Information Governance Policy

??? 2021

Version Number	2.0
Approved by	Corporate Policy and Resources Committee
Date approved	27/10/2016
Review Date	27/10/2018
Authorised by	Director of Resources
Contact Officer	Information Governance Officer

Table of Contents

1 Overview

The 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, thereby protecting individuals, the council and its employees.

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.

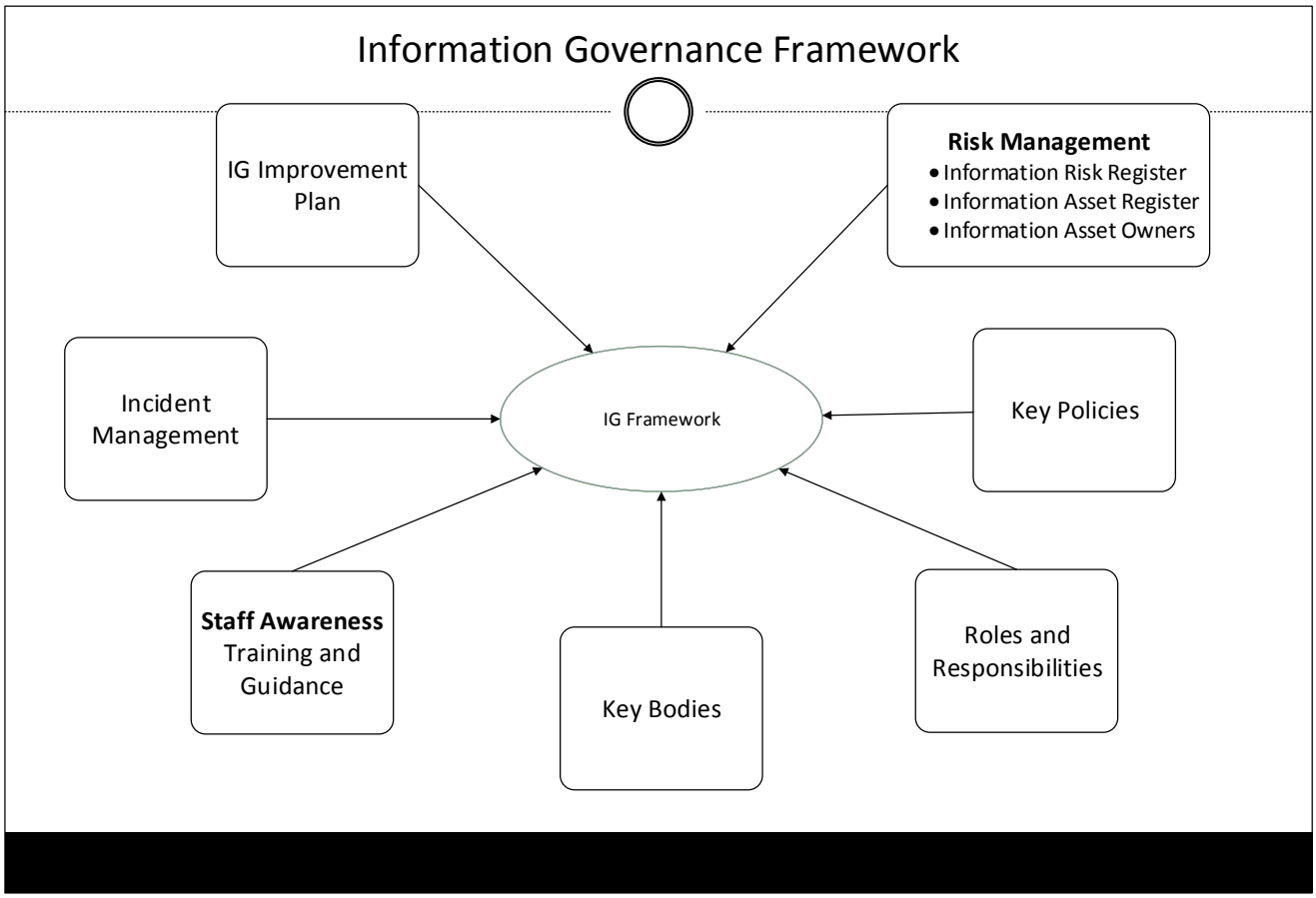
Information in whatever storage format and however transmitted (i.e. paper, voice, photo, video, audio or any digital format).

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.

Information Rights

The main legislation applying to information rights is the Data Protection Act 2018, the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and the UK GDPR. 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 of which the IT team will be responsible for 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 laid out in Articles 38 and Articles 39 of the UK GDPR. The Data Protect Officer shall have at least the following tasks:

- To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the UK GDPR and to other Union or Member State data protection provisions;

- To monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

- To provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

- To cooperate with the supervisory authority;

- To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matters.

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 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 by the IT Manager and from there feed into risk management and the information governance improvement plan.

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 2018 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 three 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.