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: • 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 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

			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."
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

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

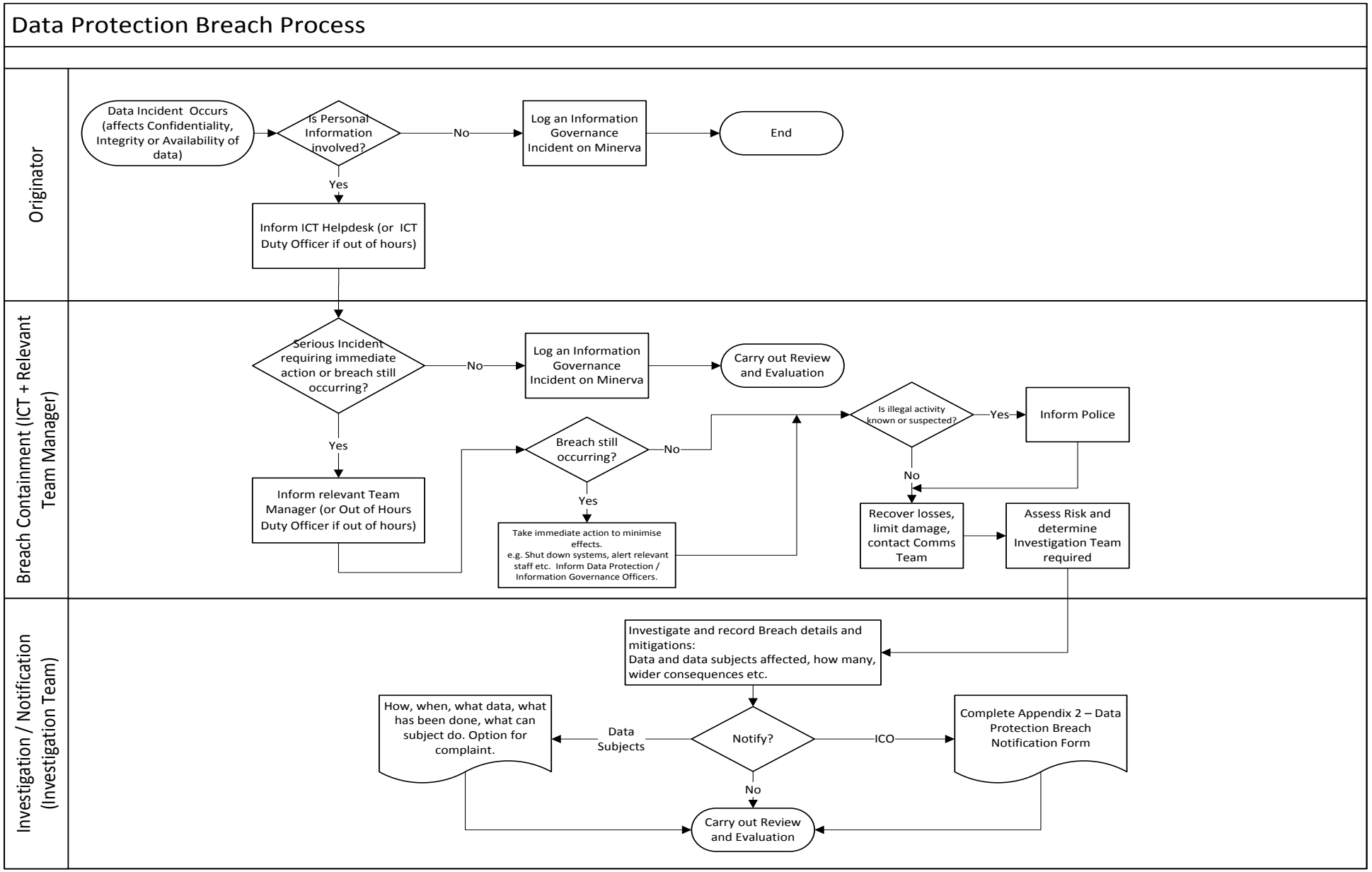
11.1. This policy takes effect immediately. All managers should ensure that staff are aware of this policy and its requirements. If staff have any queries in relation to the policy, they should discuss this with their line manager, the Information Governance Officer or the People and Organisational Development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



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)

West Lindsey DISTRICT COUNCIL
The Entrepreneurial Council

Information Governance

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

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 proving 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.

West Lindsey
DISTRICT COUNCIL
The Entrepreneurial Council

Information Governance

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?

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.

West Lindsey
DISTRICT COUNCIL
The Entrepreneurial Council

Information Governance

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

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).

West Lindsey
DISTRICT COUNCIL
The Entrepreneurial Council

Information Governance

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

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 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 whist 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.

West Lindsey
DISTRICT COUNCIL
The Entrepreneurial Council

Information Governance

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

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.

West Lindsey
DISTRICT COUNCIL
The Entrepreneurial Council

Information Governance

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

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.

West Lindsey
DISTRICT COUNCIL
The Entrepreneurial Council

Information Governance

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

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.

West Lindsey
DISTRICT COUNCIL
The Entrepreneurial Council

Information Governance

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	

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 the 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	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. Examples of common information security incidents are given in Appendix 1.
Information	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.
Confidential Information	The definition of confidential information can be summarised as: ▪ 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			
Urgency		High	Medium	Low
	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

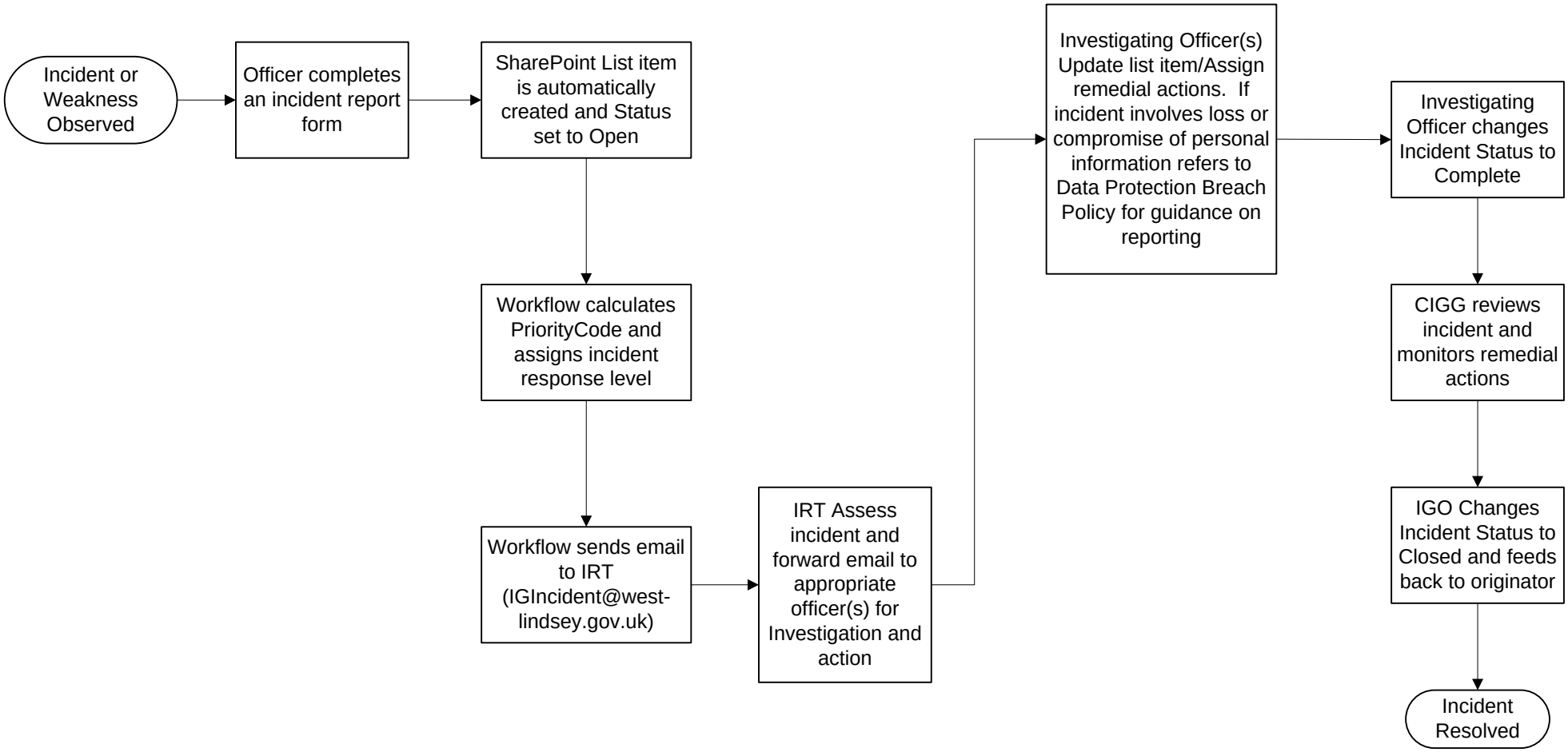
To learn from incidents and improve the response process incidents must be recorded and a Post Incident Review conducted. This is the responsibility of the Corporate Information Governance Group (CIGG) which is chaired by the SIRO. The following details must be retained:

- 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



West Lindsey
DISTRICT COUNCIL
The Entrepreneurial Council

Information Governance

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

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:	

West Lindsey
DISTRICT COUNCIL
The Entrepreneurial Council

Information Governance

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

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

West Lindsey
DISTRICT COUNCIL
The Entrepreneurial Council

Information Governance

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

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 accidently 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 accidently 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	• 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.