staff are required to complete Information Governance "refresher" training annually and PSN access is to be withdrawn from users who have not completed the refresher training within the preceding 12 months.

This Policy and statement does not replace the Council's existing acceptable usage, or any other, policies. It is a supplement to them.

2 Scope

All users of the PSN must be aware of the commitments and security measures surrounding the use of this network. This Policy must be adhered to by all Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council using PSN services.

3 Definition

This Policy must be adhered to at all times when accessing PSN services.

4 Risks

The Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This Policy aims to mitigate the following risks:

- User either accidentally or deliberately upload malicious software/Trojans to the PSN.

- User seeks to download large quantities of corporate data or OFFICIAL/OFFICIAL-SENSITIVE PSN data to removable media, hard-copy, or to an internet site.
- User seeks to access information for which they do not have authorisation.
- User or third party with administrative privileges either accidentally or deliberately misconfigures security controls to allow a compromise.
- A thief steals a corporate computing device.
- A hacker attacks the PSN from the Internet or via wireless networks.
- A hacker attacks the corporate network from the PSN.
- Interception of traffic or interruption of service.
- Non-reporting of information security incidents.
- The loss of direct control of user access to information systems and facilities.

Failure to comply with this Policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

5 PSN Acceptable Usage Policy

Each PSN user must read, understand and sign to verify they have read and accepted this Policy.

- I understand and agree to comply with the security rules of my organisation.

For the avoidance of doubt, the security rules relating to secure e-mail and information systems usage include:

1. I acknowledge that my use of the PSN may be monitored and/or recorded for lawful purposes.
2. I agree to be responsible for any use by me of the PSN using my unique user credentials (user ID and password, access token or other mechanism as provided) and e-mail address;
3. I will not use a colleague's credentials to access the PSN and will equally ensure that my credentials are not shared and are protected against misuse;
4. I will protect such credentials at least to the same level of secrecy as the information they may be used to access, (in particular, I will not write down or share my password other than for the purposes of placing a secured copy in a secure location at my employer's premises);
5. I will not attempt to access any computer system that I have not been given explicit permission to access;
6. I will not attempt to access the PSN other than from IT equipment and systems and locations which have been explicitly authorised to use for this purpose;
7. I will not transmit information via the PSN that I know, suspect or have been advised is of a higher level of sensitivity than my PSN domain is designed to carry;

8. I will not transmit information via the PSN that I know or suspect to be unacceptable within the context and purpose for which it is being communicated;
9. I will not make false claims or denials relating to my use of the PSN (e.g. falsely denying that an e-mail had been sent or received);
10. I will protect any sensitive or not protectively marked material sent, received, stored or processed by me via the PSN to the same level as I would paper copies of similar material;
11. I will appropriately label, using the Council's protective marking scheme which is detailed in the Information Management and Protection Policy, information up to OFFICIAL/OFFICIAL-SENSITIVE sent via the PSN;
12. I will not send OFFICIAL-SENSITIVE information over public networks such as the Internet;
13. I will always check that the recipients of e-mail messages are correct so that potentially sensitive or OFFICIAL-SENSITIVE information is not accidentally released into the public domain;
14. I will not auto-forward email from my GCSx email account to any other non-GCSx email account;
15. I will not forward or disclose any sensitive or OFFICIAL-SENSITIVE material received via the PSN unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel;
16. I will seek to prevent inadvertent disclosure of sensitive or OFFICIAL-SENSITIVE information by avoiding being overlooked when working, by taking care when printing information received via the PSN (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc) and by carefully checking the distribution list for any material to be transmitted;
17. I will securely store or destroy any printed material;
18. I will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via the PSN (this will be in accordance with the Computer, Telephone and Desk-Use Policy - e.g. logging-off from the computer, activate a password-protected screensaver etc, so as to require a user logon for activation);
19. Where the IT Department has implemented other measures to protect unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked requiring a user logon for reactivation), then I will not attempt to disable such protection;
20. I will make myself familiar with the Council's security policies, procedures and any special instructions that relate to the PSN;

21. I will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security in accordance with the Information Security Incident Management Policy;
22. I will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended;
23. I will not remove equipment or information from Council premises without appropriate approval;
24. I will take precautions to protect all computer media and portable computers when carrying them outside my organisation's premises (e.g. leaving a laptop unattended or on display in a car such that it would encourage an opportunist theft) in accordance with the Council's Remote Working Policy and the Removable Media Policy;
25. I will not introduce viruses, Trojan horses or other malware into the system or the PSN;
26. I will not disable anti-virus protection provided at my computer;
27. I will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that the Council informs me are relevant (please refer to the Legal Responsibilities Policy); and,
28. If I am about to leave the Council, I will inform my manager prior to departure of any important information held in my account and manage my account in accordance with the Council's Email and Records Management Policy.

Name of User:	
Position:	
Department:	
User Access Request Approved by: (Team Manager)	
User Access Request Approved by: (People and Organisational Development)	
Username Allocated (IT Department)	
Email Address Allocated: (IT Department)	@west-lindsey.gcsx.gov.uk
User Access Request Processed: (IT Department)	

6 PSN Personal Commitment Statement

I,, accept that I have been granted the access rights to the PSN. I understand and accept the rights which have been granted, I understand the business reasons for these access rights, and I understand that breach of them, and specifically any attempt to access services or assets that I am not authorised to access, may lead to disciplinary action and specific sanctions. I also accept and will abide by this Policy, personal commitment statement, and all other relevant policies. I understand that failure to comply with this agreement, or the commission of any information security breaches, may lead to the invocation of the Council's disciplinary policy.

Signature of User:

Dated

A copy of this agreement is to be retained by the User and the Team Manager, People and Organisational Development.

7 Policy Compliance

If any user is found to have breached this Policy, they may be subject to the Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this Policy or how it may apply to you, seek advice from the People and Organisational Development Department.

8 Policy Governance

The following table identifies who within West Lindsey District Council is Responsible, Accountable, Consulted, or Informed with regards to this Policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	All Team Managers
Accountable	Senior Information Risk Owner (SIRO)
Consulted	<ul style="list-style-type: none">• Customer First Strategic Lead• DWP CIS Key Contact• Unison
Informed	Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council using the PSN services.

9 Review and Revision

This Policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the Corporate Information Governance Group (CIGG).

10 References

The following West Lindsey District Council Policy documents are directly relevant to this policy, and are referenced within this document:

- Legal Responsibilities Policy
- Computer, Telephone, and Desk-Use Policy.
- Information Security Incident Management Policy.
- Remote Working Policy.
- Removable Media Policy.
- Email Policy.
- Records Management Policy.

The following West Lindsey District Council Policy documents are indirectly relevant to this Policy:

- Internet Acceptable Usage Policy.
- IT Access Policy.
- IT Infrastructure Policy.

This page is intentionally left blank



**Corporate Policy and
Resources Committee**

Date: 13 April 2017

Subject: Implementation of PCI-DSS Security Policy

Report by:

Director of Resources

Contact Officer:

Steve Anderson
Information Governance Officer
01427 676652
Steve.anderson@west-lindsey.gov.uk

Purpose / Summary:

The purpose of this report is to introduce a new Council policy to comply with the PCI-DSS standard

RECOMMENDATIONS:

- 1) That members, approve the attached PCI-DSS Security Policy for formal adoption.
- 2) That delegated authority be granted to the SIRO to make minor house-keeping amendments to the Policy in the future, in consultation with the Chairpersons of the Joint Staff Consultative Committee and the Corporate Policy and Resources Committee.

IMPLICATIONS

Legal: This report has direct positive implications on the Council's compliance with the Payment Card Industry Data Security Standard.

If an organisation loses card data and is not PCI DSS compliant then there is the potential for financial penalties to be imposed such as:

- fines for the loss of this data;
- fraud losses incurred against the cards involved; and
- bank operational costs associated with replacing the accounts.

Financial: None from this report

Fin Ref: [FIN/1/18](#)

Staffing : None from this report

Equality and Diversity including Human Rights:

None from this report

Risk Assessment: None

Climate Related Risks and Opportunities : None from this report.

Title and Location of any Background Papers used in the preparation of this report:

Call in and Urgency:

Is the decision one which Rule 14.7 of the Scrutiny Procedure Rules apply?

i.e. is the report exempt from being called in due to urgency (in consultation with C&I chairman)

Yes

No

X

Key Decision:

A matter which affects two or more wards, or has significant financial implications

Yes

No

X

1. Background

The Payment Card Industry Data Security Standard (PCI DSS)

1.1 PCI DSS is a worldwide standard that was set up to help businesses process card payments securely and reduce card fraud. It does this through tight controls surrounding the storage, transmission and processing of cardholder data that businesses handle. PCI DSS is intended to protect sensitive cardholder data. If an organisation loses card data and is not PCI DSS compliant then there is the potential for financial penalties to be imposed such as:

- fines for the loss of this data;
- fraud losses incurred against the cards involved; and
- bank operational costs associated with replacing the accounts.

1.2 Customers may also opt for alternate, more resource intensive payment methods. As the Council takes a substantial number of payments by card (21,153 between Apr 2016 and Nov 2016) this would have a detrimental effect on the Medium Term Financial Plan.

1.3 Requirement 12 of the Standard requires all organisations who take card payments to:

“Maintain a policy that addresses information security for all personnel. A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.

For the purposes of Requirement 12, “personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are “resident” on the entity’s site or otherwise have access to the cardholder data environment.”

1.4 This report presents a **NEW** Policy to comply with Requirement 12.

1.5 The Policy will be a sub-policy of the Council's IT Security Policy and, while essentially standalone, must be read and applied in conjunction with other policy documents in the set. It has been developed with advice and assistance from Internal Audit and relevant experts in the Council and supports a number of recommendations in the recent PCI DSS Compliance Internal Audit Report dated December 2016.

2. Scope

2.1 The Policy applies to staff, contractors and third parties who access the Council's Cardholder Data Environment (CDE) for the purposes of taking payments or maintaining the payment systems.

3. **The Policy**

The Policy is relevant to the Council's 3 methods of taking card payments:

1. Web Payments (Cardholder Not Present).
2. Face to Face Card Payments (Cardholder Present).
3. Self-serve Kiosk in Customer Services.

The document has been structured to comply with the PCI DSS Standard with sections for the following:

- General policy statements;
- Handling of credit cards;
- Physical security;
- Acceptable use; and
- Responsibilities.

Appendix 1 of the Policy provides information on the card readers in use in the Council to enable staff to inspect the devices for tampering or damage.

4. **Policy Implementation**

All staff, contractors and third parties who access the Cardholder Data Environment either to take payments or maintain our payment systems will be required to read and sign this Policy. They will also be required to undertake specialist PCI-DSS training on our Corporate Learning Platform.

5. **Decisions Required**

- 1) That members, approve the attached Information Governance Policy, Legal Responsibilities Policy and Information Sharing Policy for formal adoption.
- 2) That delegated authority be granted to the SIRO to make minor house-keeping amendments to the Policy in the future, in consultation with the Chairmen of the Joint Staff Consultative Committee and the Corporate Policy and Resources Committee.

PCI-DSS Security Policy

Table of Contents

1	Overview.....	3
2	Purpose	3
3	Scope	3
4	Policy	3
4.1	General	3
4.2	Credit Card Handling.....	4
4.2.1	Scope	4
4.2.2	Policy Statements	4
4.3	Physical Security	7
4.3.1	Device Checking.....	7
4.3.2	Personnel Checking	7
4.4	Acceptable Use	8
4.5	Responsibilities	8
5	Policy Compliance	9
5.1	Compliance Measurement	9
5.2	Exceptions.....	9
5.3	Non-Compliance	9
5.4	Policy Review.....	9
6	Related Standards, Policies, and Processes	9
	Appendix 1 - Detecting Evidence of Device Tampering	10
	Device Details	10
	Reverse Side Unique Identification Labels	11
	Reverse Side Connectors	12
	Screw Positions	13
	Left Side Tether	13
	POI Weights	13
	Inspecting the Device	13
	Example of an Inspection Log of all Card Machines.....	14

1 Overview

This Policy provides essential information for everyone tasked with handling credit and debit cards, credit and debit card data and the systems processing such data within West Lindsey District Council (the Council).

2 Purpose

The Policy is designed to make sure we can meet the standards required by the Payment Card Industry's Data Security Standard (PCI-DSS), which the Council is obliged to meet in order to be able to process credit card payments.

3 Scope

All environments within the Council where credit and debit cards are handled.

4 Policy

4.1 General

- System users shall not send confidential data, such as credit or debit cardholder data, unencrypted, via end-user messaging technologies such as, e-mail, instant messaging or chat without using an approved encryption solution. Where a solution is not available the data shall not be sent via any of these methods.
- All employees, 3rd parties or contractors shall not attach or use within the Council's cardholder data environments network devices including but not limited to modems, remote-access technologies, wireless technologies, removable electronic media, personal laptops, tablets, PDAs, iPods or personal storage media (e.g. memory sticks).
- Users shall not store confidential data, such as credit and debit cardholder data on local hard drives, USB sticks, or other external or mobile media. If anyone must store confidential data on a hard disk that is not in a securely protected environment, they must report this to the ICT Department so that the data can be encrypted with Council-approved encryption solutions.
- All employees, 3rd parties or contractors are responsible for the Council's assets, (particularly confidential data) that they use to carry out their function. Any suspicious activity or suspect breach in security must be immediately reported in accordance with the Council's Information Security Incident Management Policy.
- Ensure documents containing credit and debit cardholder data are securely locked away.

4.2 Credit Card Handling

4.2.1 Scope

This section provides the minimum mandatory requirements that need to be applied to all employees that handle or come across credit or debit cardholder data, in any format within the Council environment. Furthermore any third party that uses or accesses any of the Council's credit cardholder data, either physically or logically must also comply with this section. It is not the Council's intention to hold cardholder data, however, this section outlines what to do if such a situation arises.

4.2.2 Policy Statements

4.2.2.1 General

- Failure to protect card data can lead to large fines from banks, expensive investigations, expensive litigation, loss of reputation, and in the worst case scenario, withdrawal of the ability to take payment by credit cards; which would greatly hinder the Council's ability to conduct business.
- No staff should handle cardholder data unless you have explicit authorisation to do so.
- Cardholder data should only be handled in such a manner as is explicitly authorised by job roles.

4.2.2.2 Card Data Definitions and Requirements

- 'Credit Card Data' means most of the information on a Credit Card or Debit Card and includes the long 16 digit card number (Primary Account Number - PAN). It also includes the issue and expiry dates and the cardholder's name. The three digit security code on the back of the card is known as the Card Verification Value (CVV). The PAN must always be encrypted when electronically stored and the Cardholder data, if stored with the PAN must be protected.
- The CVV should be handled with great care and should never be written down or stored anywhere, whether on a piece of paper, a form, in a database, in a spreadsheet or any other electronic format, even if encrypted. The only exception to this is where you are taking a payment and need to store the CVV temporarily (pre-authorisation) whilst you arrange to take the payment. After the transaction has been authorised the CVV data must be destroyed immediately.
- If during the performance of your job you can see, by error or intention, a full card number when it is not required for you to do your job, please report this in accordance with the Council's Information Security Incident Management Policy. If, however, your job requires that you need access to the full credit card number and it is not mentioned in your job description, please report this to your line manager so that they can update your job description and confirm it with HR.

4.2.2.3 Card Data Handling Requirements

- Credit card data **MUST NOT** be routinely stored within the Council.
- Credit card data is classified as OFFICIAL-SENSITIVE, in accordance with the Council's Protective Marking Scheme (see the Information Management and Protection Policy). This means that if credit card data has to be stored for a particular reason then it must be protected. If it is stored in systems, it has to be encrypted. If it is stored on paper it must be locked away at all times unless in use. In the first instance, report any credit card number storage to the Council's ICT Manager.
- Do not store credit card data on laptops, desktop computers, file shares, memory sticks etc. unless these are on systems specifically approved for the storage of credit card data. If in doubt, do not store the data.
- Do not store credit card data in spreadsheets and other office documents, unless specifically required for your work, approved in writing by the Director of Resources and the document is encrypted to AES-256 bit standard.
- Any card data found or detected on Council systems must be reported in accordance with the Council's Information Security Incident Management Policy immediately upon discovery.

4.2.2.4 Printing of Documents Containing Card Data

There will be no cardholder data stored routinely within the Council and therefore there will be no printing of cardholder data. Should cardholder data exist, printing of it is expressly forbidden.

4.2.2.5 Handling Documents Containing Card Data

There are numerous cases where card data is legitimately stored on paper, be it a chargeback letter, a fraud document, an exceptions report, or when IT systems are unavailable and manual card payments are in operation. These data need to be retained only until the systems are back up again and card data can be processed electronically.

4.2.2.6 Vigilance and Awareness

- Credit card data can be inadvertently left on printers, fax machines, on a desk, on a screen, in a clear email (although this is against this Policy), in the 'trash' or 'recycle bin' file on a computer, in a temporary file, memory swap files etc.
- A good example of unusual locations to find credit card data is in call recordings. Occasionally telephone calls are recorded for quality and security purposes. These recorded calls can obviously contain the customer giving us their credit card details. To use these call recordings for training purposes the calls should be edited beforehand to remove any mention of a customer's credit or debit card details. So if you are listening to a call recording for training purposes, you should not hear a credit card number.

- If, however, as part of your job you are required to listen to complete calls (for example for real-time quality checking) this is acceptable. However, storing such calls for any length of time must be done securely within an approved storage system.
- Each employee or contractor is responsible to protect Council assets which include all forms of data. It is therefore important that, should you see any credit card data or other confidential data in a place that is insecure, inappropriate or where you do not expect to see it, even if your role includes the ability to work with credit card data you must:
 - a) secure the data, e.g. lock it in your desk;
 - b) report it to your team manager; and
 - c) report the incident in accordance with the Council's Information Security Incident Management Policy immediately.

4.2.2.7 PCI-DSS Data Retention

- Cardholder data must not be routinely stored on any Council system. Cardholder data that is approved to be stored temporarily must be deleted as soon as the reason for storing it has expired.
- Other data referring to the Cardholder Data Environment (CDE) will be treated as outlined below.

4.2.2.8 Payment Card Data

Payment card data will not be stored within the Council.

4.2.2.9 Revenue Protection Correspondence

This refers to all correspondence relating to charge-backs, revenue protection and fraud prevention. These will typically be paper copies and must be destroyed by cross-cut shredding once they have exceeded their retention period.

4.2.2.10 Information Systems and Physical Location Documentation

All documentation relating to Information Systems within the PCI-DSS CDE, including network diagrams, firewall access, system configuration, system passwords and backup documentation must be marked and treated as OFFICIAL-SENSITIVE and held securely with privileged access.

4.2.2.11 Audit Logs

There will be no cardholder data in the Council, therefore no audit logs fall in scope.

4.2.2.12 Cardholder Data Storage Locations

The Council does not store cardholder data.

4.2.2.13 Cardholder Data Disposal

The Council should not routinely hold any cardholder data.

However, if cardholder data exist on any system, the following actions must be taken where appropriate:

- All data must be securely disposed of when no longer required regardless of the media or application type on which it is stored.
- All hard copies of cardholder data must be manually destroyed as soon as it has reached the end of its retention period. A quarterly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.
- The Council requires that all hardcopy materials are crosscut shredded, incinerated or pulped BEFORE they leave Council premises so they cannot be reconstructed.
- All cardholder information awaiting destruction must be held in lockable storage containers clearly marked "To Be Shredded" - access to these containers must be restricted.

4.3 Physical Security

4.3.1 Device Checking

Devices must be inspected at least monthly by staff to look for tampering (for example, addition of card skimmers to devices) or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). More information on how to inspect devices for tampering is given in Appendix 1.

Personnel will be trained to be aware of suspicious behaviour and to report tampering or substitution of devices.

Any tampering or suspicion that tampering has taken place must be reported immediately in accordance with the Information Security Incident Management Policy

4.3.2 Personnel Checking

- Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
- Do not install, replace, or return devices without verification.
- Be aware of suspicious behaviour around devices (for example, attempts by unknown persons to unplug or open devices).
- Report suspicious behaviour and indications of device tampering or substitution to the ICT Help-desk on Ext 165.

4.4 Acceptable Use

- The information system facilities of the Council are provided for business purposes and use of these facilities must be authorised in accordance with the IT Access Policy.
- It is mandatory for all users of systems and equipment within the Council's CDE to sign and adhere to the terms of the Transacting Officers' Protocol for Credit and Debit Card Data Management and the IT Access Policy.
- Employees and other users who deliberately breach the terms of this Policy will be subject to disciplinary action up to and including summary dismissal. Serious offenders are liable for prosecution under the Computer Misuse Act 1990.
- Every user is responsible for the proper use of the equipment they have been assigned and must comply with the Council's policies and all applicable laws.
- Users must ensure anti-virus is installed, up-to-date and operating on all Council devices, and report any failure of provision to the ICT Help Desk.
- It is prohibited to install and download any software on Council computers within the CDE, unless authorised by the ICT Manager.
- Any IT Systems equipment not belonging to the Council should not be installed on the Council network within the CDE, unless permitted, with the authorisation of the ICT Manager. Any such equipment must adhere to the standards within this document.

4.5 Responsibilities

All users within the CDE are responsible for:

1. Familiarising themselves with and adhering to the policies and procedures applicable to their area of responsibility;
2. Protecting Council equipment issued to them against unauthorised access and damage;
3. Using Council equipment for business purposes only;
4. Protecting Council and customer information against unauthorised access and loss;
5. Not disclosing their passwords or sharing user accounts;
6. Ensuring that Council IT systems and facilities (e.g. email or Internet) are used in accordance with the Council's policies;
7. Clearing desks of all sensitive material and logging off or locking workstations at the end of the day and when leaving their desk;
8. Not removing equipment, information or any other Council property from the organisation's premises without authorisation;
9. Not connecting personal equipment to Council networks within the CDE;

10. Not installing, copying or modifying any software on Council equipment without authorisation;
11. Immediately reporting security incidents in accordance with the Council's Information Security Incident Management Policy.

Responsibilities for carrying out specific information security duties will be defined in job descriptions where applicable.

5 Policy Compliance

5.1 Compliance Measurement

Compliance with policies is primarily enforced through process and standard documents that need to be developed by each business unit on how they perform their day to day activities in accordance with these policies.

5.2 Exceptions

Compliance with this Policy is mandatory.

5.3 Non-Compliance

Failure to follow this Policy will be considered as gross misconduct and may result in disciplinary action, up to and including summary dismissal.

5.4 Policy Review

This Policy will be reviewed at least annually by the IT Manager supported by the Corporate Information Governance Group (CIGG).

6 Related Standards, Policies, and Processes

This Policy is a part of West Lindsey District Council's Information Technology Security Policy set and must be read and applied in conjunction all relevant policies in the set.

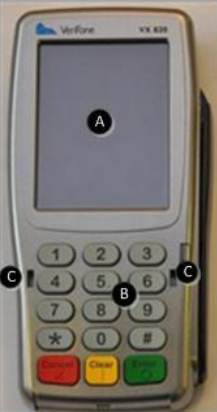




Appendix 1 - Detecting Evidence of Device Tampering

Device Details

Any devices not listed in this section are not MasterCard Payment Gateway Services P2PE supported devices.

Product Numbers: [Verifone Vx820] M282-701-C3-EUA-3 (Silver) M282-701-C3-EUB-3 (Black)

TNSPay – Pin Entry Device – Data Sheet

FRONT	REVERSE	BOTTOM	LEFT SIDE	RIGHT SIDE
				
<p>The top or front panel of the Vx820 PED is shown. This contains:</p> <ul style="list-style-type: none"> A - colour touch screen B - keypad C - pin guard connector slots <p>The facias are available in silver and black.</p>	<p>The back or reverse side panel of the Vx820 is shown. On this side the device labels can be found.</p> <p>The labels provide general information, specifically:</p> <ul style="list-style-type: none"> A – Serial No. B – PTID C – MAC Address <p>At the top end of the panel is a removable cover where the power and data cable is connected, and other connectors that can be used for mounting cradles.</p>	<p>The bottom of the Vx820 device is shown.</p> <p>Located at the bottom end of the device is the card reader for EMV/ICC cards (A).</p> <p>The MSR (magnetic stripe reader) is located on the right side of the unit (B).</p> <p>There are no identification or security markings/labels for these readers.</p>	<p>The left side of the Vx820 device is shown.</p> <p>It has no external marks or identifiers.</p> <p>The panel does contain a connector housing allowing other tethering options for enabling the unit to be physically fixed.</p>	<p>The right side of the Vx820 device is shown.</p> <p>The MSR (magnetic stripe reader) is located on this side of the unit.</p> <p>There are no additional identification marks, security identifiers, or connector options within this panel.</p>

Reverse Side Unique Identification Labels



- 1=General Information Label
 - Model Name
 - Power
 - Product Reference
- 2=S/N Unique Serial No*.
- 3=PTID (Physical terminal identifier)
- 4=MAC address
- 5=Cradle/Mount Connectors



- 1=Serial Number shown through the PED pack cover.

* Please note that if a PED pack option has been selected, the reverse side of the PED will be restricted and the PTID will not be visible. For the Tail Wind and Space Pole PED packs, only the serial number will be visible, an example is shown below:

Reverse Side Connectors



1=Data Connector Cable

Note: There is only once connection point in this device.

2=Security Seal

VeriFone's security seal covering a screw point only used at manufacture. The seal has an image of a VeriFone logo in silver.

3=SAM slots. 3 additional SAM slots.

Screw Positions



There are six screw positions on the back facia. Four are visible below the general information label. Two more are located under the back panel, one is covered by the VeriFone security seal.

Left Side Tether



A Secure Tether Adapter is located on the left facia of the device to allow secure tether options to be attached to the device.

POI Weights

The Vx820 weighs 0.68lb or 308g.

Source: http://global.verifone.com/media/540007/2667-vf-vx820_data-sheet_web.pdf

Inspecting the Device

Deployed payment devices in the merchant's environment must be inspected periodically. This is to detect evidence of tampering, substitution or modification.

The pictures above show the P2PE devices in their manufacturer issues state. Merchants can use this information to conduct visual and physical inspections to validate the integrity of the devices.



**Corporate Policy and
Resources Committee**

Date 13th April 2017

Subject: Mayflower 400 Resources

Report by:

Manjeet Gill
Chief Executive
01427 676500
Manjeet.gill@west-lindsey.gov.uk

Contact Officer:

Karen Whitfield
Leisure & Cultural Services Team Manager
01427 675140
Karen.whitfield@west-lindsey.gov.uk

Purpose / Summary:

To agree appropriate budgets be set aside to support Mayflower 400.

RECOMMENDATION(S):

Members agree the recommendation from Prosperous Communities that a total budget of £30,000 per year for three years is set aside to support Mayflower 400.

IMPLICATIONS

Legal: None

Financial : FIN/137/17
Budget requirement over the 3 years would be £90k. This will be a revenue expense which can be funded from General Fund Balances.
The current General Fund Balance stands at £1,188m with a further £0.6m contribution from revenue underspends as per Q3 monitoring.

Staffing :

Equality and Diversity including Human Rights :

Risk Assessment :

Climate Related Risks and Opportunities : None

Title and Location of any Background Papers used in the preparation of this report:

Call in and Urgency:

Is the decision one which Rule 14.7 of the Scrutiny Procedure Rules apply?

i.e. is the report exempt from being called in due to urgency (in consultation with C&I chairman)

Yes

No

Key Decision:

A matter which affects two or more wards, or has significant financial implications

Yes

No

1 Introduction

- 1.1 2020 marks the 400th anniversary of the sailing of the Mayflower and it has been nationally recognised that Gainsborough Old Hall has an important part in the story.
- 1.2 Mayflower 400 is a national initiative lead by Plymouth City Council to join up the various locations associated with the story and to promote international tourism opportunities, particularly looking at the American market. In 2015 WLDC signed a Compact signifying their commitment to working to promote and commemorate the anniversary.
- 1.3 Since that date work has continued to support both the national initiative being headed up by Plymouth City Council and also at looking what can be done on a local/regional level to optimise the benefit for the local area.
- 1.4 To date this activity has been monitored by the Leisure, Culture, Events and Tourism Member working group which reports into Prosperous Communities Committee.

2. Background

- 2.1 In March this year Prosperous Communities considered a report setting out the national, regional and local opportunities presented by Mayflower 400 and agreed the benefits of adopting a regional approach to the initiative and resourcing this accordingly. This approach avoids the risk of duplication of effort across neighbouring authorities, strengthens the case for funding and provides efficiencies in terms of financial commitment.
- 2.2 Work has already commenced to secure appropriate levels of funding from other Districts including Doncaster, Bassetlaw and Lincolnshire County Council.

3 Budget Required

- 3.1 Prosperous Communities Committee acknowledged the need for West Lindsey District Council funding to be secured both in terms of a contribution towards the Officer resource and also as cash match for funding bids and recommended that this be brought before Corporate Policy and Resources Committee for approval.
- 3.2 The suggested level of financial contribution from West Lindsey District Council is £30,000 per year for three years. This comprises £20,000 per year contribution to a regional Officer post and £10,000 as cash match for funding applications.

4 Recommendation

4.1 It is hereby RECOMMENDED that:

Members agree the recommendation from Prosperous Communities and a total budget of £30,000 per year for three years is set aside to support Mayflower 400.



**Corporate Policy and
Resources Committee**

Date 13th April 2017

Subject: Strategic Transport Model and Development Study

Report by:

Rachael Hughes/Eve Fawcett-Moralee

Contact Officer:

Rachael Hughes, Developer Contribution Officer
Telephone: 01427 676548
Email: Rachael.hughes@west-lindsey.gov.uk

Eve Fawcett-Moralee, Commercial Director
Mobile: 07890 910178
Email: Eve.Fawcett-Moralee@west-lindsey.gov.uk

Purpose / Summary:

To support the procurement of a strategic transport model in the Gainsborough urban area for the purpose of promoting sustainable growth through improving traffic flows within the town whilst also maintaining connectivity from Nottinghamshire and South Yorkshire into the District safeguarding the economic benefits to West Lindsey of the primary routes to Scunthorpe, Lincoln and the coast. .

RECOMMENDATION(S):

1. That members acknowledge the need and agree the procurement of the Strategic Transport Model and Development Study, agreed by Prosperous Communities Committee in February 2017.
2. Members accept the Single Growth Fund 3 Grant award
3. Members approve the release of £271,000 of the grant to fund this study

IMPLICATIONS

Legal: The contract for the Strategic Transport Model and Development Study is with Lincolnshire County Council and therefore falls outside of normal procurement rules

Financial: FIN/3/18

Lead Officer Comments

The £271k cost of this Strategic Transport Model and Development Study will be a revenue expense which can be funded from the Single Local Growth Fund 3, "Housing Unlocking," secured via the GLLEP.

S151 Officer Comments

As part of the successful grant bid to support the Gainsborough Growth Project, the Single Local Growth Fund 3 has now confirmed an award of £4m. The bid included for the improvement of transport infrastructure and connectivity, which this model and study will support.

The cost of this Strategic Transport Model and Development Study is £271k

Lincolnshire County Council have undertaken an appropriate tender process in awarding the contract to Mouchel and it is therefore a competitive price.

Approval of a revenue budget, for the purpose of this expenditure will be required, this will be funded from Single Local Growth Fund 3 grant award.

Staffing: Resources are already in place to project manage this study and all other resources required to undertake the work have been secured as part of the contract with Mouchel.

Equality and Diversity including Human Rights: This project has been developed to improve connectivity between Nottinghamshire and the wider district of West Lindsey promoting the delivery of sustainable and affluent communities and improving the quality of life of residents as well as supporting the regeneration programme for Gainsborough.

Risk Assessment :

Key Risk: The success of this project is based on the timely delivery of the strategic traffic model so that it may be utilised effectively as part of the wider regeneration programme to facilitate the delivery of land use allocations (including sustainable urban extensions) identified in the emerging Central Lincolnshire Local Plan.

Mitigation: Ensuring that the project is managed robustly against the project plan, specifically in relation to the key milestones identified.

Climate Related Risks and Opportunities: The purpose of commissioning a new traffic modelling project is to improve traffic flows and access through the town and wider area, reducing the frequency and volume of queuing and idling traffic.

Title and Location of any Background Papers used in the preparation of this report:

Call in and Urgency:

Is the decision one which Rule 14.7 of the Scrutiny Procedure Rules apply?

i.e. is the report exempt from being called in due to urgency (in consultation with C&I chairman)

Yes

No

Key Decision:

A matter which affects two or more wards, or has significant financial implications

Yes

No

1 Introduction

The Council's regeneration plans for Gainsborough and wider area are predicated on housing led economic growth which is formalised through statutory obligations to seek to deliver the emerging Local Plan. The scale of housing growth required is very ambitious with Gainsborough accounting for 12% of the overall housing growth planned for Central Lincolnshire.

Due to the position of Gainsborough and its relationship with the Trent Bridge River crossing it is important to consider the impact of any growth in the town on the wider District. Gainsborough because of the river crossing is considered a key gateway providing access routes from South Yorkshire and Nottinghamshire to Scunthorpe and surrounding villages on A156, to Lincoln and surrounding villages on the A159 and finally a popular route from Sheffield and Rotherham to the Coast on the A631 through Market Rasen.

In February 2016 members approved a Regeneration Delivery Plan for Gainsborough, this included an outline project for infra-structure delivery. In May of this year the Homes and Communities Agency funded an infrastructure study for the town. As part of this regeneration programme Mouchel were commissioned by ALTAS (Part of the Homes and Communities Agency) and West Lindsey District Council to produce the Gainsborough Infrastructure and Planning Delivery Strategy (GIPDS). The purpose of the GIPDS was to set out a clear strategy for the delivery of key infrastructure required in Gainsborough in the emerging plan period up to 2036 to support an ambitious growth agenda for the town and ensuring connectivity to the wider district is supported and improved.

The Nexus Mouchel study however only offers a high level understanding of Gainsborough's future growth's impact on the local and wider transport network and as such it was recommended that in the short term a more coordinated approach to assessing the impact of development on the highways network is undertaken, making specific reference to using a strategic traffic model for the town to ensure the cumulative impact of growth is captured.

As a partner of Lincolnshire County Council, Mouchel have been invited to provide a proposal, including a methodology and fee structure to undertake a more detailed study of a number of development related transport issues in Gainsborough with a view to safeguarding the gateway routes from South Yorkshire and Nottinghamshire into the District of West Lindsey, focussing specifically on connectivity and traffic flows.

2. Context

As part of the Greater Lincolnshire devolution bid to Central Government in 2015 the 10 authorities commissioned Mott MacDonald to deliver a Greater Lincolnshire Strategic Infrastructure Delivery Plan (GLSIDP) with the core purpose of recommending how Greater Lincolnshire should prioritise and fund investment in infrastructure so as to realise the ambitious growth targets across the County.

The GLSIDP categorised 36 major infrastructure projects into short, medium and long term timeframes and used a multi-criteria analytical approach (MCA)

to assess the impact of projects based on the schemes costs and benefits. The methodology evaluated the strategic and economic impact of the project alongside the cost and deliverability of the scheme. It was determined that the Trent Bridge crossing from Flood Road onto Bridge Road/Bridge Street and Thorndike Way junctions were ranked 8th out of 36 demonstrating that this project was deemed both cost effective and appropriate, playing a key role in the delivery of the 4,350 homes proposed by the Central Lincolnshire Local Plan.

Alongside this work there has also been a further study into the Flood Road junction as part of the Local Development Order application. This study sought to establish whether a second river crossing was going to be necessary in order for the town to sustainably deliver the levels of growth allocated in the emerging Local Plan. The Traffic Assessment Study (June 2016) concluded that the Bridge would reach capacity by 2021, however it also provided alternative solutions to increasing capacity of the junction without the need for a second river crossing. The solutions proposed have helped provide developer confidence in the town and have finally confirmed that there is no need for a second river crossing.

Whilst it is acknowledged that devolution is currently no longer an option for Greater Lincolnshire we have been advised by the Commissioner for Place and Environment at Lincolnshire County Council that the methodology used to evaluate infrastructure projects remains the same and that it is important for projects detailed within the GLSIDP to continue development to ensure deliverability so that they can be considered for future funding. This approach has been demonstrated by the work undertaken previously by North Kesteven District Council who are now benefiting from £10m worth of road improvements in Sleaford following the commissioning of a Transport and Development Study.

The study proposed in this report goes further than just modelling solutions for the Flood Road, Bridge Road and Thorndike Way junctions, this is because it is acknowledged that whilst the Flood Road junction is a priority; ensuring traffic is also able to flow through the town is key to maintaining the economic benefits to the District via the primary routes to Scunthorpe, Lincoln and the coast.

3. Study Objectives and Project Approach

The purpose of the commission is two-fold:

- To enhance the work undertaken on the GIPDS for the Gainsborough area and to support the future development of the town, including attracting investors, by clearly identifying what transport infrastructure improvements are required to facilitate the delivery of the land use allocations identified in the emerging Central Lincolnshire Local Plan and improve connectivity with the rest of the district.
- To build on the assessment work undertaken for the Flood Road, Bridge Road and Thorndike Way junction; providing more detailed proposals for junction improvements culminating in the provision of a full Option Assessment Report.

The project will be managed through three primary work streams which are broken down into:

- Work stream 1 – Project Management and Information Collation
- Work stream 2 – Strategic Model Development
- Work stream 3 - Flood Road, Bridge Road and Thorndike Way junction scheme development

The model identified for this project will be the SATURN highway model which is based on methodology supported by the Department of Transport, providing two key benefits. Due to the model methodology used the study provides a robust basis for future funding bids and grant applications. It also allows enhanced options assessments of specific junctions or other modes of transport e.g. cycling and walking to be overlaid ensuring a cohesive strategy which also considers the cumulative impact of development and traffic volumes.

4. Project Plan

Work stream	Stage	Product	Description	Week
1	Inception	Inception meeting	-	Week 3, January 17
		Project Initiation Document (PID)	Sets out key project management structures and processes for the project	Week 4, January 17
		Programme	Detailed programme for full project	Week 4, January 17
2	Strategic Model Development	Model Specification Report (MSR)	Sets out the detailed specification of the traffic model (this is a live document that is updated as the project progresses)	Week 2, February 17
		Traffic Data Collection Specification	Forms the basis for procuring traffic surveys	Week 2, February 17
		Traffic Data Collection Tender Documentation	Tender documentation for appointing survey contractors	Week 2, February 17
		Traffic Data Collection Report	Report on the process and outputs from the traffic survey	Week 2, April 17
		Local Model Validation Report (LMVR)	Key document reporting on the model development process and adherence of the model performance to required standards	Week 4, July 17
		LMVR Appendices (requirements TBC): <ul style="list-style-type: none"> • Network coding • Demand data processing • Calibration and validation statistics • Journey Time validation • Realism tests 	LMVR supporting documentation	Week 4, July 17
		Uncertainty Log (Core scenario future network and development assumptions for each forecast year)	Log of committed and planned highway network and land use changes over the forecast years	Week 4, August 17
		Forecasting Report (FR)	Report of the traffic forecasting process and outputs	Week 4, October 17
		FR Appendices (requirements TBC): <ul style="list-style-type: none"> • Demand Model responses 		Week 4, October 17

		<ul style="list-style-type: none"> Reference Case statistics 		
3	Flood Street Scheme Development	Working Paper 1 – The Need for Intervention	Reporting on the early stages of Work stream 3 including current and future situations, the need for intervention and scheme objectives	Week 4, October 17
		Working Paper 2 – Option Identification and Initial Sifting	Reports on the long list of options and the sifting process to select a shortlist for further development	
		Option Assessment Report (OAR)	Overall output from Work stream 3 including development of preferred option/s	Week 4, March 18
		OAR Appendices (requirements TBC): <ul style="list-style-type: none"> EAST (or other sifting tools for long-list and short-list) Do Something Scheme Performance (Flood Street Junction Improvements) Junction Model interface EAR (see below) Environmental Constraints mapping Scheme Costs Highway Design feasibility 	OAR supporting documentation	Week 4, March 18
		Economic Assessment Report (EAR)	Reports on the outputs from the economic assessment of the scheme/s	Week 4, March 18
		EAR Appendices (requirements TBC): TUBA user benefits COBALT Accident impacts	EAR supporting documentation	Week 4, March 18
		Stakeholder Report	Reports on stakeholder engagement undertaken during the commission	Week 4, March 18
All	All	Monthly Progress Report	-	Week 4 each month

5. Project Costs

Below are the anticipated costs for the study outlined above.

Work stream		Fee
Work stream 1 – Project management & information collection		£18,500
Work stream 2 – Strategic model	Traffic modelling	£146,000
	MPOD data (Allowance)	£5,000
	Traffic surveys (Allowance)	£35,000
Work stream 3 – Flood Road, Bridge Road & Thorndike Way Junction		£65,750
	Total	£270,250

The Authority has successfully secured grant funding from the Greater Lincolnshire Local Enterprise Partnership for the Housing Unlocking fund for £4million as part of the Gainsborough Growth Programme. £1.85 million of this is earmarked to accelerate the delivery, specifically in relation to infrastructure. This allocation will be used to fund this study removing any cost liability to the authority.

Along with the grant funding we have also negotiated with Lincolnshire County Council for them to help client this work, with a view to providing specialist knowledge to support the project management element of this study. This in kind benefit provides approximately £5,000 worth of consultancy fees.

Overall this study provides good value to the Authority, not only will it deliver a much needed set of solutions for the Trent Bridge crossing ensuring the gateway to the district remains fit for purpose, supporting economic migration and tourism but will also facilitate the delivery of the wider regeneration programme for Gainsborough.

This page is intentionally left blank



**Corporate Policy and
Resources Committee**

13th April 2017

Subject: Commercial Delivery Plan 2016 Annual Review

Report by:

Manjeet Gill

Contact Officer:

Manjeet Gill
Chief Executive
01427 676500
manjeet.gill@west-lindsey.gov.uk

Purpose / Summary:

This report brings the annual review of the Commercial Delivery Plan agreed in November 2015 by Council.

It also summarises future themes as a result of reviews in December 2016, when the Commercial Director role was discontinued to focus management roles and therefore resources, on delivery themes now that the Commercial Plan and future business plans have been established over 2016.

Those themes are, External Funding, Commercial Investments Portfolio, Commercial Community Projects (such as Leisure Provision), Growth and Regeneration, continued development of Commercial capability.

RECOMMENDATIONS:

It is recommended that:

1. Committee approve the Commercial Delivery Plan review
2. Committee advise on future governance as outlined in Section 5.3 and 5.4.
3. Committee approve the future delivery themes as outlined in Section 5.2

IMPLICATIONS

Legal:

Governance to ensure decisions are safe, is regularly reviewed, with emphasis on role of Monitoring Officer, Section 151, Director and Committee.

Monitoring Officer Comments

The law regarding the ability to trade for Local Authorities is contained in:

- Section 1 of the Localism Act which gives Local Authorities the General Power of Competence to do anything an individual can do as long as there is no express statutory prohibition against it; or
- Section 1 of the Local Authority Goods and Services Act which allows Councils to carry out and charge for Professional, Technical and Administrative services for other defined public bodies.

Each project will need to be reviewed by the Monitoring Officer to ensure that the proceedings are legally safe and that an appropriate delivery model is used for project.

Where necessary changes to the Council Constitution will need to go through the normal governance for such amendments.

Financial : FIN/5/2018

S151 Officer Comments

The Commercial Plan is intended to guide the Council's activity in generating income and contributing to overheads whilst achieving value for money. In addition to supporting the Council's ambition of financial self-sufficiency. The Commercial Plan is intended to make a contribution to closing this 'funding gap' as Government grants reduce.

The Council established an Invest to Earn Fund (earmarked reserve) of £1m for 2015-2020. The Invest to Earn Fund helps finance the development of commercial projects and proposals including research and development activity such as market analysis, sales opportunities, to support the development of project business cases. There remains a balance of £0.615m as at 31.3.2017

This report comments on some growth and regeneration projects and in particular the Hotel Development. This project was not in the original Commercial Plan. It was introduced to the capital programme during 2016/17 and was supported by the Growth and Regeneration earmarked reserve. The Growth and Regeneration earmarked reserve has a balance of £5.5m as at 31.3.2017

Staffing :

New staff roles and changes have been outlined in the report.

Equality and Diversity including Human Rights :

Risk Assessment :

A key role is effective PolITICAL Governance and ensuring members have seen all information necessary to make decisions.

Climate Related Risks and Opportunities :

Commercial Energy Projects can help meet this.

Title and Location of any Background Papers used in the preparation of this report:

Call in and Urgency:

Is the decision one which Rule 14.7 of the Scrutiny Procedure Rules apply?

i.e. is the report exempt from being called in due to urgency (in consultation with C&I chairman)

Yes

No

X

Key Decision:

A matter which affects two or more wards, or has significant financial implications

Yes

No

X

1.0 EXECUTIVE SUMMARY

- 1.1 To share with Committee the update on the Commercial Delivery Plan for 2016/17. The Plan has been appended to this report (Appendix 1). The report also outlines future themes and governance arrangements. A list of achievements and progress is also highlighted.
- 1.2 The Commercial Delivery Plan for the year was approved in November 2015 by Council as part of its annual process of delivery for the Commercial Plan.
- 1.3 A Commercial Member Steering Group was established in 2016. Its Terms of Reference are appended (Appendix 2). This group has provided advice, challenge and steer to shape key decisions that come to Committee. Examples are:
 - Surestaff - Company acquisition
 - Gainsborough Hotel proposal
 - Business Proposals
 - Commercial Investment Portfolio
 - Commercial Projects

2.0 ACHIEVEMENTS

- 2.1 In our quest for continual improvement and assurance of risk and value for money, we must not lose sight of the achievements and how they inform learning.
 - a) Commercial Plan, business cases and cultural awareness of commercial approaches developed. The foundations before quality delivery.
 - b) Acquisition of an external company to reduce costs to the Council with net benefits to Council expected to exceed £100,000 by year 3.
 - c) External Funding from 2016/17 year – indicative bides of circa £6 million have been announced. These will be subject to the GLEP and other funders such as the Homes and Communities Agency, the Lotter etc to help bring more money into the District and to enable Councils funds to be invested on other projects or utilised to lever in further funding.
 - d) Trading in areas such as Trade Waste and Business Improvements has increased our income compared to 2015/16.
 - e) Development of our talents 'growing our own'. Managers have been promoted to new roles such as Strategic Manager Trading and Environmental Operations, Community Commercial Investment Programmes Manager and Commercial & Economic Growth Director and in the process, making efficiency savings by merging vacant and existing roles of over £100,000.

2.2 Commercial Member Steering Group

The Commercial Member Steering Group has reviewed delivery and it has been agreed their focus and that of Committees should be to ensure safe value for money delivery with timely decisions. In areas where delivery may need further acceleration, more governance will be required or where business results anticipated are not being achieved, to stop, to learn and refocus on other areas and prevent further unnecessary resources being deployed. In addition potential for future conflict with some Members was highlighted.

The Terms of Reference need to be reviewed by Committee and recommendations made, taking into account the overall direction for Commercial Plan priorities and governance matters such as risk management and Member conflict.

2.3 Financial, Risk and Legal Governance

Independent advice has been deployed to provide assessments of proposed decisions for projects such as the hotel, town centre, joint venture procurement etc. In addition a review has taken place for certain projects especially one that has been delayed and to ensure appropriate governance and programme management resources are in place.

This area together with a review of governance of programmes, roles and procedures, will be the subject of a future report as relevant, once those reviews have identified further improvements needed. At this stage these are reviews for the Chief Executive and her management team. This report seeks to assure Committee that the Chief Executive is undertaking the second line of assurance as part of her duties to inform Council's third line of assurance, Members and External Audit.

3.0 Review

3.1 A review of the Commercial Delivery Plan took place last Autumn and in December it was decided by the Chief Executive, in her capacity as Head of Paid Service along with decisions by the Chief Officer Committee that;

- a) Future roles and resources would focus on delivery at management levels. Therefore we did not now need a Director role, as at Director level, the role of developing a Commercial Plan and arrangements was no longer now the priority as focus and delivery (the Direction) established.
- b) Effective and the right resources were needed to support actual delivery performance management and oversight of results delivered and especially the management of high risk investment programmes.
- c) The further support and development of Committee and Member role to ensure they were able to make decisions based on adequate

information, assessment of risk to support the delivery of the Council's ambitions and ensure safe value for money decisions.

4.0 Moving forward – 2017/18 Focus

4.1 2017-18 the focus will be about delivery of the projects agreed in Delivery Plans or by Committee otherwise.

4.2 Future Themes

4.2.1 The future themes are based on the key delivery priorities and business cases decided in the Council's Commercial Plan. The proposed themes have now been organised based on individual strategic responsibilities at an officer level and for assurance to Committee and Council on the resource allocation and roles to ensure delivery. Note:

4.2.2 As Head of Paid Service, the Chief Executive is responsible for accountability and appropriate revisions to roles for officers as the Council progresses on its journey that is influenced much by external factors such as changes in legislation, reduction or refocus of Government grants or what Government expect of local Government in the legislation if changes to prescribe how we can or cannot act and where we are given a statutory duty the need to ensure resources are devoted to those areas first.

4.2.3 Key themes, Strategic Manager Trading and Environmental Operations

a) Trading – to increase surplus as a contribution towards our net cost of services. For example, we may need to provide statutory waste services but we can reduce the costs by bringing in income from services such as Waste Services to businesses (Trade Waste) which also offers other benefits in helping our business to thrive and trade with other services of the Council.

Services such as;
Trade Waste
Surestaff – agency staff for seasonal work
Leisure Centres
Trinity Arts

All provide examples of where they can generate income and therefore reduce reliance on other areas being reduced to balance Council budgets when Government grants have been reduced substantially since 2010 due to austerity policies.

b) Community Commercial Projects – Community Commercial Investment Programmes Manager

These are projects (other than regeneration and growth projects, a separate theme) that require careful risk and programme management as well as focus on commercial return.

The key projects are:

- Leisure Centre Services Procurement and future provision at nil subsidy by Council
 - Community projects that have social as well as commercial benefits as the basis for the business case decision.
- c) Growth and Regeneration – Commercial & Economic Growth Director

These are Land and Property related growth projects that are predominately focussed on Gainsborough. The Local Plan sought to reduce uncontrolled impact on fringe villages and therefore to focus growth on Gainsborough and to ensure sustainability of the Districts main town.

Key programmes of work are, the Gainsborough Regeneration programme that includes:

- Housing Zone Sites (other than listed below)
- Urban extensions
- Town Centre Joint Venture
- Hotel Development
- Heritage and Public Realm
- The Gateway site

d) Commercial Investment Portfolio – Corporate Director of Resources

This is as per the Commercial Plan and Commercial Delivery Plan for 2016/17 and about increasing the Council's Commercial Land and Property portfolio in order to generate a return (revenue) that would address reductions in our overall revenue budget due to cuts in Government grants.

4.3 In line with a Commercial approach as is the case with businesses and reinforced by Commercial Member Steering group, it is proposed we are more focussed on tracking ability to delivery projects proposed by business cases and business development. Regular reviews at key stages must ask the question.

- Is the business case still valid?
- Is further expense in development justified against evidenced benefits and returns?
- Should we stop/continue/continue but with a change in original business case.

4.4 **Member Governance**

It is proposed that Committee review the role of the Commercial Member Steering Group, should this be rethought?.

As far as possible all business should be via Public Committees in the principle of Public Interest and transparency balanced with what maybe warranted to be exempt due to reasons of commercial or legal reasons.

Same options are Prosperous Communities Committee monitor;

- a) Trading Services progress and results
- b) Community Projects progress as the committee with the policy and budget responsibility for these areas.

Corporate Policy and Resources receives six monthly reports, and an annual review of all themes in addition to any specific project reports that may require decisions.

The **Commercial Member Steering Group** has provided constructive governance to steer quality reports and decisions. A view is needed from Committee on the role of any future member steering group and its current Terms of Reference are attached at Appendix 2, and can be built upon. One option is to focus on Land and Property – Growth and Regeneration Programmes. This will need consideration as to how governance can be effectively discharged by the Council member process of advice and steer outside of Committee processes as the purpose is to inform and aid effective Committee decisions.

Appendices

Appendix 1 – Commercial Delivery Plan

Appendix 2 – Commercial Steering Group Terms of Reference

Commercial Plan 2015 to 2020

Delivery Plan - 2016/17

Progress Update

ST1: Generating greater income from the council's services through charging, trading and investment (in order to reduce the net subsidy for each service)

Theme	Responsible Officer	Milestones	Due Date	12mth Update	RAG
ST1.1 Reviewing the trading and income potential of all services	Ady Selby	<ul style="list-style-type: none"> • 2016/17 Business plans to identify income generation opportunities • Systematic review of traded services in delivery • Business Planning review for savings/income 2017/18 • "Closer to the customer" review 	October 2016	2017/18 business planning underway and identifying further income generation activity	Green
				Business Plan in place for Surestaff and being developed for Trading Co	Amber
				Review of Commercial Waste complete-business plan for 2017/18 in draft	Amber
				Other services being evaluated in Exceeding Expectations forum	Green

Theme	Responsible Officer	Milestones	Due Date	12mth Update	RAG
<p>ST1.3 Developing a systematic approach to customer insight, market analysis and environmental scanning for business opportunities</p>	Michelle Carrington	<ul style="list-style-type: none"> • Experian Mosaic has been used as a customer segmentation for several initiatives • Establish effective corporate approach to capturing and analysing customer intelligence and management information as part of the “closer to the customer” programme 	<p>March 2017</p> <p>November 2016</p>	<p>This activity has been deferred due to the delay in commencing the “Closer to the Customer” programme.</p> <p>The decision was made to hold off renewing the Mosaic licence due to lack of analytic skills and capacity to undertake customer insight; and until a clearer understanding of what customer insight requirements and information is required; and how Mosaic can support that agenda.</p>	Amber

Theme	Responsible Officer	Milestones	Due Date	12mth Update	RAG
ST1.4 Establishing an 'Invest to Earn' fund to stimulate business development	Ady Selby	<ul style="list-style-type: none"> All services aware of 'invest to earn' funding Funding drawn down to support development of commercial project(s) 	March 2017	Invest to earn fund in place, services aware Funding drawn down to support Surestaff, Commercial Waste, etc.	Green
ST1.5 Establishing effective financial systems for trading services to help manage direct and indirect costs	Alan Robinson	<ul style="list-style-type: none"> Payment systems reviewed further to facilitate customers' payment preferences with variable/flexible invoicing 	June 2016	An enhanced invoicing facility has been procured and is currently at the implementation phase. The new system is due to go live in April 2017.	Amber

Theme	Responsible Officer	Milestones	Due Date	12mth Update	RAG
		Trading and income reviewed regularly for established Commercial Projects	Quarterly as a minimum		
ST1.6 Establishing appropriate charging policies (fees and charges) that balance the need for full-cost recovery with market sensitivity and legal constraints	Alan Robinson	<ul style="list-style-type: none"> • Fees and Charges reviewed • Pricing/Trading approach reviewed. 	December 2016	This has been incorporated into the fees and charges process for the 2017/2018 year.	Complete

Theme	Responsible Officer	Milestones	Due Date	12mth Update	RAG
ST1.7 Developing alternative service delivery models as appropriate	Michelle Carrington	<ul style="list-style-type: none"> Options for service delivery models considered as part of individual commercial project business cases 	March 2017	This has been included for services within the Customer Cluster; such as Building Control. Further review will be undertaken during the service reviews under the Closer to the Customer programme.	Green

ST2: Securing greater external funding for the council and the district

Theme	Responsible Officer	Milestones	Due Date	12mth Update	RAG
<p>ST2.1. Developing a pipeline of strategic projects that can secure external funding</p>	<p>Eve Fawcett-Moralee</p>	<p>Implement capital programme:</p> <ul style="list-style-type: none"> • Gainsborough Housing Zone, Hemswell Cliff Food Enterprise Zone and Gainsborough Growth Infrastructure. • One Public Estate Feasibility • Joint venture to improve Caistor • GP/health facilities. 	<p>March 2017</p>	<p>£4m SLGF3 to be announced Feb17 – unlocking housing Business cases and funding bids being developed to HCA Builders finance fund for Albion works and RGW.</p> <p>£1.6m SLF3 now looking at delivery options and agri-food strategy</p> <p>£10k feasibility funding achieved work underway. £100k bid for public sector hub Gainsborough decision awaited</p> <p>Little movement from the NHS property services. Now being reviewed as part of OPE</p> <p>EFM working with a GP training practice to set up new premises on JC/commercial basis</p>	<p>Green</p>

<p>ST2.2 Establishing an approach for encouraging and approving external funding bids</p>	<p>Ian Knowles</p>	<ul style="list-style-type: none"> Establish staff resources for coordinating and developing external funding bids 	<p>June 2017</p>	<p>Bids are developed as opportunities arise. Coordinated through Grant White supported by Finance where needed.</p>	<p>Green</p>
--	--------------------	---	------------------	--	--------------

Theme	Responsible Officer	Milestones	Due Date	12mth Update	RAG
		<ul style="list-style-type: none"> Amount of external funding reported through P&D as KPI 		YTD figure to be added	
ST2.3 Developing and influencing networks to maximise opportunities and success in securing external funding.	Eve Fawcett-Moralee	<ul style="list-style-type: none"> Regular stakeholder meetings held. Further develop networks to maximise horizon-scanning and potential opportunities 	Monthly Right cont'd: add HIG and SIDP prioritization of Gainsborough traffic study/capacity 6 th in Greater Lincs. Acknowledge fall out from DEVO on housing pipeline work ST engaged in?	Input into GLLEP board meetings via comments to District Rep plus regular catch ups with Director. Met with GLLEP Chair December 16. Quarterly meetings Lead County Cllr Colin Davy. Regular working with Team Lincs – Inward investment. Attendance at MIPIM UK and projects at MIPIM. Dialogue with HCA – local reps bi monthly and regional director. Established relationship with new fund leaders re: Infrastructure and builders finance. Place board. Continuous market engager	Green

<p>ST2.4 Maximising the leverage from the council's external funding activities</p>	<p>Mark Sturgess</p>	<ul style="list-style-type: none"> Regularly monitor and report value of additional resources leveraged through council grant/loan funding 	<p>Quarterly</p>	<p>Not started. Needs to be properly incorporated in the Progress and Delivery process. Annual position for 2016/17 is Grants awarded: 127 Amount awarded: £124,668.16 Amount levered/matched: £1,012,210.14</p>	<p>Red</p>
--	----------------------	---	------------------	---	------------

ST3: Increasing capital and revenue returns to the council through delivering housing and economic growth.

Theme	Responsible Officer	Milestones	Due Date	12mth Update	RAG
<p>ST3.1 Developing and delivering a land and property programme (capital development programme) to add value and diversify the Council's property portfolio.</p>	<p>Karen Whitfield – only for Crem should be EFM going forward</p>	<ul style="list-style-type: none"> Land and Property Management Plan implemented – being reviewed by EFM and new structure on and A <p>Add OPE here</p>		<p>Could say Development partnership addressing – looking JV approach to development/growing our own assets</p> <p>Project to develop crematorium underway. Suitable land is being identified and project team assembled. Project support agreed by Daventry DC and support/joint working possibilities with Doncaster BC.</p>	<p>Red Note PS/ST didn't progress beyond the Crem</p>

<p>ST3.2 Strengthening the council's approach to estate management (including facilities management) to maximise surplus and return on investment.</p>	<p>Eve Fawcett-Moralee</p>	<ul style="list-style-type: none"> • Internal Audit review of asset management completed and reported to Committee • Planned maintenance programme established 	<p>July 2016</p> <p>January/ February 2016</p>	<p>Delayed by P and A restructure</p> <p>Underway</p>	<p>Red</p> <p>Amber</p>
---	----------------------------	--	--	---	-------------------------

Theme	Responsible Officer	Milestones	Due Date	12mth Update	RAG
	Ian Knowles	<ul style="list-style-type: none"> Recruit resources (as appropriate and subject to approval) to support land and property management Commission and procure the development and management of a commercial investment portfolio (subject to member approval) NOTE IK PROJECT SPONSOR/EFM SUPPORT 	<p>July 2016</p> <p>December 2016</p>	<p>As above</p> <p>Revised strategy to be taken to April committee</p>	<p>Red</p> <p>Amber</p>
ST3.3 Establishing a housing company to develop, own and manage new homes and return empty properties to use	Eve Fawcett-Moralee	<ul style="list-style-type: none"> Housing Company business case considered by Committee Establish Housing Company 	<p>May 2016</p> <p>July 2016</p>	Business case not proven; pursuing via development partnership project	If can change to development partnership this can be green – as far as I am aware this was never approved??

Theme	Responsible Officer	Milestones	Due Date	12mth Update	RAG
ST3.4 Stimulating business growth and investment by implementing the district's Economic Development Delivery Plan	Eve Fawcett-Moralee	<ul style="list-style-type: none"> Implement Capital Programme 	March 2017	Skills partnership established. Setting new Employers group aligned to industrial strategy. Highly successfully see benefits realized	Green
		<ul style="list-style-type: none"> Develop and implement targeted marketing strategy 	October 2016		Green
		<ul style="list-style-type: none"> Adopt Local Development Orders for Food Enterprise Zone and additional Housing Zone site 	March 2017	To PC committee 31.1.17 adopt for consultation	Green
		<ul style="list-style-type: none"> Implement Gainsborough Growth Delivery Plan 	March 2017	New JVco Market St. renewal enacted 20.2.17 £250k private sector investment Plus development partnership	Green

ST4: Enhancing the council's commercial culture and capability

Theme	Responsible Officer	Milestones	Due Date	12mth Update	RAG
<p>ST4.1 Developing a communications and engagement plan to involve all staff and members in the council's commercial approach</p>	<p>Ady Selby</p>	<ul style="list-style-type: none"> Implement programme of regular Commercial sessions. 	<p>March 2017</p>	<p>Aspire sessions organized and in delivery, staff aware and engaged in commercial aspirations</p>	<p>Green</p>
		<ul style="list-style-type: none"> Commercial updates included in Corporate Updates 	<p>March 2017</p>	<p>Commercial updates included in next round of Corporate update.</p>	<p>Amber</p>
		<ul style="list-style-type: none"> Review Commercial Member Steering Group and membership 	<p>May 2016</p>	<p>Membership was reviewed and Cllr Kinch was added at Annual Council</p>	<p>Complete</p>

Theme	Responsible Officer	Milestones	Due Date	12mth Update	RAG
		<p>Commercial Plan progress update considered by Corporate Policy and Resources Committee</p> <ul style="list-style-type: none"> Commercial Plan annual review in line with MTFP and updated delivery plan considered by Full Council 	<p>March 2017</p> <p>March 2017</p>	<p>Due to April Committee</p> <p>Actions Summarised in the MTFP</p>	<p>Amber</p> <p>Green</p>

ST4.2 Establishing a development programme for staff and elected members as part of the people strategy that underpins the council's commercial ambitions	Alan Robinson	<ul style="list-style-type: none"> • Finance Matters 2 training rolled-out 	June 2016	Finance Matters II has commenced and includes specifics on Commercial management as well the general financial literacy which is essential for commercial activity	Amber
		<ul style="list-style-type: none"> • Review of member development programme to support commercial ambitions 	April 2016	Member Development plan is in place	Complete
		<ul style="list-style-type: none"> • Commercial competencies as part of annual staff appraisals 	June 2016	Appraisal include commercial competencies under the Creative and Business Smart theme	Complete

Theme	Responsible Officer	Milestones	Due Date	12mth Update	RAG
ST4.3 Strengthening corporate systems and processes to support the council's commercial activities.	Ian Knowles	<ul style="list-style-type: none"> Review approach to project/programme management 	June 2016	A review has been undertaken regarding how we approach programme management and a change to the Board structure has introduced a RACI approach. We are currently working with sponsors and project leads to ensure good programme/project management continues.	Amber
		<ul style="list-style-type: none"> Business planning process to encompass commercial/income generation proposals 	October 2016	Business Planning for 2017/18 included a specific requirement for commercial options to be considered alongside efficiencies	Green

Theme	Responsible Officer	Milestones	Due Date	12mth Update	RAG
		<ul style="list-style-type: none"> Implement systems improvements to financial processes as required 	March 2017		
ST4.4 Ensuring that the council's commercial activities are resourced appropriately.	Ady Selby	<ul style="list-style-type: none"> Recruit resources required to support commercial activities and delivery 	June 2016	Exceeding Expectations group in place, Aspire delivering. Support in place for business cases and Invest to Earn for delivery	Amber
		<ul style="list-style-type: none"> All commercial business cases to consider staffing implications of project development and implementation 	March 2017	Business cases consider staffing implications. EB and EE groups provide some challenge	Amber

COMMERCIAL MEMBER STEERING GROUP TERMS OF REFERENCE

1 Context

West Lindsey District Council has agreed a Corporate Plan that with other priorities promotes the entrepreneurial approach whilst delivering robust governance and decision-making. This document sets out the Terms of Reference for the Commercial Member Steering Group which will exercise its role within the policy and governance framework set by West Lindsey District Council in order to support delivery of the Commercial Plan and its contribution to the Corporate Plan.

2 Purpose/Objectives of the Commercial Member Steering Group

The purpose of the Commercial Member Steering Group is to provide strategic advice, guidance and support to officers in the development, implementation and delivery of the Council's commercial plan and associated work programme.

The Commercial Member Steering Group will review progress on implementing the Commercial plan in line with the four strategic themes:

- Developing the trading potential of Council Services
- Optimising the use of external funding
- Optimising the capital and revenue returns generated from land and property assets
- Developing a more commercial culture

3 Operating Principles

The Commercial Member Steering Group will adopt the following principles:

1. The Steering Group will work together collaboratively to oversee and guide the Council's commercial approach;
2. The Steering Group will respect the Commercial Confidentiality of discussions.
3. All Members of the Steering Group will adhere to the Code of Conduct and Constitution.
4. The Steering Group will follow the Council's agreed policies for procurement, land and property acquisition and disposal, and programme and project management.
5. The Steering Group has been established by Council with joint membership from Corporate Policy & Resources Committee and Prosperous Communities Committee.

4 Meeting Frequency

The Steering Group will meet as often as is required to administer its functions in an effective, efficient and economical manner. However, it is anticipated that the Steering Group will meet quarterly. Papers to be considered by the Board will be available for circulation 24 hours prior to the meeting, or due to the commercial sensitivity tabled on the day of the Steering Group, unless with prior agreement from the Chair of the Steering Group.

5 Governance

The Commercial Member Steering Group is not a decision-making body. Decisions relating to the commercial plan and associated activities will be made by Corporate Policy and Resources Committee and Prosperous Communities Committee as appropriate.

6 Commercial Member Steering Group Membership

The Commercial Member Steering Group comprises 2 representatives nominated from Corporate Policy & resources Committee, 2 representatives from Prosperous Communities Committee and any additional Members member of Challenge and Improve (Cllr Kinch as agreed at Council) Nominations are made annually at Annual Council.

Where possible, the Steering Group should include cross-party representation.

The Commercial Member Steering Group will nominate a Chair for the year. This position will be reviewed annually.

For a meeting to convene a quorate of a minimum of one member from P&R committee and one member of PC Committee are in attendance or represented.

The Commercial Member Steering Group will be advised and supported by the Commercial Director, Director of Resources, Chief Executive and Monitoring Officer. Other officers may attend meetings as appropriate.

7 Review

The operation and success of the CMSG will be the subject of an annual Review, to be conducted by the CMSG and considered at the first meeting in each financial year. The outcome of each review will be reported to Annual Council for consideration.

This page is intentionally left blank

Corporate Policy & Resources Committee Work Plan

Purpose:

This report provides a summary of reports that are due on the Forward Plan over the next 12 months for the Corporate Policy & Resources Committee.

Recommendation:

1. That members note the schedule of reports.

Date	Title	Lead Officer	Purpose of the report
04/05/2017	Budget and Treasury Management Monitoring Q4	Tracey Bircumshaw	To present budget monitoring and Treasury Management information as at the end of period 4 and the outturn position
	Progress and Delivery Q4	Mark Sturgess	To present Progress and Delivery (Projects and Services) monitoring information to the end of Period 4
	Development Loan	Ian Knowles	To approve a commercial loan for the development of land in support of the Local Plan. Market loan to enable works for the housing delivery
	Rural Transport Programme	Grant White	To present Rural Transport programme and seek approval for specific projects and initiatives. Activity approval required from PCC and budget approval required from CP&R.
	Revised Committee Timetables 2017-2019	Alan Robinson	To arrange additional meetings to accommodate Q4 reports before Annual Council
15/06/2017	ICT Strategy	Ian Knowles	To present the ICT Strategy for approval
	Commercial Property Portfolio	Ian Knowles	To seek approval for the acquisition of a commercial property portfolio in line with the capital programme and Medium Term Financial Plan.
	Housing Strategy	Diane Krochmal	to present the new Housing Strategy for approval
	Managed Workspace: Revised Proposal	Joanna Walker	Seeks member support for a revised proposal for managed workspace on an alternative site in Saxilby. This is due to difficult ground conditions inflating construction costs and therefore the offer to the Council on the original site (agreed in October 2016).
	REVIEW OF CAR PARKING STRATEGY	Eve Fawcett-Moralee	to review the car parking strategy in accordance with brief provided by Chief Operating Officer .
	Potential Land Acquisition - Gainsborough	Elaine Poon	Confidential
27/07/2017	Annual Health and Safety report	Kim Leith	Summary of Performance of the Health and Safety Service throughout the Authority
	annual fraud report	Carol Bond	to present the annual report focussing on the commercial side of the service, income generated etc

	Review of Flexi-Time Policy	Emma Redwood	To review the council's Flexi-Time policy and update accordingly
21/09/2017	Market Rasen Car Parking	Eve Fawcett-Moralee	To provide an update on the impact of introducing car parking charges in Market Rasen
	Review the Relocation Policy	Emma Redwood	To review the Council's Relocation Policy
11/01/2018	Leisure Contract Procurement	Karen Whitfield	To update Members on the conclusion of the leisure contract procurement exercise and to approve the preferred contractor
