Information Strategy
2018-2022

Contents

1. Introduction and overview

Information is an important part of our daily working lives. South Lanarkshire Council recognises the importance of further maintaining/sustaining the framework it has developed to manage the information it creates and manages.

This Information Strategy sets out the Council's plans on how it intends to manage its information over the next four years.   It continues from the Information Strategy which was created in 2014 and expired in 2017

Information management can also be referred to as information governance but the principle is the same – appropriate and efficient management of information, in all formats, including electronic and paper.

Good information management brings together all of the requirements, standards and best practice that apply to the handling of information. It allows the Council and individuals to ensure that information is accurate, dealt with legally, securely and efficiently in order to deliver the best possible service. It will help protect individuals and the Council from the risk of data loss, theft or misuse.

This strategy makes the Council's aims and objectives clear in order to achieve the best information management framework possible, using the main themes of information governance as a basis.

- Information governance management
- Information security
- Information legislative compliance
- Records management
- Information sharing

It also highlights who is responsible and accountable for these and how we will implement, monitor and review the strategy.

There is already a range of good practice in evidence across the Council and these practices are being integrated with new policies and procedures being developed by the Information Governance Board (see 3.1).

2. Background and context

This section considers the nature of the information we hold, responsibility for managing it, the legal context, the risk posed by inadequate information management, before reviewing links to the Council plan, information management principles and the benefits of good information management.

2.1 Information management, legal and council context

As an employee, information management is your responsibility. Information plays a key role in all our daily working lives. The actions we take when processing data and information have an impact. We must make sure that the information we use is accurate, shared safely and managed in a secure way for the appropriate length of time that it is legally required.

Much of the information we hold contains personal information about individual members of the public, so when we are collecting, collating and presenting information, we must remember that we are looking after something which has personal significance for our service users.

In other instances the information we hold will be available on request with certain restrictions. We are all therefore custodians of information, responsible for managing and safeguarding it according to our range of policies, procedures and standards.

The pace of technological change has presented new opportunities as well as challenges in terms of information management for the Council. We have had to adapt in the way we are creating, using and handling information.

Data Protection, Freedom of Information and Environmental Requests
As well as being an important asset for the Council, information is also subject to various legislation such as the Data Protection Act 1998 (DPA), Freedom of Information (Scotland) Act 2002 (FOISA) and Environmental Information (Scotland) Regulations 2004 (EISR). This legislation requires that we have controls in place for managing information and also requires us to be open and transparent in allowing access to information.

General Data Protection Regulation (GDPR)
In May 2018 the Data Protection Act 1998 will be repealed and replaced with a new Act which will comply with the new GDPR which comes into force in the European Union on 25 May 2018. The Council requires to prepare for the new Act and to develop new procedures and review its current practices in order to be compliant.

Public Records (Scotland) Act 2011
As part of the requirements of the , the Public Records (Scotland) Act 2011, which came into force in January 2013, The Council prepared and submitted a records management plan (RMP) to the National Records of Scotland (NRS) outlining the way it manages its records. The RMP was approved by the Keeper of the Records at the NRS in June 2017, a number of improvement areas were highlighted and onging development of the plan will require to be monitored. This monitoring forms part of the Information Strategy.

Council risk register
 The Council has identified information management as one of the top risk areas in its 2016-17 risk register, with the risk being that it is "not subject to adequate control". Every year the register is reviewed and the risk of "information management not subject to adequate control" regularly appears in the top ten of Council risks.   In recognising this as a top risk the Council will expect managers to use corporate

policies and guidance to put in place appropriate local procedures to mitigate against a failing in this area. Employees must adhere to local procedures relating to their area of work.

2.2 Links to Council plan - Connect

Good information management will assist the Council in honouring its core values as outlined in the Council plan Connect 2017-2022

Ensuring that information is efficiently and appropriately managed will help the Council achieve its vision of improving quality of life for everyone in South Lanarkshire. This Information Strategy will support the Council's aims and objectives by collecting, protecting, storing and making available the information that the Council needs to inform its decision making process.

The Information strategy will contribute to the Council plan values of

- Accountable, effective, efficient and transparent
- Fair, open and sustainable
- Ambitious, self aware and improving
- Focused on people and their needs

It will also assist in the Council ambition to

- Achieve results through leadership, good governance and organisational effectiveness

2.3 Principles

To ensure good information management, attention must be given to the key principles in the following areas.

People
Everyone who works for the Council works with information and records. All Council employees must be aware of their role in good information management and how their contribution can really enhance the Council's performance in achieving its information governance aims. Employees must follow information management guidance to name, classify and store information more accurately. Doing this will improve the ease with which information can be retrieved. They must also follow procedures which are set down for the security of data, records and information.

Managers
Managers and team leaders must set a culture of good information management within their service. This responsibility should be evident from the top level down ensuring that information management and accountability is regarded as a key component of every business function the Council undertakes. Managers must take responsibility for the ownership of the data sets and information for which they and their team are responsible. In taking responsibility they must ensure that the information they manage is accurate, timely, relevant and not excessive. This will help the service by supporting informed decision-making.

Training is also a key activity in information management and managers must ensure that their team members receive appropriate and regular training on information management and its related topics. A suite of Learn On Line courses is available on information governance, information security and data protection.

Services must be prepared to be audited internally on compliance with the Information Strategy. Findings will be reported to senior management teams and the Corporate Management Team.

Processes
Good records management practices should be applied to all stages in the information lifecycle (see diagram depicting the lifecycle of a record under 3.4). Where corporate policies are in place these should be examined for local implications and operational procedures must be developed to comply. Local procedures and processes must be reviewed and monitored to ensure that good practice is maintained.

Technology
Technology solutions should support people and processes throughout the information lifecycle. Technology solutions that enable you to find and manage information across a range of electronic and paper based systems in straightforward and meaningful ways should be considered and adopted.

The Council will also act to minimise any risks to people's privacy that may be posed by the introduction of new information technology to existing processes. This will be achieved by undertaking privacy impact assessments and data protection compliance assessments at the start of any project.

2.4 Benefits

Benefits of good information management
Good information management will bring many clear benefits to the Council, its employees and for its customers.

For the Council

- The Council will have reliable information resources on which to support its decision making process
- Properly managed information and records will provide evidence of the Council's decisions
- There will be efficiencies in storage space, ease of retrieving records and ways of working
- The Council will have the confidence of having more security control over its information
- Having good information management in place will protect and augment the Council's reputation
- Ability to meet legislative obligations in terms of data protection, freedom of information and environmental information regulations
- Supports corporate working within the Council and collaborative working with outside partners

For customers and service users

- Customers' information will be securely maintained and protected
- The Council will not inappropriately disclose or share customer information
- Where appropriate, the Council will attempt to capture information once and not have to keep going back to the customer
- Our information will be more reliable, accurate, accessible and up to date and will not be stored longer than is necessary
- The customer journey with the Council will be improved through efficient availability of the appropriate information
- Customers will be assured that the decisions the Council makes are based on reliable and accurate information

For the employee

- There will be an improved working environment
- It provides easier and efficient ways to find the information required which means less frustration
- The quality of the information can be trusted
- There will be the potential for increased productivity due to the fact that information will be easier to find
- A good framework will give employees more guidance on what to keep and what to destroy and defined guidance on how to store the important information
- There will be clearer guidance on how to share information which will lead to improved partnership working
- Provides guidance on how to meet our legal obligations
- Helps employees maintain the security of information for our customers

3. Objectives for information governance 2017-2021

3.1 Information governance management

The Information Governance Board was established in January 2010. The board takes responsibility for information management policy, training and practice within the Council. It is chaired by the Head of Administration and Legal Services and reports to the Executive Director (Finance and Corporate Resources) who is also the Senior Information Risk Officer (SIRO). The board reports its progress to the Council's Corporate Management Team. The board is made up of managers from all Resources. Action plans are reported to the Resource Senior Management Teams as appropriate, for prioritisation and implementation. In terms of scrutiny, management of the information governance risk will be reported to the Risk and Audit Scrutiny Forum.

Information management contributes to the values and ambitions of the Council plan – Connect 2017-2022 and measures to record performance in this area are recorded on IMPROVe (the Council's performance measurement system). These measures are subject to scrutiny by the Executive Directors and Chief Executive.

This Information Strategy is approved by the Corporate Management Team and the Council's Executive Committee and will be reviewed every four years. (See 6.2)

Information governance is therefore managed at a corporate, senior manager and operational level across the organisation.

We will ensure that this management hierarchy for information governance is maintained.

Strategic objective:
To further strengthen the culture of information governance for all employees of South Lanarkshire Council.

3.2 Information security

Our Information Security Policy is based on the international security management standard ISO27001. This management standard provides guidance on best practice and identifies the controls that are recommended to protect information assets in electronic, paper as well as other formats such as disks or tapes.

Where these controls are appropriate to the legislative obligations and business needs of the Council they are mandatory and must be implemented.

The policy covers the key areas of control identified in ISO27001:

- security policy
- security organisation
- asset management

- personnel security
- physical and environmental security
- computer and network management
- access control
- information systems acquisition, development and maintenance
- information security incident management
- business continuity planning
- compliance

Our Information Security Management System will ensure that appropriate risk management processes are in place for each information asset.

A range of business continuity and disaster plans have been put in place and asset registers, identifying the information holdings of the Council, have been created through the information audit process.. Where appropriate, risk assessments will be carried out to identify potential threats and appropriate controls will be put in place. Security procedures will be developed to safe-guard how we manage our paper files with such measures as file tracking processes being introduced and access control being placed on physical storage.

Information security incident reporting procedure
Mention new information incident reporting procedure and information asset owners as per review of Information Security Policy.
There are policies and procedures and codes of practice already in place to support this area and these include the Information Security Policy, IT Acceptable Use Policy, the Employee Code of Conduct, Privacy Policy, Confidential Waste Policy, as well as our Corporate Standards.

We will continue to apply and review these on a regular basis.

Strategic objective:
All information created, received, managed and processed by South Lanarkshire Council will be kept secure and protected.

3.3 Information legislative compliance

Our information compliance policy sets out how we deal with requests for information from the public. It also explains who is responsible for ensuring that we comply with the legislation. The Data Protection Act 1998 (DPA) and the Freedom of Information (Scotland) Act 2002 (FOISA) cover records management. The DPA controls how we use personal data. The DPA is being repealed and replaced in May 2018 and a new Act will be put in place aligning with the General Data Protection Regulation coming into force in the European Union on 25 May 2018.

All legislative compliance issues are dealt with through the Information Governance Board.   A network of resource representatives coordinates information requests and responses under FOISA, the DPA and the Environmental information (Scotland) Regulations 2004. The information compliance manager coordinates Council wide subject access requests under the Data Protection Act and advises on our use of personal data.

Other relevant legislation covered includes the Pupils' Educational Records (Scotland) Regulations 2003.

We will continue to manage information requests using the guidelines and procedures established by the Information Governance Board and review the information compliance policy at appropriate intervals.

General Data Protection Regulation (GDPR) and new DPA

On 25 May 2018 the GDPR comes into force and the United Kingdom will have replaced the DPA with a new Act. The Council has prepared a GDPR action plan and is preparing and working towards compliance with the new regulation. All Resources are working together to develop the necessary procedures and put in place the required processes in order to comply with the new legislation.

Information quality assurance

To comply with the DPA and GDPR the Council requires to ensure that it holds good quality data and information.

The key characteristics of good quality data are:
- accuracy – data should be sufficiently accurate for its intended purposes;
- validity – data should be recorded and used in compliance with relevant requirements;
- reliability – data should reflect stable and consistent data collection processes across collection points and over time;
- timeliness – data should be captured as quickly as possible after the event or activity and must be available for the intended use within a reasonable time period. Data must be available quickly and frequently enough to support information needs and to influence service or management decisions;
- relevance – data captured should be relevant to the purposes for which they are used;
- completeness – data requirements should be clearly specified, based on the information needs of the Council, and data collection processes matched to these requirements.
- it should not be excessive – especially in terms of personal data only the minimum should be collected
- that it is not kept for longer than necessary – data must be collected for appropriate business requirements only

Scanning electronic files

Scanning procedures for EDRMS will be reviewed, revised and applied as required to meet BS10008: Evidential weight and legal admissibility of electronic information. We want to ensure that records created during the scanning process containing signatures are legally admissible[1] allowing for the destruction of hardcopy files after a retention period appropriate to the information set. We will ensure, on a case by case basis, that we hold records in a format that will comply with legal admissibility only duplicating format where necessary.

Strategic objective:
To ensure that South Lanarkshire Council complies with information management legislation and adheres to information management best practice, standards and codes of practice
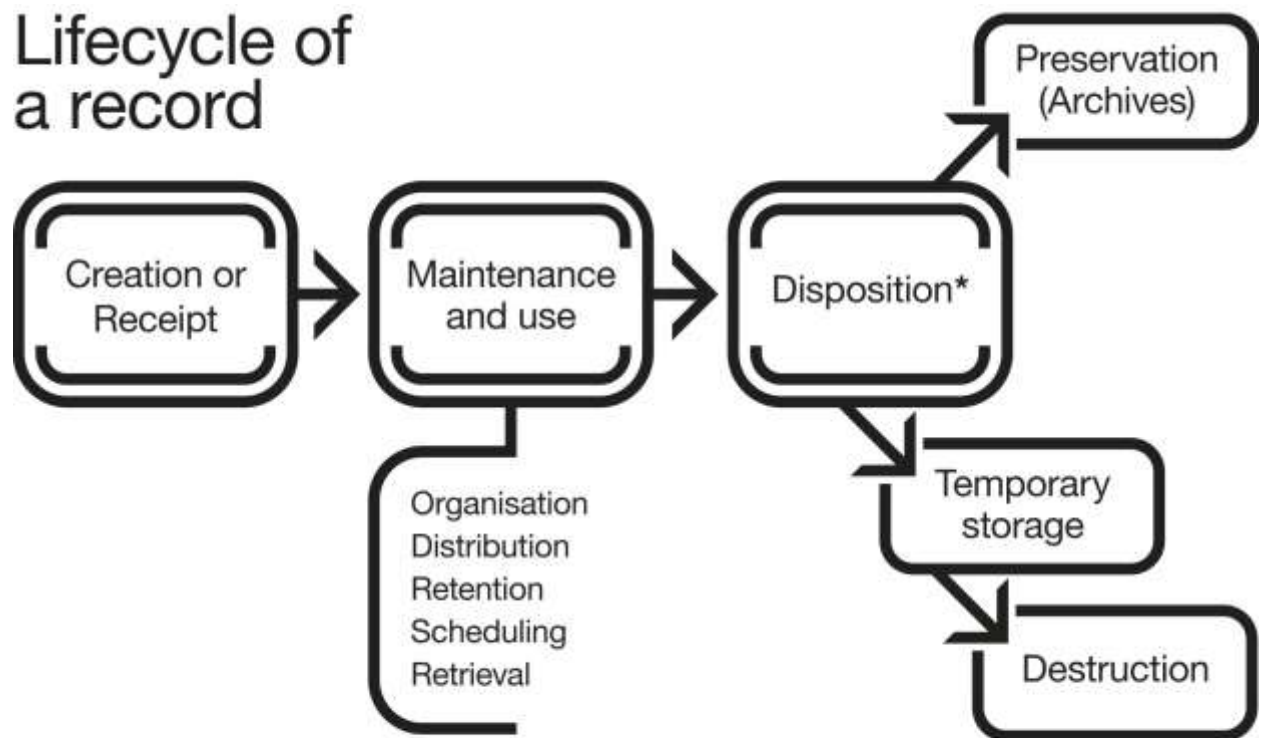
---

[1] Of sufficient quality to be used as evidence in court

3.4 Records management

It is essential that the records the Council creates, receives, manages and processes when carrying out its business activities are properly managed.

Records management covers the process of creating, describing, using, storing, archiving and disposing of organisational records according to a defined set of standards. This applies to all records including paper, electronic records, emails, CCTV footage, DVD, CD, VHS and digital. Good records management helps us comply with the principles of Data Protection and respond to freedom of information enquiries. It will also help the Council meet its obligations under the Public Records (Scotland) Act 2011.

It is the responsibility of the people who create, use, transfer and destroy the Council's information and records to make sure, that at each and every stage of its lifecycle, it is managed appropriately.

Lifecycle of a record

Creation or Receipt → Maintenance and use → Disposition*

Maintenance and use:
Organisation
Distribution
Retention
Scheduling
Retrieval

Disposition* → Preservation (Archives)
Disposition* → Temporary storage → Destruction

★ **Disposition** - This is the stage at which the decision is taken to either transfer the record to temporary storage and/or destruction or permanent preservation.

The main principles upon which records management is implemented throughout the Council are:
- All employees should create the necessary records to provide comprehensive, reliable and authentic evidence of the organisation's decisions and activities

- Records are subject to a retention/disposal policy and supporting schedules which are properly implemented to ensure records are destroyed or transferred elsewhere at the appropriate time
- There will be provision for the preservation and secure storage of records for as long as they are required
- All systems and processes dealing with records ensure the quality and reliability of the organisation's records

We will continue to review our policies and procedures on records management to ensure they are relevant to the needs of the organisation.

Electronic records management and digital preservation
A large percentage of the records the Council processes are now what is known as "born digital" meaning that the records exist in electronic format and may never become a paper record. This poses additional challenges for the Council in terms of the management of these records.   Digital records that are required to be retained for long periods of time e.g. Some Social Work children's files which have a retention period of 100 years, must be monitored for the duration of their life cycle to ensure that they will be accessible and usable in 100 years time. Digital preservation strategies include making sure that there is more than one copy of the data, held in different locations, making sure that the data is stored in a format that will be easily accessed in the future and monitoring the file at regular intervals to ensure that it is still accessible. In order to plan effectively for the future, the Council requires to assess its digital preservation requirements. An action to take this forward, and identify the associated implications will be incorporated into the Information Strategy Action Plan.

Records Management Plan
South Lanarkshire Council submitted a records management plan under the Public Records (Scotland) Act 2011 which was approved by the Keeper of the Records in June 2017.

The records management plan (RMP) will help the Council meet its statutory obligations, introduce improvements and efficiencies and assist the Council in responding to its users' needs. It will allow the Council to better monitor its services, maintain accurate records of the circumstances and experiences of individuals, and safeguard the records of vulnerable people.

The RMP must be updated on a regular basis and will require to be refreshed and re-submitted to the National Records of Scotland in five years time.

A number of areas for improvement were highlighted in the Keeper of the Records' assessment report on South Lanarkshire Council's RMP. These included action in the following elements of the plan:
- Element 4 Business Classification
- Element 5 Retention Schedule
- Element 6 Destruction Procedures
- Element 11 Audit Trail

Electronic Document Records Management System (EDRMS)
An area of strategic importance in terms of records management is the implementation of a replacement EDRMS across the Council. The new EDRMS will be implemented across Council business areas from 2018 on a phased basis. This

programme will eventually replace the Council's shared network drives for document storage, with few exceptions.

Strategic objective:
South Lanarkshire Council will ensure that records are properly managed for the duration of their lifecycle

3.5 Information sharing

Information sharing covers the proper governance of information sharing practice across South Lanarkshire Council and its partners. It is essential that care is taken when sharing information as this could potentially involve sharing personal information about our customers, staff and other stakeholders. It is our duty of care to ensure that we adhere to the highest quality of standards and that our protocols meet with Data Protection legislation. The Council and its partners need to work effectively and efficiently together to tailor services to the individual needs of its customers and service users. Sharing information between parties is vital to the provision of certain services but it is also important to maintain a certain degree of security to guarantee the confidentiality, integrity, and availability of information resources.

Our data sharing policy deals with the following areas:

- Definitions of information that requires to be protected
- Identification of potential threats to the security of the information
- Protective measures which can be put in place to prevent breaches of security
- Determining information access protocols
- Defining roles and responsibilities
- Monitoring the effectiveness of the policy

The strategy takes account of the Lanarkshire Information Sharing Protocol and each agency's employees have different access permission levels to shared information.

There is also other guidance available for information sharing including the Scottish gold standard protocol for health, education and social care services and the UK framework code of practice for sharing personal information developed by the Information Commissioner.

We will ensure that information-sharing protocols are established, maintained and reviewed in all areas of our activities and service provision.

Knowledge sharing
Less tangible than information, knowledge is however an extremely important asset of the Council. It is increasingly important when resources are limited or reducing that organisational knowledge is shared in order to minimise mistakes, avoid unnecessary effort and make informed decisions. This can be achieved through both formal and informal approaches to knowledge management. There are a range of tools and techniques in this area, from the improved use of contact databases to find people in the know - to using communities of practice to share knowledge and expertise.

We will support the use of appropriate knowledge management tools and techniques to improve knowledge sharing within the Council and with others outside.

Strategic objective:
The Council will actively share information with other organisations adhering to data sharing protocols and procedures which ensure the appropriate level of security.

4. Accountabilities and responsibilities

4.1 Accountabilities

There is shared accountability amongst all employees across the Council for information management. However, specific officers have accountability for:
- Information governance management (Finance and Corporate Resources Executive Director and Head of Administration and Legal Services)
- Senior Information Risk Officer (SIRO)
- Information security (Information Security Manager)
- Information compliance (Information Compliance Manager)(may come out)
- Data Protection Officer (to be confirmed)
- Information quality assurance (Data custodian for property information, managers)
- Records management (Administration Adviser, Resource electronic records managers/Administration officers)
- Information sharing (IT Business Systems Managers, Information Asset Owners (as noted in Information Audits),)
- Data controller (the Council)

The Information Governance Board is responsible for co-ordinating the creation of this strategy, implementing associated actions and monitoring their progress.

4.2 Responsibilities

The Council is responsible for the information assets it owns and possesses. However, responsibility is delegated as follows to certain custodians, information authors and users (see definitions, below).

All – You are responsible for your wider personal actions as an employee of the Council, ensuring there are no conflicts of interest. This includes your responsibilities under the code of conduct, including confidentiality and not using Council information for your own use.

Employees – responsible for applying the range of information management policies and procedures in their day-to-day activities.
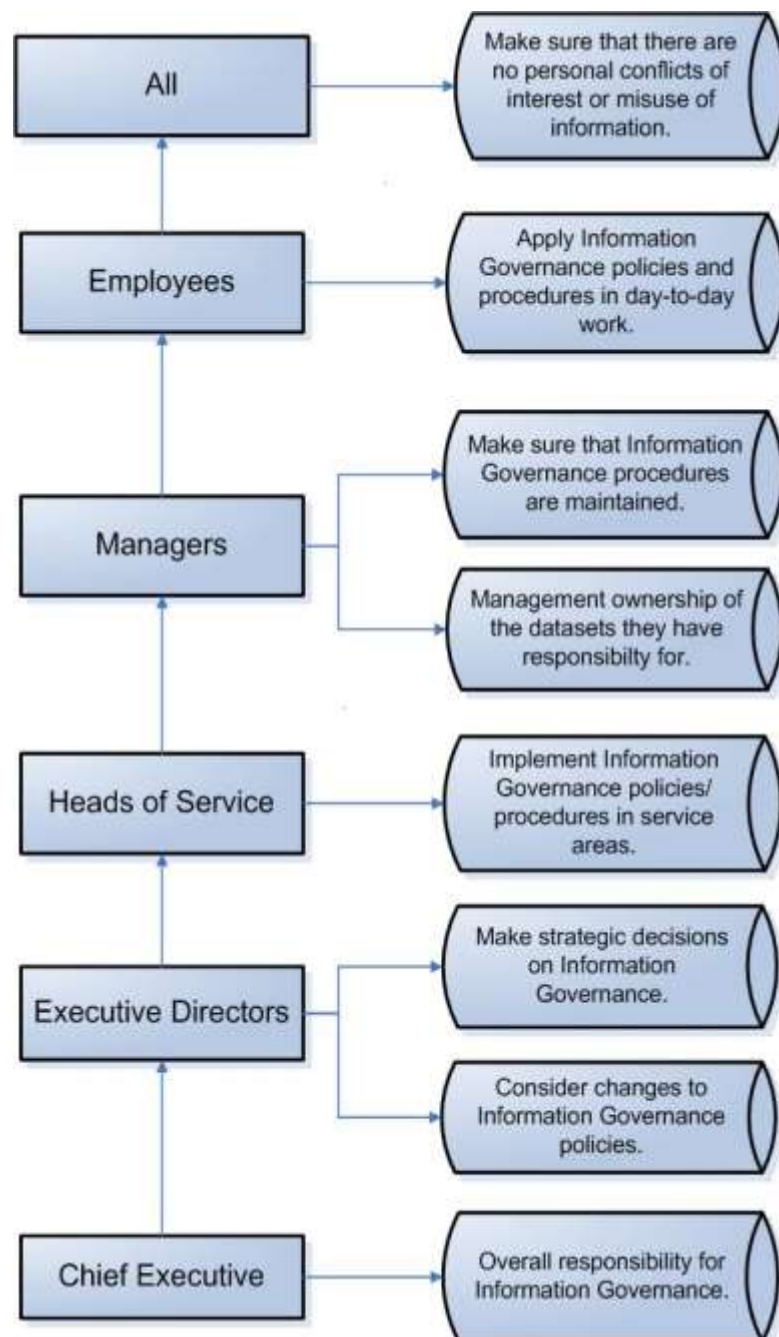
Managers - responsible for:
- taking management ownership of data sets they are responsible for,
- information quality assurance
- ensuring that information management procedures are maintained. These could be subject to inspection by Internal Audit
- ensuring data sharing protocols are adhered to

Heads of Service – responsible for ensuring information management polices and procedures are implemented within service areas.

Executive Directors – responsible for strategic decisions on information governance and approval of relevant policies dealing with the themes of information security, information compliance, information quality assurance, records management and information sharing.

Chief Executive – overall responsibility.

Who has responsibility for what?

Role	Responsibility
All	Make sure that there are no personal conflicts of interest or misuse of information.
Employees	Apply Information Governance policies and procedures in day-to-day work.
Managers	Make sure that Information Governance procedures are maintained.
Managers	Management ownership of the datasets they have responsibilty for.
Heads of Service	Implement Information Governance policies/procedures in service areas.
Executive Directors	Make strategic decisions on Information Governance.
Executive Directors	Consider changes to Information Governance policies.
Chief Executive	Overall responsibility for Information Governance.

5. Policies and procedures

5.1 Existing policies, procedures and training

A number of existing policies, procedures and training courses are available to support the main themes of information management. These polices are all available to employees on the Council intranet and the courses are available on Learn On Line. There are also individual resource procedures which support how information is handled on a local level.

A list of these policies, procedures and relevant training is available in appendix 1.

6. Implementation, monitoring and review

6.1 Information Strategy Improvement Action Plan

An Information Strategy Improvement Action Plan has been developed to accompany the Information Strategy. The plan includes action from each of the main themes of the strategy and links each task to a main strategic objective.
The Information Strategy Improvement Action Plan is available as appendix 2.

6.2 Monitoring and review

The action plan is reviewed regularly by the Information Governance Board. Regular reports are also submitted to the Corporate Management Team in order to satisfy them that the appropriate controls are in place to ensure good information management across the Council.

Measures to record performance on information governance are monitored and assessed via the Council's performance management system – IMPROVe.

This Information Strategy will be refreshed every four years and will be approved by the Corporate Management Team and the Council's Executive Committee as part of this process.

Information management will also be monitored on the Council's risk register with annual reviews taking place.

Internal Audit
The Council's Internal Audit Team also incorporate regular information governance internal audit investigations into their annual audit programme. They will also independently review the Information Strategy Improvement Action Plan by taking a sample of the actions when they are completed to provide an independent assurance that they are completed as intended.

Records Management Plan
The Council will be required to keep its Records Management Plan up to date and regularly reviewed. It will require to be refreshed and re-submitted to the Keeper of the Records at the National Records of Scotland every five years.

7. Strategic objectives - summary

The main strategic objectives of the information strategy are summarised below:-

Information governance management

Strategic objective:
To further strengthen the culture of information governance for all employees of South Lanarkshire Council.

Information security

Strategic objective:
All information created, received, managed and processed by South Lanarkshire Council will be kept secure and protected.

Information legislative compliance

Strategic objective:
To ensure that South Lanarkshire Council complies with information management legislation and adheres to information management best practice, standards and codes of practice

Records management

Strategic objective:
South Lanarkshire Council will ensure that records are properly managed for the duration of their lifecycle

Information sharing

Strategic objective:
The Council will actively share information with other organisations adhering to data sharing protocols and procedures which ensure the appropriate level of security.

Appendix 1

Policies, procedures and training courses

Subject title	Policies and procedures	Training courses
Information governance management	Information Strategy Employee Code of Conduct	Information Governance – an Introduction - Learn On Line course
Information security	Information Security Policy Confidential Waste Policy Risk Bulletins	Information Security - Learn On Line course
Information legislative compliance	Information Compliance Policy Freedom of Information Policy Privacy Policy Information Security Incident Notification Process Data Protection Subject Access Procedure Privacy Impact Assessment Guidance	Introduction to Data Protection - Learn On Line course How Data Protection Works - Learn On Line course Suite of Freedom of Information courses
Records management	Records Management Policy Retention schedules Retention and Disposal Policy EDRMS procedural documentation Version Control Guidance Naming Convention Guidance Confidential Waste Policy	Records Management – Learn On Line Course
Information sharing	Data Sharing Policy Lanarkshire Information Sharing Protocol – Good Practice Guide CCTV Operation and Information Management Policy	Data Sharing - Learn On Line Course Information Sharing Protocol