# Information Governance Policy

**Document Control**

| | |
|---|---|
| **Organisation** | City of Lincoln Council |
| **Title** | Information Governance Policy |
| **Author – name and title** | Becky Scott, Legal & Democratic Services Manager |
| **Owner – name and title** | Becky Scott, Legal & Democratic Services Manager |
| **Date** | July 2018 |
| **Approvals** | July 2018 Executive |
| **Filename** | Information Governance Policy |
| **Version** | V.1.1 |
| **Protective Marking** | Official |
| **Next Review Date** | July 2020 |

**Document Amendment History**

| Revision | Originator of change | Date of change | Change description |
|---|---|---|---|
| V 1.1 | Becky Scott LDSM | June 2018 | Updating policy in view of General Data Protection Registration ("GDPR") and new Data Protection Act 2018 ("the Act"), and amendments to roles |
| | | | |
| | | | |

# 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/Data 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 City of Lincoln 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.

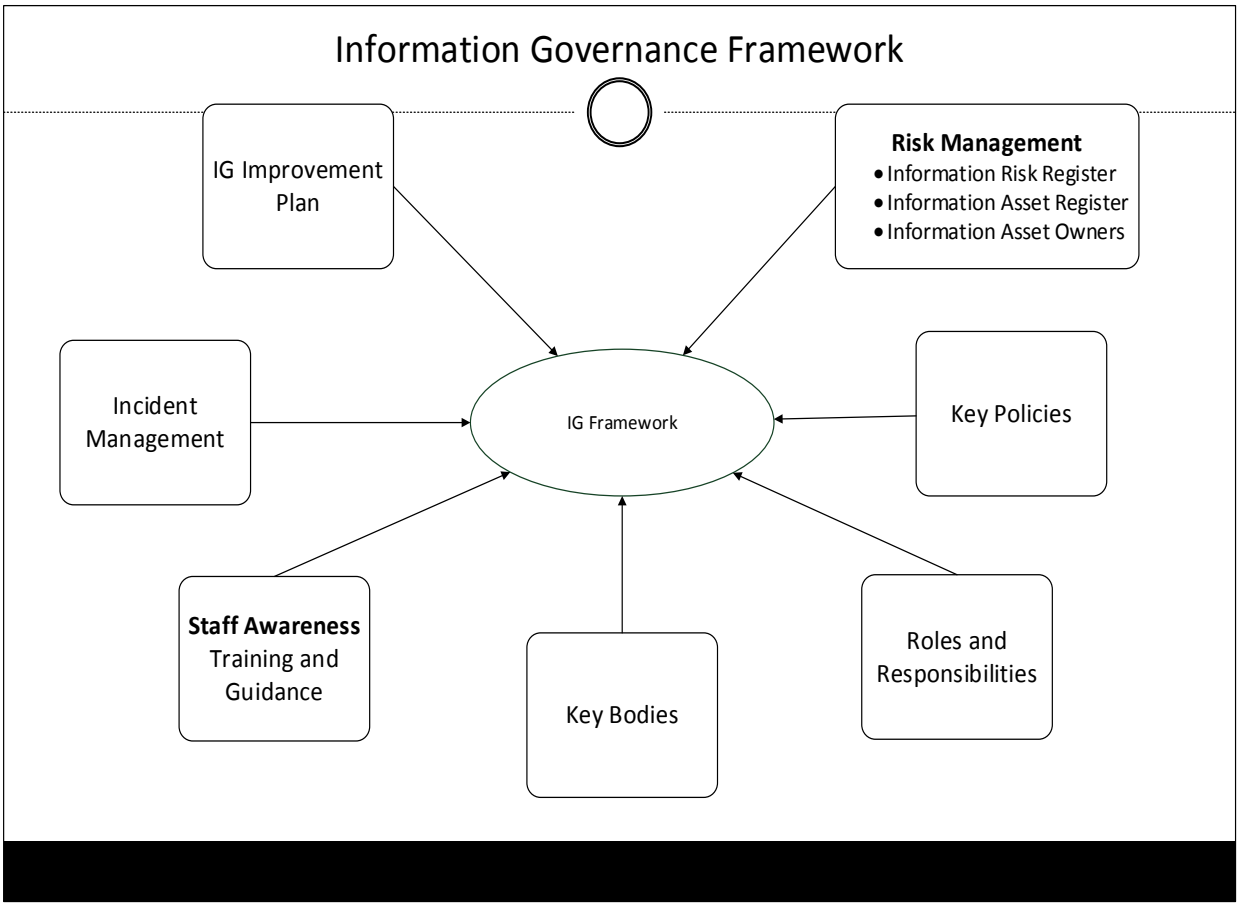
It applies to information in any storage format and however transmitted (including paper, voice, photo, video, audio or any digital format).

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




Note IG Improvement is the IG Action Plan

### 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 three 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.

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 2018 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 seven 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. There is a Data Protection Breach Management Policy to provide assistance in the event of an incident.

b. A Freedom of Information Policy the 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.

c. 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 Paragraph 6.

### 4.1.3 Information Governance Roles

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

**The Senior Information Risk Owner (SIRO)**

The SIRO will be a senior member of the management 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 directorate and 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 management team is adequately briefed on information risk issues.

**The Data Protection Officer** - The Data Protection Officer is the representative from the senior level of management who acts as the overall Information Governance Lead and co-ordinate the information governance work programme. The post is required under the new GDPR and is therefore a statutory requirement.. They will be accountable for ensuring effective management, accountability, compliance and assurance for all aspects of information governance. They will provide a focal point for the resolution and/or discussion of information governance issues.

Key tasks are to:

- To inform and advise the Council and its staff/members who carry out processing of their obligations pursuant to data protection laws;

- To monitor compliance with data protection laws of the Council's data protection provisions and policies, in relation to the protection of personal data, including the assignment of responsibilities, awareness training and training staff/members involved in processing operations and the related audits;

- To provide advice where requested as regards the data protection impact assessment and monitor its performance.

- To co-operate with the Information Commissioner's Office (ICO)

- To act as a contact point for the ICO on issues relating to processing, including prior consultation where required and where appropriate with regard to any other matter.

**Information Asset Owners**

The Information Asset Owners (IAO) 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:

- Complete a six monthly asset owner checklist which outlines their responsibilities, and include; identifying and documenting the scope, importance and process map of all Information Assets they own. The Information Asset Owner checklist is attached at Appendix A.

- 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 IT and Information Governance Board (AD Group) 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 in their teams 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.

- 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.

**Service 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.
- 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.
    - 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 data protection breaches/information security incidents.

### 4.1.4 Key Bodies

The Information Governance Strategy has been approved by the Assistant Directors Group who also sit as the Information Governance Board. They will receive updates at least every 3 months.

Audit Committee have changed their Terms of Reference to include a role of overseeing Information Governance and progress against the action plan. The Chair has taken on the role as lead Information Governance member and the committee will receive reports on a bi-annual basis.

### 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 will take place every two years.

- Additional training for all employees routinely handling 'sensitive personal information', as defined by the DPA 2018.

- All information governance policies and guidance to be available on the Intranet/City People.

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

#### 4.1.6 Data Protection Breach Management Policy

There will be a Data Protection Breach Management Policy and procedures that set out how incidents will be reported and managed. The results of incident investigations will be reported to the information governance working group and to the Information Governance Board (AD Group)

#### 4.1.7 Information Governance Action Plan

There will be an information governance action 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 quarterly to the Information Governance Board (AD Group), and bi-annually to Audit Committee.

## 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 relating to information management will be subject to scrutiny by the Policy Scrutiny Committee and/or the Audit 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.

### 5.3 Policy Review

This Policy will be reviewed every two years 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.