Corporate Policy and Resources Committee
27 October 2016

Subject: Introduction of Information Policies

Report by:	Director of Resources
Contact Officer:	Steve Anderson Information Governance 01427 676652 Steve.anderson@west-lindsey.gov.uk
Purpose / Summary:	To introduce 3 new policy documents to support the Council's compliance with information-related legislation

RECOMMENDATION(S):

That members, approve the attached Information Governance Policy, Legal Responsibilities Policy and Information Sharing Policy for formal adoption.

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

IMPLICATIONS

Legal: These new policies demonstrate our understanding of, and commitment to, the legal framework that governs the management of information.

Financial : None – FIN/74/17

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**

The Council has, over many years, developed and maintained a framework of policies relating to Information Compliance, Information Rights, and Information Security. This report introduces 3 new policy documents that:

- demonstrate our understanding of and commitment to information governance;
- we will use to inform and govern our business processes and procedures; and
- set the standards of information management our staff and partners must attain and maintain.

2. **The Policies**

a. Information Governance Policy

The Information Governance Policy demonstrates the Council's commitment to protecting and managing information securely and effectively and to reducing the risks to the Confidentiality, Integrity, and Availability of its information assets.

The Policy sets out how the Council will organise its activities around 6 strands to achieve the objectives of information governance:

1. Risk Management;
2. Key Policies;
3. Information Governance Roles and Responsibilities;
4. Key Bodies;
5. Staff Information Security Awareness; and
6. Information Security Incident Management.

The Policy describes, at a high level, the key elements within these 6 governance strands and ensures continuous improvement of the whole function by mandating an Information Governance Improvement Plan. This plan will be monitored and progressed by the Corporate Information Governance Group (CIGG) and reported to GCLT 6-monthly.

b. Legal Responsibilities Policy

There is a plethora of legislation and regulations governing how we must collect, protect, and manage information. The Legal Responsibilities Policy lists the relevant legislation and outlines the risks to the Council (and in some cases, individuals) for failing to comply.

The Policy sets out in general terms what the Council and its employees need to do to comply with each piece of legislation. It is not intended to be a comprehensive reference of information law but it does demonstrate that the Council understands the legal framework in which it operates and is working to manage the risks to itself, its employees and partners, and its customers.

c. Information Sharing Policy

As a Data Controller under the Data Protection Act 1998 (DPA), we are responsible to our staff and citizens for processing and protecting vast amounts of their personal information. Often, there are sound business reasons or the need to comply with legislation to share this information with other agencies or partners.

Principle 1 of the DPA requires that data is processed fairly which means when deciding whether to enter into an arrangement to share personal data (either as a provider, a recipient or both) staff must consider firstly whether there is a legal power either expressed or implied by legislation or an overriding public interest to share the data.

Principle 7 requires all organisations involved to have appropriate technical and organisational measures in place when sharing personal data.

The Policy:

- provides a framework for the Council and those working on its behalf to:

  - Provide information to deliver better services;
  - Consider the controls needed for information sharing; and
  - Make sure that partners sharing information are aware of the Council's Minimum Security Standards for securing information; the obligations of consent; and how to take appropriate account of an individual's objection to the sharing.

- Establishes a mechanism for the exchange of information between the Council and other organisations.

3. **Policy Implementation**

It is proposed that these and future information policies are implemented as follows:

1. Corporate Information Governance Group (CIGG) chaired by the Director of Resources reviews and agrees the policies. (COMPLETE).
2. GCLT endorse the policies. (COMPLETE).
3. Joint Staff Consultative Committee (JSCC) recommend the policies to the Corporate Policy and Resources (CP&R) Committee. (COMPLETE).
4. Policies are approved and formally adopted by the CP&R Committee.
5. Service Leadership Team (SLT) are briefed on the content and implications of the policies.
6. Members (if the policy is applicable) and staff read and demonstrate understanding of the content in a short training module delivered on the council's Learning Platform.

4. **Decisions Required**

That members approve the attached Information Governance Policy, Legal Responsibilities Policy and Information Sharing Policy formal adoption.

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

West Lindsey District Council

Information Governance Policy

Table of Contents

1 Overview

This organisation collects and uses a wide range of information for many different purposes. As such, information is a vital asset that the organisation is reliant on, both for the provision and for the efficient management of services and resources. It is essential that there is a robust information governance management framework and policies to ensure that information is effectively managed and that the risks of loss of information confidentiality, integrity and availability are reduced.

The objectives of Information Governance are specifically:

Legal Compliance. To achieve the necessary balance between openness and security by complying with the relevant legislative requirements.

Information Security. To apply security measures that are appropriate to the contents of the information.

Information and Records Management. To ensure that the creation, storage, movement, archiving and disposal of information and records is properly managed.

Information Quality. To support the provision of quality service delivery by the availability of quality information.

Information Sharing. To ensure that information can be effectively shared internally and between partner organisations while complying with the law and best practice standards.

Awareness and Guidance. To develop support arrangements which provide employees with awareness training and access to information governance policies and guidance.

2 Purpose

The purpose of this document is to set out the Information Governance Policy, including the Information Governance Management Framework, for West Lindsey District Council ("the Council"). It demonstrates management commitment to having in place sound information governance arrangements, gives clear direction to managers and staff, and will ensure that legal requirements and best practice standards are met.

3 Scope

This policy, framework and supporting policies apply to:

All data, information and records owned by the Council, but also including those held by contractors or partner organisations.

It applies to any information that is owned by other organisations, but may be accessed and used by Council employees, where there is no specific information sharing agreement in place.

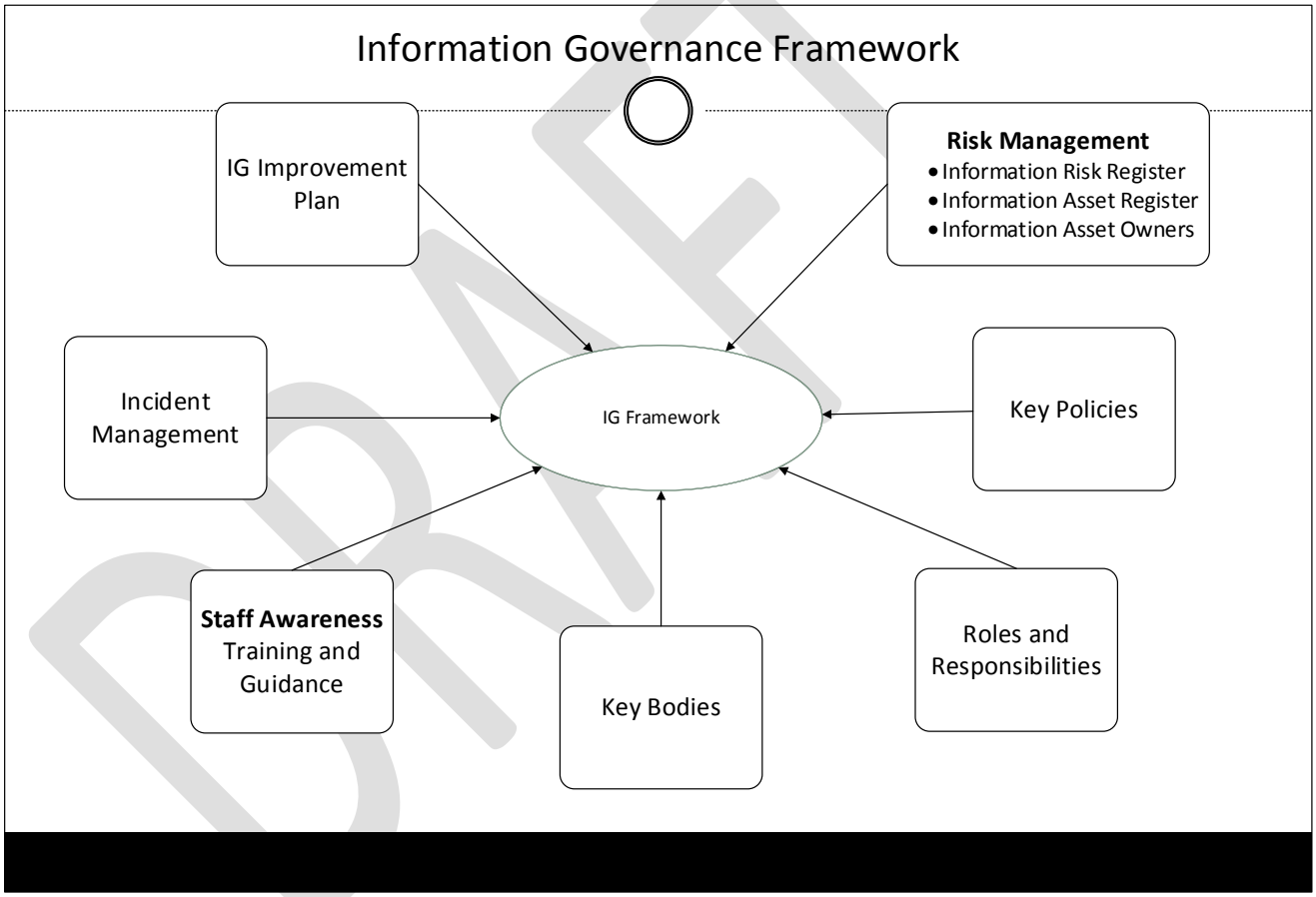
To information in whatever storage format and however transmitted (i.e. paper, voice, photo, video, audio or any digital format).

All employees of the council, and also council members, temporary workers, volunteers, student placements etc.

The employees of any other organisations having access to Council information; for example, auditors, contractors, and other partner agencies where there is no specific information sharing agreement in place.

4 Policy

4.1 The Information Governance Management Framework



4.1.1 Risk Management

It is important that information risks are acknowledged, documented, assessed and managed through the Council risk management arrangements. This puts information governance on the same footing as other corporate governance areas, and is reflected in its importance in the Senior Information Risk Owner's (SIRO) role.

4.1.2 Key Policies

An effective information governance structure is dependent on having key policies in place that cover 3 areas:

Information Compliance

Information Compliance is primarily concerned with the governance around, and the laws relating to, an organisation's information. It is also concerned with making sure information is of good quality and is properly and legally shared both internally and externally. The Council will make sure that there is:

a. An Information Governance Policy (this document) to set out a framework to manage its information governance responsibilities;

b. A Legal Responsibilities Policy to set out the main information-related legislation and the individual and collective responsibilities arising from it;

c. An Information Sharing Policy to cover any sharing of personal or confidential information with partner agencies or involving individual large transfers of such information. This Policy will make sure that an information sharing agreement based on a Council information sharing standard is in place and will set out the expected process and the standards of security and information handling; and

d. A Data Quality Policy to set out the Council's standards to make sure that information is timely, comprehensive, accurate, complete, up-to date, accessible, and relates to the correct person. Key to this is that there will be validation of data at the point of collection wherever possible, and that there are procedures for the assessment of data quality that are independent of the source of data collection.

Information Rights

The main legislation applying to information rights is the Data Protection Act 1998, the Freedom of Information Act 2000, and the Environmental Information Regulations 2004. In addition, Common Law has established a "duty of confidence" requiring us to keep other categories of information such as intellectual property confidential. In order to make sure that the requirements of information law are covered there will be:

a. A Data Protection Policy setting out the eight principles that all users of Council information must be aware of and adhere to. The principles specify how personal information and sensitive personal information must be collected and managed to ensure the fair treatment of individuals and their personal information within the rights that are given under the Act. The Act gives individuals the right to access their personal information. There are potentially severe penalties for any breach of the data protection principles.

b. A Data Protection Breach Policy detailing the actions we will take in the event of a security breach involving personal information covered by the Data Protection Act.

c. A Freedom of Information Policy that sets out the Council's policy with respect to The Freedom of Information Act (FOI) which gives any individual the right of access to information held by the organisation. This is subject to some exemptions, most notably for personal information, as defined by the DPA. To comply with the law the Council must respond to any such request within 20 working days.; and

d. A Records Management Policy to make sure that information and records are effectively managed, and that the Council can meet its information governance objectives and which sets out the Council's standards for handling information during each phase of the information lifecycle; creation, use, semi-active use, and final outcome.

Information Security

Information security is concerned with the confidentiality, integrity and availability of information in any format. This is an important and challenging area since new technologies are changing both the way we work and how we expect to access and use information. The Council's reliance on information is so great that difficulties in this area could severely impact on our ability to deliver services. Consequently, there will be an Information Security Policy with supporting policies and guidance that will comply with the law, best practice and any current certification standards.

Other relevant policies and guidance are listed at Para 6.

4.1.3 Information Governance Roles

These are the Senior Information Risk Owner, the Data Protection Officer, the Information Governance Officer, and the Information Asset Owners.

The Senior Information Risk Owner (SIRO)

The SIRO will be a member of the corporate leadership team, with an understanding how the strategic business goals of the organisation may be impacted by information risks.

Key tasks are to:

- Make sure that information risks are fully recognised in corporate risk registers;

- Take overall ownership of the risk assessment process for information risk, including review of an annual information risk assessment

- Review and agree action in respect of identified information risks;

- Make sure that the organisation's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff;

- Provide a focal point for the resolution and/or discussion of information risk issues; and

- Make sure the corporate leadership team is adequately briefed on information risk issues.

The Data Protection Officer (DPO)

The role of the Data Protection Officer is subject to the final provisions of the General Data Protection Regulation which is expected to come into full force in summer 2018.

The Information Governance Officer (IGO)

The IGO will act as the Information Governance Lead and co-ordinate the information governance work programme. The IGO will be accountable for ensuring effective management, accountability, compliance and assurance for all aspects of information governance and will provide a focal point for the resolution and/or discussion of information governance issues.

Key tasks are to:

- Provide direction in formulating, establishing, promoting and maintaining the policies and documentation that demonstrate commitment to and ownership of information governance responsibilities;

- Make sure that there is top level awareness and support for information governance resourcing and implementation of improvements;

- Make sure that the approach to information handling is communicated to all staff, made available to the public, and monitored to ensure compliance;

- Make sure that appropriate training is made available to staff and completed as necessary to support their duties;

- Establish working groups, if necessary, to co-ordinate the activities of staff given information governance responsibilities and progress initiatives;

- Make sure annual assessments and audits of information governance policies and arrangements are carried out, documented and reported; and

- Make sure that the annual assessment and improvement plans are prepared for approval by the senior level of management.

Information Asset Owners (IAO)

The Information Asset Owners will be senior members of staff who are the nominated owners for one or more identified information assets of the Council. It is a core information governance objective that all information assets of the Council are identified and that their business importance is established.

The role of Information Asset Owners is to:

- Identify and document the scope and importance of all Information Assets they own. This will include identifying all information necessary in order to respond to incidents or recover from a disaster affecting the Information Asset;

- Take ownership of their local asset control, risk assessment and management processes for the information assets they own. This includes the identification, review and prioritisation of perceived risks and oversight of actions agreed to mitigate those risks;

- Provide support to the SIRO and the Corporate Information Governance Group (CIGG) to maintain their awareness of the risks to all information assets that are owned by the organisation and for the organisation's overall risk reporting requirements and procedures;

- Make sure that staff and relevant others are aware of and comply with expected information governance working practices for the effective use of owned Information Assets. This includes records of the information disclosed from an asset where this is permitted.

- Provide a focal point for the resolution and/or discussion of risk issues affecting their Information Assets;

- Make sure that the Council's information security incident policy requirements are applied to their information assets;

- Foster an effective information governance and security culture for staff and others who access or use the information assets to ensure individual responsibilities are understood, and that good working practices are adopted in accordance with Council Policy; and

- Set out local procedures that are consistent with corporate information security policies and guidelines.

Specialist Supporting Roles and Knowledge

There will be trained staff with specialist knowledge both to support the senior information roles, and to provide staff and managers with specific advice about the policies and guidance. The specialist knowledge covers information law (Data Protection and Freedom of Information Acts), information security, data quality, information and records management.

Managers

All managers will make sure that:

- The requirements of the information governance policy framework, its supporting policies and guidance are built into local procedures;
- That there is compliance with all relevant information governance policies within their area of responsibility;
- Information governance issues are identified and resolved whenever there are changes to services or procedures; and
- Their staff are properly supported to meet the requirements of information governance and security policies and guidance, by ensuring that they are aware of:
    - The policies and guidance that apply to their work area;
    - Their responsibility for the information that they use; and
    - Where to get advice on security issues and how to report suspected security incidents.

All Staff

All staff are responsible for:

- Making sure that they comply with all information governance policies and information security policies and procedures that are relevant to their service and consulting their manager if in doubt.
- Seeking further advice if they are uncertain how to proceed.
- Reporting suspected information security incidents.

4.1.4 Key Bodies

Corporate Information Governance Group (CIGG)

The CIGG is chaired by the Council's Senior Information Risk Owner (SIRO) and comprises the information specialists from across all service areas who can share knowledge and experience where necessary. The group has a pivotal and central role in ensuring that Information Governance is effectively communicated and managed and across the organisation.

Corporate Leadership Team (CLT)

CLT comprises the Council's Chief Executive, Directors and Monitoring Officer and is responsible for:

- the leadership, development and organisation of the Authority;
- the stewardship of Authority assets;

- the development and delivery of the Authority's policies;
- the service provided by the Authority; and
- Corporate Governance and oversight of the Authority's resources.

Service Leadership Team (SLT)

The Strategic Leadership Team (SLT) is a key part of the management of the council. SLT reports to the Corporate Leadership Team and its primary function is to ensure that council services are delivered efficiently, effectively and economically and are aligned to the delivery of the council's Corporate Plan.

Governance and Audit Committee

The Governance and Audit Committee is responsible amongst other things for:

- Reviewing the adequacy of the Council's corporate governance arrangements (including matters such as internal control and risk management) and approving the annual governance statement.

Joint Staff Consultative Committee (JSCC)

The JSCC is a committee involving Councillors and employee representatives and is supported and advised by appropriate officers depending on the topics that are under consideration. The group meet regularly and are responsible for:

- Establishing regular methods of communication and negotiation between the Council and employees in order to prevent differences.
- Considering and advising on any relevant matter referred to it by any committee of the Council or by any of the employee groups.

Making recommendations to the Policy and Resources Committee as to the adoption of policies affecting employee interests (except those relating to the terms and conditions).

Corporate Policy and Resources Committee

The principal committee of the Council responsible for (amongst other things not relevant to this policy):

- The adoption and approval of strategies and policies not forming part of the Policy Framework apart from those policies for which delegated power is given to the Chief Executive to approve under Part IV of the Constitution.

4.1.5 Staff Awareness

- Staff awareness is a key issue in achieving both compliance with information governance policies and the improvements required by the improvement plan. Accordingly there will be:

- Mandatory base line training in key information governance competencies for all staff who have not received any recent relevant training as well as for all new starters;

- Additional training for all employees routinely handling 'sensitive personal information', as defined by the DPA 1998;

- All information governance policies and guidance to be available on Minerva; and,

- Staff with specialist knowledge available to provide advice across the full range of information governance areas.

4.1.6 Information Security Incident Management

There will be an information security incident management policy and procedures that set out how incidents will be reported and managed. The results of incident investigations will be reported to the CIGG and from there feed into risk management and the information governance improvement plan.

4.1.7 Information Governance Improvement Plan

There will be an information governance improvement plan that identifies the detailed requirements necessary to achieve compliance with the main policy objectives. This plan will be monitored and progressed by the information governance working group to ensure that there continuing development. Progress against the plan will be reported six monthly to the corporate leadership team.

5 Policy Compliance

5.1 Compliance Measurement

The Council will regularly review its organisational and technological processes to ensure compliance with this Policy and the relevant legislation.

Where there are particular compliance measurements, such as those required by the Data Protection Act 1998 and the Freedom of Information Act 2000 and Environmental Information Regulations 2004, these are detailed in the Council's relevant Policies.

All Policies and procedures relating to information management will be subject to scrutiny by the Joint Staff Consultative Committee (JSCC) and the Corporate Policy and Resources Committee (CP&R) and by the Governance and Audit Committee through its Annual Governance Statement monitoring activities.

5.2 Non-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.

5.3 Policy Review

This Policy will be reviewed every two years by the IGO, CIGG, JSCC and CP&R and updated in the interim as required.

6 Relevant Legislation, Standards, Policies, and Guidance

The primary legislation governing the Council's information management activities is described in the Legal Responsibilities Policy.

West Lindsey District Council

Legal Responsibilities Policy

Table of Contents

1 Overview

This Policy lists and describes the legislation and regulations that govern information management and highlights the risks both to the organisation and to individuals for failing to comply.

2 Purpose

At West Lindsey District Council ("the Council") we create, collect, hold, and use vast amounts and types of information to carry out our functions, much of which is governed by legislation. For instance, we process personal data about people and organisations with whom we deal with, information protected by copyright, and intellectual property which we must keep confidential.

In addition, we are occasionally required by law to collect and use certain types of personal information to comply with the requirements of Government departments.

However, we also make much of our information publically available to demonstrate open and transparent government and Information Rights legislation such as the Freedom of Information Act 2000 sets out how we must publish or respond to legitimate requests for our information

This Policy details our responsibilities under the wide and varied legislation that governs our information and information systems.

3 Scope

Any information must be dealt with properly irrespective of how it is collected, recorded and used, whether on paper, in a computer, or recorded on other media. For instance, there are safeguards set out in the Data Protection Act 1998 to make sure that personal information is collected and processed correctly.

This Policy relates to all information held or processed by the Council. It applies to all full time and part time employees of the Council, elected members, partner agencies, contracted employees, third party contracts (including agency employees), volunteers and students or trainees on placement with the Council, who have access to information held or processed by the Council.

4 Roles and Responsibilities

For most information-related legislation the following Council officers are accountable and responsible for compliance. Where specific responsibilities exist for legislation, these are included within the description of the particular legislation below.

- **Chief Executive**. The Chief Executive has overall responsibility for strategic and operational management, including making sure that Council policies comply with all legal, statutory and good practice guidance requirements.

- **Senior Information Risk Owner (SIRO).** The SIRO has overall responsibility for ensuring that information risks are properly recorded and managed. The SIRO is also the Council's Section 151 Officer with responsibility for exercising the proper administration of the Council's financial affairs under section 151 of the Local Government Act 1972 and section 114 of the Local Government Finance Act 1988.

- **The Information Governance Officer (IGO).** The IGO will act as the Information Governance Lead and co-ordinate the information governance work programme. The IGO will be accountable for ensuring effective management, accountability, compliance and assurance for all aspects of information governance and will provide a focal point for the resolution and/or discussion of information governance issues.

- **Information Asset Owners (IAO).** IAOs will be senior members of staff who are the nominated owners for one or more identified information assets of the Council. It is a core information governance objective that all information assets of the Council are identified and that their business importance is established.

- **Corporate Information Governance Group (CIGG).** The CIGG is chaired by the SIRO and comprises the information specialists from across all service areas who can share knowledge and experience where necessary. The group has a pivotal and central role in ensuring that Information Governance is effectively communicated and managed and across the organisation.

5 Policy

This section lists the legislation applicable to information and information systems and details specific responsibilities for complying with it.

5.1 Civil Contingencies Act 2004

Category 1 organisations (the emergency services, local authorities, NHS bodies) are at the core of the response to most emergencies and are subject to the full set of civil protection duties.

The act requires that, as Category 1 Responders, Local Authorities put in place Business Continuity Management arrangements.

5.1.1 What will the Council do?

In order to meet its obligations under the Act, the Council will:

- Assess the risk of emergencies occurring and use this to inform contingency planning;

- Put in place emergency plans;

- Put in place business continuity management arrangements;

- Put in place arrangements to make information available to the public about civil protection matters and maintain arrangements to warn, inform and advise the public in the event of an emergency;

- Share information with other local responders to enhance co-ordination;

- Co-operate with other local responders to enhance co-ordination and efficiency; and

- Provide advice and assistance to businesses and voluntary organisations about business continuity management (applicable to local authorities only).

5.1.2 What will the Council's employees do?

Council employees and other parties listed at para 3 will, where appropriate, comply with Council's policies and procedures relating to this legislation.

5.2 Companies Act 2006

Adequate precautions should be taken against the falsification of records and to discover any falsification that occurs.

5.2.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies and procedures and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

5.2.2 What will the Council's employees do?

Council employees and other parties listed at para 3 will, where appropriate, comply with Council's policies and procedures relating to this legislation.

5.3 Common Law of Confidentiality

Common Law of Confidentiality is not in any written Act of Parliament. It is "common" law which means that it has been established over a period of time through the courts.

The law recognises that some information has a quality of confidence, which means that the individual or organisation that provided the information has an expectation that it will not be shared with or disclosed to others.

For information to have a quality of confidence it is generally accepted that:

- it is not "trivial" in its nature;

- it is not in the public domain or easily available from another source;

- it has a degree of sensitivity; and

- it has been communicated for a limited purpose and in circumstances where the individual or organisation is likely to assume an obligation of confidence. For example information shared between a solicitor/client, health practitioner/patient, etc.

However, as with the Human Rights Act 1998, confidentiality is a qualified right[1]. The Council is able to override a duty of confidence when it is required by law, or if it is in the public interest to do so.

5.3.1 What will the Council do?

In order to meet its obligations under the Common Law of Confidentiality, the Council will make sure that:

- Confidentiality is included as an essential element of employee terms and conditions;

- The need to keep information confidential where appropriate is included in all security awareness training.

- Confidentiality clauses are included in all Council contracts where information may be accessed or shared.

5.3.2 What will the Council's employees do?

Council employees and other parties listed at para 3 will recognise and understand the importance of not disclosing confidential information to anyone who does not have a "need to know" and will comply with Council's policies and procedures relating to this legislation.

5.3.3 Roles and Responsibilities

Everyone who comes into contact with information has a responsibility to keep it private where necessary and in some cases may be held personally accountable for any breach of confidentiality.

5.4 Computer Misuse Act 1990

The computer misuse act makes it illegal to gain unauthorised access to a computer. The act is made up of three separate offences:

[1] Qualified Rights are rights which can be restricted not only in times of war or emergency but also in order to protect the rights of another or the wider public interest. In general, qualified rights are structured so that the first part of the Article sets out the right, while the second part establishes the grounds on which a public authority can legitimately interfere with that right in order to protect the wider public interest

Unauthorised access to computer material; the act of accessing materials without authorisation is an offence even if no damage is done, files deleted or changed

Unauthorised access with intent to commit or facilitate commission of further offences.

Unauthorised modification of computer material; including the amendment, damage of data, including the introduction of computer viruses.

5.4.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies and procedures and that any policy or specific requirements and the penalties for offenses under the Act are included in awareness training provided to staff, Members and partners.

5.4.2 What will the Council's employees do?

As well as not committing any of the 3 basic offences, Council employees and other parties listed at para 3 must not:

1. Display any information which enables others to gain unauthorised access to computer material (this includes instructions for gaining such access, computer codes or other devices which facilitate hacking)

2. Display any information that may lead to any unauthorised modification of computer materials (such modifications would include activities such as the circulation of "infected" software or the unauthorised addition of a password)

3. Display any material, which may incite or encourage others to carry out unauthorised access to or modification of computer materials.

5.4.3 What are the consequences of non-compliance?

The penalties for committing criminal offences in each of the 3 categories are as follows:

1. Unauthorised access to computer material (basic hacking) including the illicit copying of software held in any computer which carries a penalty of up to six months imprisonment or up to a £5,000 fine.

2. Unauthorised access with intent to commit or facilitate commission of further offences, which covers more serious cases of hacking which carries a penalty of up to five years of imprisonment and an unlimited fine.

3. Unauthorised modification of computer material, which includes:

    i) intentional and unauthorised destruction of software or data;

    ii) the circulation of "infected" materials on-line; and

    iii) An unauthorised addition of a password to a data file.

This offence carries a penalty of up to five years of imprisonment and an unlimited fine.

5.5 Copyright, Designs and Patents Act 1988

The law gives the creators of literary, dramatic, musical, artistic works, sound recordings, broadcasts, films and typographical arrangement of published editions, rights to control the ways in which their material may be used.

The rights cover; broadcast and public performance, copying, adapting, issuing, renting and lending copies to the public.

In many cases, the creator will also have the right to be identified as the author and to object to distortions of his work. International conventions give protection in most countries, subject to national laws.

5.5.1 Types of work protected

1. **Literary**. Song lyrics, manuscripts, manuals, computer programs, commercial documents, leaflets, newsletters & articles etc.

2. **Dramatic**. Plays, dance, etc.

3. **Musical**. Recordings and score.

4. **Artistic**. Photography, painting, sculptures, architecture, technical drawings/diagrams, maps, logos.

5. **Typographical arrangement of published editions**. Magazines, periodicals, etc

6. **Sound recording**. May be recordings of other copyright works, e.g. musical and literary.

7. **Film**. Video footage, films, broadcasts and cable programmes.

The Copyright (Computer Programs) Regulations 1992 extended the rules covering literary works to include computer programs.

Only software that is developed by the Council, or either licensed or provided by a developer to the Council should be used.

The copyright of all software developed within the Council by staff or contractors should be held by the Council.

The right of the Council to make copies, for its own use, of any software provided must be retained by the Council.

Under no circumstances should software be copied from one machine to another without the appropriate licence agreement. Only staff authorised by ICT management may install, or move software.

5.5.2 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies, procedures and approval processes and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

5.5.3 What will the Council's employees do?

Council employees and other parties listed at para 3 will, where appropriate, comply with Council's policies and procedures relating to this legislation. Specifically, employees and other authorised users of the Council's ICT equipment will not install or use software, or use images, media or other copyrighted material that has not been approved and/or licensed for Council use.

5.5.4 What are the consequences of non-compliance?

Copyright infringement that may be criminal offences under the Copyright, Designs and Patents Act 1988 are the:

- Making copies for the purpose of selling or hiring them to others;
- Importing infringing copies (except for personal use);
- Offering for sale or hire, publicly displaying or otherwise distributing infringing copies in the course of a business;
- Distributing a large enough number of copies to have a noticeable effect on the business of the copyright owner;
- Making or possessing equipment for the purposes of making infringing copies in the course of a business;
- Publicly performing a work in knowledge that the performance is unauthorised;
- Communicating copies or infringing the right to "make available" copies to the public (either in the course of a business, or to an extent prejudicial to the copyright owner); and
- Manufacturing commercially, importing for non-personal use, possessing in the course of a business, or distributing to an extent that has a noticeable effect on the business of the copyright holder, a device primarily designed for circumventing a technological copyright protection measure.

The penalties for these copyright infringement offences may include:

- Before a magistrates' Court, the penalties for distributing unauthorised files are a maximum fine of £5,000 and/or six months imprisonment;

- On indictment (in the Crown Court) some offences may attract an unlimited fine and up to 10 years imprisonment.

5.6 Data Protection Act 1998

The Act gives rights to individuals about whom personal data is recorded (Data Subjects). They may obtain personal data held about themselves, challenge it if appropriate and claim compensation in certain circumstances. The act places obligations on those who record and use personal data (Data Users). They must be open about that use (through the data protection register) and follow sound and proper practices (the Data Protection principles). Any requests to view personal data must be in line with the Data Protection and IT Access policies and must be approved by the Information Asset Owner (IAO) of the dataset or Information Asset.

The Act applies to personal data and is based upon a set of eight principles, which should form the basis of good organisational practice. The principles state that personal data:

1. Shall be obtained and processed fairly and lawfully.
2. Shall be obtained for specified lawful purposes.
3. Shall be adequate, relevant and not excessive for the purpose.
4. Shall be accurate and where necessary, kept up to date.
5. Shall not be kept longer than is necessary.
6. Shall be processed in accordance with the rights of data subjects.
7. Shall be kept secure.
8. Shall not be transferred to a country outside the EEA without adequate safeguards being in place

5.6.1 What will the Council do?

In order to meet its obligations under the Data Protection Act, the Council will make sure that:

- There is an individual with specific responsibility for data protection in the organisation.
- Everyone managing and handling personal information understands that they are legally responsible for following good data protection practice.
- Everyone managing and handling personal information is properly trained to do so and adequate advice and guidance is available.
- Persons wishing to make enquiries about handling personal information, whether a member of staff or a member of the public, is aware of how to make such an enquiry.

- Methods of handling personal information are regularly assessed and evaluated.

- All actual or potential breaches of the Data Protection Act are investigated, mitigated, and reported as appropriate.

5.6.2 What will the Council's employees do?

Employees and agents of the Council are personally responsible for complying with the Data Protection Act. In particular they will make sure that:

- They attend or complete data protection training provided by or on behalf of the Council.

- When collecting or processing personal information in the course of their duties they follow any policies, guidance, and procedures provided by the Council for that purpose.

- They report any breaches of the Act using the Council's Data Protection Breach Policy.

- Queries about handling personal information are promptly and courteously dealt with.

5.6.3 What are the consequences of non-compliance?

There are a number of tools available to the Information Commissioner's Office for taking action to change the behaviour of organisations and individuals that collect, use and keep personal information. They include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner also has the power to serve a monetary penalty notice of up to £500,000 on a data controller.

5.6.4 Roles and Responsibilities

- The **Chief Executive** has overall responsibility for strategic and operational management, including ensuring that Council policies comply with all legal, statutory and good practice guidance requirements.

- The **Council's Senior Information Risk Owner** has overall responsibility for ensuring that information risks are properly recorded and managed.

- The **Council's Data Protection Officer** will provide guidance and advice to employees to facilitate the correct handling of personal information and to enable the Council to meet its legal obligations under the Data Protection Act.

- The **Council's Data Protection Officer** is responsible for notifying the Information Commissioner's Office of the Council's purposes for processing personal information.

- **Directors** are responsible for ensuring that the Council's Data Protection procedures are communicated and implemented within their directorates.

- **Information Asset Owners** are responsible for ensuring that all their staff are appropriately trained with regards to Data Protection and for ensuring that any Data Protection related issues in their own area are handled in compliance with this policy and relevant procedures.

- **Information Asset Owners** are responsible for ensuring that all personal data is disposed of securely and in line with the Retention Guidelines for Local Authorities.

- All **Council employees** must attend relevant Data Protection training.

- All **Council employees** are responsible for understanding, and adhering to this Policy and the Council's Policy and procedures relating to Data Protection.

- All **Council employees** should seek Data Protection advice from the Council's Data Protection Officer when necessary.

5.6.5 Sharing Personal Information with other Organisations

Personal information must not be disclosed to any other person or organisation via any insecure method.

Where such information is disclosed/shared it should only be done so in accordance with a documented Information Sharing Agreement.

The Council's Data Protection Officer is responsible for the Information Sharing Agreements.

5.7 Environmental Information Regulations 2004

The Environmental Information Regulations provide members of the public with the right to access environmental information held by public authorities.

Environmental information covers:

- The state of the elements of the environment, such as air, water, soil, land, fauna (including human beings);
- Emissions and discharges, noise, energy, radiation, waste and other such substances;

- Measures and activities such as policies, plans and agreements affecting or likely to affect the state of the elements of the environment;

- Reports, cost-benefit and economic analyses;

- The state of human health and safety and contamination of the food chain; and

- Cultural sites and built structures (to the extent they may be affected by the state of the elements of the environment).

The Council is required to respond to a request for environmental information within 20 working days although further reasonable details can be requested to identify and find the information in line with the legislation.

5.7.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies, procedures and approval processes and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

5.7.2 What will the Council's employees do?

Council employees and other parties listed at para 3 will, where appropriate, comply with Council's policies and procedures relating to this legislation.

5.8 Freedom of Information Act 2000

Gives a general right of access to all types of recorded information held by public authorities, sets out exemptions from that right and places a number of obligations on public authorities.

Subject to the exemptions, any person who makes a request to a public authority for that information must be informed whether the public authority holds that information. If it does, that information must be supplied, subject to certain conditions.

Every public authority is required to adopt and maintain a publication scheme setting out how it intends to publish the different classes of information it holds, and whether there is a charge for the information.

Two codes of practice (s. 45 and s. 46) issued under the Act provide guidance to public authorities about responding to requests for information, and records management. The Act is enforced by the Information Commissioner.

5.8.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies, procedures and approval processes and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

5.8.2 What will the Council's employees do?

Council employees and other parties listed at para 3 will, where appropriate, comply with Council's policies and procedures relating to this legislation.

5.8.3 What are the consequences of breaching the Act?

The Council may be breaching the Freedom of Information Act if it does any of the following:

- Fail to respond adequately to a request for information;

- Fail to adopt the model publication scheme, or do not publish the correct information; or

- Deliberately destroy, hide or alter requested information to prevent it being released.

This last point is the only criminal offence in the Act that individuals and public authorities can be charged with.

Other breaches of the Act are unlawful but not criminal. The Information Commissioner's Office (ICO) cannot fine the Council if it fails to comply with the Act, nor can it require us to pay compensation to anyone for breaches of the Act. However, we should correct any mistakes as soon as we are aware of them.

5.9 Human Rights Act 1998

An individual's privacy and protection of property rights must be respected. This includes ensuring the security of personal data. Infringements could lead to breaches of these rights.

An employee's privacy is, however, subject to the provisions of the **Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000**

5.9.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies, procedures and approval processes and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

5.9.2 What will the Council's employees do?

Council employees and other parties listed at para 3 will, where appropriate, comply with Council's policies and procedures relating to this legislation.

5.10 Privacy & Electronic Communications (EC Directive) Regulations

The Privacy and Electronic Communications Regulations (PECR) originally came into force in 2003 and were amended in 2004, 2011, and again in 2015. The regulations sit alongside the Data Protection Act and give people specific privacy rights in relation to electronic communications.

There are specific rules on:

- Marketing calls, emails, texts and faxes;

- Cookies (and similar technologies);

- Keeping communications services secure; and

- Customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

5.10.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies, procedures and approval processes and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

5.10.2 What will the Council's employees do?

Council employees and other parties listed at para 3 will, where appropriate, comply with Council's policies and procedures relating to this legislation.

5.10.3 What are the consequences of not complying with the Regulations?

The regulations carry a number of sanctions for non-compliance. These are enforced by the ICO and include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner also has the power to serve a monetary penalty notice imposing a fine of up to £500,000.

5.11 Re-use of Public Sector Information Regulations 2015

The Regulations are concerned with the re-use by businesses and citizens of information held by public sector bodies. "Re-use" essentially means the use of existing information in new products and services. Its aim is to support technology driven growth and civil society applications, for example, in the use of mapping information in satellite navigation products.

The Regulations affect how information can be re-used once it has been legitimately accessed, by placing obligations on the public sector to the benefit of re-users.

The Regulations do not create rights of access to information. They do not override or modify data protection rules. Re-use of public sector information in the UK must therefore comply with the Data Protection Act and any related regulations

5.11.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies, procedures and approval processes and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

5.11.2 What will the Council's employees do?

Council employees and other parties listed at para 3 will, where appropriate, comply with Council's policies and procedures relating to this legislation.

5.12 Regulation of Investigatory Powers Act 2000 (RIPA)

RIPA is the law governing the use of covert techniques by public authorities. It requires that when public authorities, such as the police or government departments, need to use covert techniques to obtain private information about someone, they do it in a way that is necessary, proportionate, and compatible with human rights.

RIPA's guidelines and codes apply to actions such as:

- Intercepting communications, such as the content of telephone calls, emails or letters;
- Acquiring communications data: the 'who, when and where' of communications, such as a telephone billing or subscriber details;
- Conducting covert surveillance, either in private premises or vehicles (intrusive surveillance) or in public places (directed surveillance);
- The use of covert human intelligence sources, such as informants or undercover officers; and
- Access to electronic data protected by encryption or passwords.

RIPA applies to a wide-range of investigations in which private information might be obtained. Cases in which it applies include:

- Terrorism
- Crime
- Public safety
- Emergency services

5.12.1 What will the Council do?

The Council will make sure that it considers this legislation when developing its policies, procedures and approval processes and that any policy or specific requirements are included in awareness training provided to staff, Members and partners.

5.12.2 What will the Council's employees do?

Council employees and other parties listed at para 3 will, where appropriate, comply with Council's policies and procedures relating to this legislation.

6 Policy Compliance

6.1 Compliance Measurement

The Council will regularly review its organisational and technological processes to ensure compliance with this Policy and the relevant legislation.

Where there are particular compliance measurements required by the Data Protection Act 1998 and the Freedom of Information Act 2000 and Environmental Information Regulations 2004 these are detailed in the Council's relevant Policies.

All Policies relating to information management will be subject to scrutiny by the Corporate Policy and Resources Committee.

6.2 Non-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.

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 the Data Protection Officer being the City Solicitor and the Freedom of Information Officer/the Legal and Democratic Services Manager or a member of the Legal Services Team.

6.3 Policy Review

This Policy will be reviewed every two years by the Corporate Information Governance Group and approved by the Corporate Policy and Resources Committee. Authority to approve interim updates may be delegated to the Director of Resources in consultation with the Chairmen of the Joint Staff Consultative Committee and the Corporate Policy and Resources Committee as required.

7 Related Standards, Policies, and Processes

- Information Governance Policy
- Data Protection Policy
- Freedom of Information and Environmental Information Regulations Policy.
- Information Sharing Policy
- Data Quality Policy
- Data Protection Breach Policy
- Records Management Policy
- Information Security Policy
- Retention and Disposal Policy

West Lindsey District Council

Information Sharing Policy

Table of Contents

1 Overview

Information sharing is key to West Lindsey District Council's ("the Council") goal of delivering better and more efficient services that are coordinated around the needs of the individual. Sharing information both internally and with our partners is essential to support early intervention and preventative work, for safeguarding and promoting welfare and for wider public protection. Information sharing is a vital element in improving outcomes for all.

The Council understands that it is most important that people remain confident that we keep their personal information safe and secure and that staff maintain the privacy of the individual, whilst sharing information to deliver better services. It is therefore important that all staff are aware of how they can share information appropriately as part of their day-to-day responsibilities and do so confidently.

2 Purpose

The purpose of this policy is to:

- Provide a framework for the Council and those working on its behalf to:
    - Provide information to deliver better services;
    - Consider the controls needed for information sharing; and
    - Make sure that partners sharing information are aware of the Council's Minimum Security Standards for securing information; the obligations of consent; and how to take appropriate account of an individual's objection to the sharing.
- Establish a mechanism for the exchange of information between the Council and other organisations.

3 Scope

This Policy applies to all staff including those who are responsible for managing partnerships where information will be shared and those who are responsible for creating or providing the information that is to be shared.

Information sharing, in the context of this policy, means the disclosure of personal information from one or more organisations to a third party organisation or organisations. Information sharing can be:

- A reciprocal exchange of data;
- One or more organisations providing data to a third party or parties;
- Several organisations pooling information and making it available to each other;
- Several organisations pooling information and making it available to a third party or parties; or

- Exceptional, one-off disclosures of data in unexpected or emergency situations.

Sharing non-personal information with other organisations. This is where the Council shares key information with other organisations to: improve customer experience; facilitate commissioning of services; manage and plan future services; assure and improve the quality of services; statutory returns and requests; to train staff; to audit performance.

Sharing Personal information with other organisations. As long as it is necessary and proportionate, the Council can share personal information with other organisations: to prevent crime; to investigate complaints or potential legal claims; to protect children and adults at risk; to assess need and service delivery.

This policy covers two main types of information sharing. These are explained in more detail in Para 4:

- "Systematic", routine information sharing where the same data sets are shared between the same organisations for an established purpose; and

- Exceptional, one-off decisions to share information for any of a range of purposes.

4 Policy

4.1 Factors to consider before sharing information

When deciding whether to enter into an arrangement to share personal data (either as a provider, a recipient or both) staff must consider firstly whether there is a legal power either expressed or implied by legislation or an overriding public interest to share the data.

If staff are unsure about this they must seek advice from the Data Protection Officer or the Information Governance Officer.

If the answer is the above question is yes, staff must then consider what the sharing is meant to achieve and there should be a clear objective, or set of objectives. Being clear about this will identify the following:

- Could the objective be achieved without sharing the data or by anonymising it? It is not appropriate to use personal data to plan service provision, for example, where this could be done with information that does not amount to personal data.

- What information needs to be shared? You should not share all the personal data you hold about someone if only certain data items are needed to achieve the objectives. The third Data Protection principle states, "Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed."

- Who requires access to the shared personal data? You should employ 'need to know' principles, meaning that when sharing both internally between departments and externally with other organisations individuals should only have access to your data if they need it to do their job, and that only relevant staff should have access to the data. This should also address any necessary restrictions on onward sharing of data with third parties.

- When should it be shared? It is good practice to document this, for example setting out whether the sharing should be an on-going, routine process or whether it should only take place in response to particular events.

- How should it be shared? This involves addressing the security surrounding the transmission or accessing of the data and establishing common rules for its security.

- How can we check the sharing is achieving its objectives? You will need to judge whether it is still appropriate and confirm that the safeguards still match the risks.

- How do we make individuals aware of the information sharing? Consider what to tell the individuals concerned. Is their consent needed? Should the individuals be provided with a Privacy Notice, notifying them of who you are going to share their data with? Do they have an opportunity to object? How do you take account of their objections? How do you ensure the individual's rights are respected and can be exercised e.g. how can they access the information held once shared?

- What risk to the individual and/or the organisation does the data sharing pose? For example, is any individual likely to be damaged by it? Is any individual likely to object? Might it undermine individuals' trust in the organisations that keep records about them?

In all circumstances of information sharing, staff will make sure that:

- When information needs to be shared, sharing complies with the law, guidance and best practice;

- The information must processed lawfully and fairly to comply with the Data Protection Act 1998 (DPA) and the ICO's Code of Practice on Data Sharing published under section 52 of the DPA must be followed. This Policy has been written in accordance with the Code although further information on the Code can be found on the ICO's website www.ico.org.uk

- The sharing must not contravene other laws such as Article 8 of the Human Rights Act 1998 being The Right to Privacy.

- Only the minimum information necessary for the purpose will be shared and, if sharing with providers, will only be shared when the contract explicitly permits it;

- Individuals' rights will be respected, particularly regarding the confidentiality and security of their personal information and the sharing must not contravene laws such as the Common Law of Confidentiality;

- Confidentiality will be maintained unless there is a robust public interest or a legal justification in disclosure; and

- They undertake reviews of information sharing to make sure the information sharing is meeting the required objectives/purpose and is still fulfilling its obligations.

4.2 Information Sharing Agreements

Information sharing agreements – sometimes known as 'Information or data sharing protocols' – set out a common set of rules to be adopted by the various organisations involved in an information sharing operation. These could well form part of a contract between organisations. It is good practice to have a data sharing agreement in place, and to review it regularly, particularly where information is to be shared on a large scale, or on a regular basis.

An information sharing agreement must at least document the following:

- The purpose, or purposes, of the sharing;

- The legal basis for sharing;

- The potential recipients or types of recipient and the circumstances in which they will have access;

- Who the data controller(s) is and any data processor(s);

- The data to be shared;

- Data quality – accuracy, relevance, usability;

- Data security;

- Retention of shared data;

- Individuals' rights – procedures for dealing with access requests, queries and complaints;

- Review of effectiveness/termination of the sharing agreement;

- Any particular obligations on all parties to the agreement, giving an assurance around the standards expected; and

- Sanctions for failure to comply with the agreement or breaches by individual staff.

4.3 Privacy Impact Assessments

Before entering into any information sharing arrangement, it is good practice to carry out a privacy impact assessment. This will help to assess the benefits that the information sharing might bring to particular individuals or society more widely. It will also help to assess any risks or potential negative effects, such as an erosion of personal privacy, or the likelihood of damage, or causing distress or embarrassment to individuals.

As well as harm to individuals, staff should consider potential harm to the organisation's reputation which may arise if information is shared inappropriately, or not shared when it should be. Further information on privacy impact assessments can be found on Minerva.

5 Policy Compliance

5.1 Compliance Measurement

The Council will regularly review its organisational and technological processes to ensure compliance with this Policy and the relevant legislation.

Where there are particular compliance measurements, such as those required by the Data Protection Act 1998 and the Freedom of Information Act 2000 and Environmental Information Regulations 2004, these are detailed in the Council's relevant Policies.

All Policies relating to information management will be subject to scrutiny by the Corporate Policy and Resources Committee.

5.2 Non-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.

Where personal information is being shared a breach of this Policy could result in a breach of the Data Protection Act 1998, for which the Council could face substantial fines, reputational damage and possible criminal sanctions.

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).

The Council encourages the notification of Data Protection breaches by staff in accordance with the Data Protection Breach Management Policy at the earliest opportunity. Notification will also be taken into account in any resulting disciplinary investigation, where the individual/s concerned have assisted in the containment of the breach.

If you do not understand the implications of this Policy or how it may apply to you, seek advice from the Data Protection Officer or the Information Governance Officer.

5.3 Policy Review

This Policy will be reviewed every two years by the Corporate Information Governance Group and approved by the Corporate Policy and Resources Committee. Authority to approve interim updates may be delegated to the Director of Resources in consultation with the Chairmen of the Joint Staff Consultative Committee and the Corporate Policy and Resources Committee as required.

6 Related Standards, Policies, and Processes

- Information Governance Policy
- Legal Responsibilities Policy
- Data Protection Policy
- Data Quality Policy
- Data Protection Breach Policy
- Freedom of Information Policy & Environmental Information Regulations Policy
- Records Management Policy
- Information Security Policy
- Staff Code of Conduct
- Member's Code of Conduct
- Retention and Disposal Policy

7 Definitions

Data Sharing	The disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. Can take the form of systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and exceptional, one off decisions to share data for any of a range of purposes.
Data Controller	A data controller is the "person" recognised in law (i.e. an individual; organisation; or other corporate and unincorporated body of persons) who determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data Processor	Any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller.

Data Sharing Agreements	Set out a common set of rules to be adopted by various organisations involved in a data sharing operation.
Privacy Impact Assessments	A formalised document which shows the possible threats to privacy which could arise from a business activity.
Data Quality	Data quality relates to the accuracy, validity, reliability, timeliness, relevance and completeness of data and information.
Data Security	The policies, procedures and practices required to maintain and provide assurance of the confidentiality, integrity and availability of information.
Information	*"Information is data imbued with meaning and purpose". Anon* Information is something which tells us something and can also be communicated to someone else in a meaningful way. Information is data that is put into context, can be comprehended, understood and shared with other people and / or machines.
Retention	Means the length of time for which records are to be kept. Thus it normally represents and will be expressed as a disposal period.
ICO-Information Commissioner's Office	The UK's independent authority who upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. www.ico.org.uk

Personal Data	Defined in s(1) of the DPA, as 'data which relates to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller' (the Council is a data controller), and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other in respect of the individual. At least one of the conditions in Schedule 2 to the DPA must be met to process personal data.
Processing	Covers a broad range of activities such that virtually any use of personal information or data will amount to processing.
Processed fairly and lawfully	Data must be processed in accordance with the 3 provisions of the DPA. These are the data protection principles, the rights of the individual, and notification.
Privacy Notice	As a minimum, a Privacy Notice should tell people who you are, what you are going to do with their information and how it will be shared with. However it can also tell people more than this. It can for example provide information about people's rights of access to their data or your arrangements for keeping their data secure. Whatever you include in your Notice, its primary purpose is to make sure that information is collected and used fairly.

Appendix 1 – Flowchart of Key Questions for Information Sharing