WEST LOTHIAN COUNCIL INFORMATION GOVERNANCE POLICY

Data Label: Public

INFORMATION GOVERNANCE POLICY

CONTENTS

1. INTRODUCTION

Information is a vital council asset that helps service areas and partners in delivering improvement to services and supporting better outcomes for local people as set out in the council's Corporate Plan 2023/24 to 2027/28. It plays a key role in council governance, service planning and performance management. Good information governance monitors, improves and provides assurance that the council create, acquire, manage, use, share, dispose of and preserve information efficiently, appropriately and lawfully.

This policy defines accountabilities and responsibilities of all who handle and manage council information. It establishes the principles of information governance and how these are achieved. This policy covers compliance with key information legislation such as, Data Protection Act 2018 and UK GDPR, Freedom of Information (Scotland) Act 2002, Environmental Information (Scotland) Regulations 2004 and the Public Records (Scotland) Act 2011.

The Head of Corporate Services, in consultation with the Senior Information Risk Owner, is authorised to adjust the wording of this policy to reflect changes in management structures, job titles, legislation, guidance, codes of practice and industry standards where those changes do not represent any meaningful change to the policy. Meaningful changes require committee or council approval. The procedures and management guidance which supports this policy are prepared and implemented by the Head of Corporate Services under the guidance of the Governance & Risk Board.

The appendices to this Policy set out the following:

- Appendix 1 – sets out definitions of specific terms used in this policy.
- Appendix 2 – sets out relevant acts, regulations, codes of practice and standards.

2. INFORMATION GOVERNANCE PRINCIPLES

The following principles drive activities relating to effective information governance within West Lothian Council:

- Information is a **valuable asset** and is managed as such;
- Information governance is the **responsibility of all** who handle or manage council information;
- Information is acquired, created, maintained, shared and disposed of in **accordance with legislation**, **regulations**, **guidance**, **standards** and **best practice**;
- The rights of data subjects are recognised and respected in all aspects of Information governance;
- Information is appropriately **secured** and **protected**;
- Information is **shared** appropriately and **not duplicated** unnecessarily;
- Information is **stored within approved systems** not in personal filing;
- Information is **accessible** and **preserved** for as long as required;
- Staff are **trained** in information governance procedures;
- Risks are identified and mitigated;

- Information governance **supports the council values** being open, honest and accountable.
- Councillors have **awareness**, **oversight**, the opportunity and ability to **scrutinise** information governance and regulatory compliance;
- Information governance practice is **compliant with duties** under the Equality Act 2010 and Human Rights Act 1998.

3. SCOPE

- **Information** – All information, records and data held, maintained and used by, or on behalf of, the council in all locations and in all formats (electronic and physical).
- **Staff** – All council employees and workers, such as, contractors, consultants, volunteers and agency staff that have authorised access to council information/systems or process council information.
- **Systems** – All systems used for storing, processing, managing and sharing council information.
- **Third parties** – All third party organisations that process information on behalf of the council in partnership and or under contract or agreement.

4. RESPONSIBILITIES

4.1. Senior Information Risk Owner (SIRO)

The Depute Chief Executive (Corporate, Operational and Housing Services) serves corporately as the council's Senior Information Risk Owner (SIRO) in relation to information governance and security related matters. The SIRO understands the strategic business goals of the council, how business goals may be impacted by information risks and how those risks may be managed. The SIRO implements and leads the information governance risk assessment and management processes within the council and advises on the effectiveness of information risk management.

4.2. Heads of Service

Heads of Service are ultimately responsible for information, including that of a personal or sensitive nature, processed within, or on behalf of, their respective services. Responsibilities include:

- Appointing and supporting officers responsible for the implementation of compliance measures;
- Accounting for information risks in service planning, strategies, projects and resourcing;
- Ensuring appropriate communications, contractual and legal arrangements are in place for any third party accessing or processing council information;
- Ensuring that information governance principles and standards of operation are consistently enforced;
- Ensuring that staff are appropriately trained in, and comply with, this policy and associated procedures;
- Ensuring business continuity plans and processes are in place to safeguard information from inappropriate access, loss, removal or destruction and that any breaches are identified and appropriately responded to;

4.3. Data Protection Officer (DPO)

The council has appointed the Information and Systems Manager as the council's Data Protection Officer (DPO). The DPO informs and advises the council with data protection obligations, including:

- Establishing arrangements that recognise and respect the rights of data subjects;
- Maintaining comprehensive records of all data processing activities (ROPA);
- Proactively monitoring, reporting and communicating internal compliance with data protection law;
- Advising staff on their data protection responsibilities;
- Ensuring appropriate arrangements are in place between the council and other organisations processing or sharing personal data;
- Managing, reporting and notifying of data protection breaches;

The DPO also acts as a point of contact for data subjects and the supervisory authority, the Information Commissioners Office.

4.4. Corporate Governance Board

The role of the board is to ensure that effective corporate governance arrangements are in place. As part of these arrangements, the board instructs the work of and receives reports from various Working Groups covering Governance, Risk Management and Information Management.

4.5. Data Controllers/Processors

To provide services, the council may share personal information with third parties, such as, NHS, Police, other Local Authorities and Charities. Third parties may also process data on behalf of the council. These arrangements are formalised in agreements, such as, Integration Schemes, Memorandum of Understandings (MOU), Data Sharing Agreements, Data Processing Agreements or Contracts. Each arrangement identifies the organisation(s) that act as Data Controller(s) or Data Processor(s).

Data Controller

For some processing activities, the council is a data controller. This means that the council is accountable for when and how personal data is collected and processed. To provide joined up services, the council may be a joint data controller with other organisations.

Data Processor(s)

To deliver services, there may be other organisations or third parties that carry out work and process personal data on behalf of the council. The council may also act as a data processor for other organisations.

4.6. Service Managers

Service Managers assume delegated responsibilities that include:

- Ensuring that records of council activities, business, decisions, its history and inhabitants are appropriately created, shared, secured, protected, archived and disposed of;

- Ensuring the service entries in the Information Asset Register is accurate and regularly reviewed;
- Ensuring that statutory requests for information are appropriately handled and responded to;
- Ensuring the proactive publishing of information wherever appropriate;
- Ensuring that staff are aware of the disciplinary and/or legal consequences of any breach of this policy and associated procedures;
- Managing their service investigation, response and resolution of security incidents and data breaches;
- Owning and managing service Data Protection Impact Assessments (DPIAs) and Risk Assessments associated with information systems and processes;
- Completing annual compliance reviews.

4.7. Business Support Service

The service is responsible for:

- Supporting the DPO in the delivery of the Information Governance arrangements across the council in line with current legislative requirements;
- Leading on the implementation of the Public Records (Scotland) Act 2011 within the council. Providing support to service areas on the development and application of local records management practice supported by the council's Records Manager, in accordance with the Council's Records Management Plan;
- Supporting the development of the council's information asset register and file plans;
- Developing this policy and assisting in the maintenance of associated guidance;
- Providing advice and guidance on the completion of DPIAs and arrangements;
- Developing council retention schedules and supporting the implementation of record disposals in council information systems;
- The storage, management and disposal of council records held within the records store;
- Applying council retention schedules to implement record disposals within the records store.

4.8. IT Services

IT Services are responsible for:

- Managing information security configurations, information system backups and disaster recovery capability;
- Identifying, monitoring, mitigating and managing system and application vulnerabilities and cyber-attacks in conjunction with services, partners and suppliers;
- Developing and maintaining cyber security standards and procedures;
- Co-ordination, advocacy and the management of risks concerning cyber security and information security;
- Monitoring and reporting on device inventories, access and security logs;
- Providing evidence and analysis of log information for periodic audits, compliance checks and investigations;
- Acting as sign-off authority on the council's firewall and network security changes and updates;

- Ensuring compliance standards are met for the Public Services Network (PSN) and Cyber Essentials.

4.9. Legal Services

Legal Services support the council and other services by providing advice and guidance relating to:

- Particular legal issues regarding the handling of information requests and the application of exclusions or exemptions;
- Developing data sharing protocols and agreements between the council, third party organisations and other partner agencies;
- Compliance requirements where the processing of personal data is complex (e.g. multi-agency working);
- The application of the law to the handling and management of personal/ special category data.

4.10. Information Liaison Officers (ILOs)

Information Liaison Officers are nominated representatives from each service. They primarily have responsibility for co-ordinating, monitoring compliance activities. Responsibilities include:

- Acting as a point of contact for information governance and compliance issues affecting their services;
- Providing support to staff and managers on the implementation of the Information Governance Policy, associated procedures and training;
- Maintaining the council's Records of Processing Activities (ROPA) and Information Asset Register (IAR);
- Co-ordinating, processing, advising on and responding to information and subject access requests;
- Co-ordinating reviews of the council's Records Retention Schedules;
- Monitoring and reviewing the effectiveness of the Information Governance Policy and procedures.

4.11. Museum and Archives Service

The Museum and Archives Service is responsible for the preservation and management of all historical records held by the council, including private deposits held under defined terms of acquisition. Responsibilities include:

- Records of historical significance are identified and permanently preserved;
- Review and appraise Archive deposits and transfers;
- Maintaining and communicating the Archives Acquisition process;
- Managing archival records held by the council, including appraisal, accessioning, storage, cataloguing, preservation, conservation and provision of access;
- Management and care of museum collections in accordance with the UK Museum Accreditation Scheme.

4.12. Staff

Managing information effectively and lawfully is the responsibility of all staff. All staff take responsibility for adhering to this policy and associated guidance for the information they acquire, create, file and handle. Staff are responsible for:

- Understanding their responsibilities and respect the confidentiality of information they access, produce, share or receive;
- Treating information as an asset and filing it in approved systems;
- Raising information governance issues with their line manager;
- Reporting any potential security incidents or breaches to their Line Manager and the IT Service Desk;
- Assisting individuals to understand their rights and the council's responsibilities under the legislation covered by this policy;
- Completing information governance related training.

4.13. Elected Members

This policy does not change any duties, rights or responsibilities imposed by any other enactment. Elected Members are subject to the same rules that apply to employees when acting as a member of committee or personally in relation to information controlled or processed by the council and when the rights of data subjects in relation to that information apply. Elected members are data controllers under GDPR and are responsible for the personal data that they collect, store, use and delete.

When acting on behalf of a member of the public, Elected Members are entitled to have access to information held by the council where it is reasonably required for them to perform their councillor duties. Requests for personal data will be dealt with by officers under the relevant regulations and ICO guidance on the provision of personal data to elected representatives and the council's Officer/Member Protocol. That may require the authorisation by the data subject.

5. POLICY OBJECTIVES

5.1. The council comply with legislation and regulations

This policy and associated guidance have been developed within the context of national legislation, regulations, professional standards and codes of practice. As far as is practical, this policy addresses as a minimum the principles defined within the following legislation and regulations:

- **Data Protection Act 2018**

  The Data Protection Act 2018 (DPA) and UK General Data Protection Regulation (GDPR) requires all organisations that handle personal data, special category data and criminal offence data (hereby referred to as personal data) to comply with data protection principles. Further provisions with regards to the councils processing of special category data are detailed in the council's Special Category Data Policy.

  1. ***Principle (a) - Personal data is processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency').***
     The council only process personal data where there is consent to do so or where one of the conditions detailed in data protection law apply. The council also process personal data to comply with other obligations imposed on the council in its capacity as a public authority, such as, those detailed in the Equality Act 2010.

The council keep records of its processing activities in respect of personal data in accordance with the requirements of Data Protection law. In order to collect and process personal data for any specific purpose, the council must have a lawful basis for doing so. The council provide clear and transparent information about our processing of personal data including the lawful basis for each specific purpose or group of related purposes in privacy notices.

Where the council obtains any personal data about a data subject from a third party, appropriate checks are conducted to ensure that the sharing of that data is lawful.

2. ***Principle (b) - Personal data is obtained for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')***
   The council only collect personal data for specified, explicit and legitimate purposes, and we will inform data subjects what those purposes are in a privacy notice. Specifically, the council process personal data for purposes of substantial public interest when the processing is necessary for us as a local authority to fulfill our statutory duties, to establish whether an unlawful or improper conduct has occurred, to protect the public from dishonesty, preventing or detecting unlawful acts or for disclosure to elected representatives. As a public authority, we are authorised by law to process personal data for these purposes. We may process personal data collected for any one of these purposes or, for any of the other purposes, providing the processing is necessary and proportionate to that purpose. If we are sharing data with a third party, we will document that they are authorised by law to process the data for their purpose. We will not process personal data for purposes that are incompatible with the reason(s) for which it was collected. The council specify the lawful basis for processing in its privacy notices.

3. ***Principle (c) - Personal data processed is adequate, relevant and limited to what is necessary ('data minimisation').***
   The council minimise the processing of personal data to only the necessary information that it needs to fulfil its purpose. We ensure that the data we collect is adequate and proportionate to our identified purposes.

4. ***Principle (d) - Personal data is accurate and, where necessary, kept up to date ('accuracy').***
   The council has procedures in place to ensure the accuracy and currency of the personal data it processes. Where inaccuracies are discovered or notified to us, we will take every reasonable step to rectify or erase that data without delay. If we decide not to either erase or rectify it we will document our decision.

5. ***Principle (e) - Personal data is not to be kept longer than is necessary for that purpose ('storage limitation').***
   The council maintain retention schedules to ensure that personal data is only kept for as long as is necessary for the purposes for which it is collected, or where we have a legal obligation to do so. We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs. The periods for which the council holds personal data are contained in its privacy notices.

6. ***Principle (f) - Personal data is appropriately secured and protected ('integrity and confidentiality').***
   The council takes appropriate technical and organisational measures to prevent unauthorised or unlawful processing, loss, damage or destruction of personal data.

7. ***The Accountability Principle – data controllers must be responsible for, and be able to demonstrate, compliance with these principles.***
   The council is accountable for the data that we process and we are able to demonstrate compliance with the previous principles. The council has a number of measures in place including:
   - The appointment of a data protection officer who reports directly to our highest management level;
   - Taking a 'data protection by design and default' approach to our activities;
   - Maintaining documentation of our processing activities;
   - Adopting and implementing appropriate policies and ensuring we have written contracts in place with third party data processors;
   - Implementing appropriate security measures in relation to the personal data we process;
   - Carrying out data protection impact assessments for our high-risk processing;
   - We regularly review our accountability measures and update or amend them when required. The council maintain procedures for the management of personal/special category data and individual's rights. These documents set out individual's rights and explain the process for enacting these rights.

- **Closed Circuit Television (CCTV)**

  The council has in place Closed Circuit Television (CCTV) systems covering the council's premises both internally and externally. CCTV systems are covered by the council's CCTV Policy.

- **Freedom of Information (Scotland) Act 2002**

  The Freedom of Information (Scotland) Act 2002 (FOISA) provides the public with a general right of access to information held by the council. The council produces and maintains a publication scheme and routinely publishes certain types (or classes) of information.

  In addition, the council follows the Scottish Ministers Code of Practice on Records Management issued under section 61 of the Freedom of Information (Scotland) Act 2002. The Code of Practice sets out recommended good practice in records management including responsibilities, policies, record keeping systems, storage, security and disposal.

- **Environmental Information (Scotland) Regulations 2004**

  Similar to FOISA, the public have a general right of access to environmental information that the council holds. The council also has a duty to make available environmental information and do so by routinely publishing information on our website. Environmental information includes:

- information on the state of the environment, such as air, water, soil, land and landscape;
- emissions and discharges, noise, energy, radiation, waste and other releases into the environment;
- measures and activities such as policies, plans and agreements affecting or likely to affect the above elements;
- reports on the implementation of environmental legislation, cost benefit and economic analyses used within the framework of the above measures and activities;
- the state of human health and safety, contamination of the food chain; cultural sites and built structures as they may be affected by environmental factors.

- **Public Records (Scotland) Act 2011**

  The Public Records (Scotland) Act 2011 (hereafter referred to as 'the Act') came fully into force in January 2013. The Act obliges public authorities to prepare and implement a Records Management Plan (RMP). West Lothian Council's Records Management Plan is based on the Model Records Management Plan published by the Keeper of the Records of Scotland (the Keeper). The council's plan, as agreed with the Keeper, sets out proper arrangements for the identification, management, preservation and disposal of council records including those handled by any contracted out service. It is assessed and reviewed on an annual basis.

  In addition, the council's Records Management Plan sets out arrangements for the management and preservation of records of local or general interest and those records that may be placed into custody of the council (referred to as the council's archives). The council has a Terms of Acquisition and an Archives Development Plan in place to ensure that these records are appropriately registered, preserved and remain accessible.

- **Re-use of Public Sector Information Regulations 2015 (RoPSI)**

  Public sector information is a valuable resource that can be useful to the private sector and to citizens. The purpose of the Re-use of Public Sector Information Regulations is to establish a framework for the effective re-use of public sector information.

  Access to a large proportion of public sector information is provided under Freedom of Information legislation. The RoPSI Regulations do not change the access provisions. Instead, they provide a framework for re-use of information once access has been obtained.

- **Regulation of Investigatory Powers (Scotland) Act 2000**

  RIPSA provides specified public authorities with a regulatory framework within which covert activity can be undertaken lawfully. It does this by requiring that public authorities set out fully the reasons for covert activity being necessary and demonstrate that such a course of action is proportionate to what it seeks to achieve. Using this framework requires the council to consider potential infringements on individual's rights. The council maintain a separate policy and procedure for authorising and managing covert surveillance operations under RIPSA.

- **Equality Act 2010**

  The public sector equality duty is a duty on public authorities to consider or think about how their policies or decisions affect people who are protected under the Equality Act. This policy and associated guidance adhere to the duties and requirements of the Equality Act 2010.

5.2. The council promote transparency and open access to information

The council has arrangements in place to ensure that it responds appropriately to requests for information and promotes greater openness of decision-making, including:

- **Managing Information Requests**

  The Freedom of Information (Scotland) Act 2002 (FOISA) together with the Environmental Information (Scotland) Regulations 2004 provide the public with a general right of access to information held by the council. The council has procedures in place to ensure that requests for information are handled with due care to legal obligations and the rights of individuals.

  When a valid request for information is made, the council provide a response within 20 working days. If the council holds the information requested then the council provide the requestor with the information or state which exemption has been applied. Information is only withheld when allowed (or required) to do so by specific exceptions granted to us by law.

- **Managing Individuals Rights**

  The Data Protection Act 2018 and UK GDPR gives individuals rights in relation to how organisations collect and process their personal data. The council maintains procedures which set out what individual's rights are and explains the process for enacting or utilising these rights.

  All requests are considered without undue delay and within one month of receipt. However, where requests are complicated, we may take longer to respond and will inform individuals of such. In most circumstances, the council do not charge for processing requests. However, where a fee is deemed appropriate, we will notify the individual and explain why.

  In some circumstances the council are unable to process the request, such as, in cases where it would be unlawful to do so. Where this is the case, we will explain why.

- **Maintaining a Publication Scheme**

  The Freedom of Information (Scotland) Act 2002 requires the council to produce and maintain a publication scheme. The council has adopted a Publication Scheme in line with the Scottish Information Commissioners Model Publication Scheme. The council's Publication Scheme guide provides a listing of documents routinely published or made available to the public. The Publication Scheme is regularly reviewed and updated.

- **Maintaining Privacy Notices and Managing Consent**

  The Data Protection Act 2018 requires the council to advise individuals about the processing of their data. The council provides this information in the form of 'Privacy Notices'. These are provided free of charge at the point information is

collected and by the same means, for example, if the information is gathered in printed form, the privacy notice is available in printed form. The details provided to individuals include:

- the data that is being processed about them (including the legal basis for this processing);
- who the council is sharing data with (both within and outside the organisation);
- how long we will keep it for;
- their rights in relation to the data and how they can request information from the council.

In some circumstances, we ask individuals for their consent to collect and process personal data. Where consent is required, the council:

- Ensure individuals are informed by being clear and concise about how we, and any third parties, will use personal data;
- Ensure that individuals have real choice and control;
- Will not use personal data for any purpose other than that for which consent was given, respecting individuals wishes about the use of their data;
- Make it easy for individuals to withdraw consent and inform them how to do so;
- Keep records of consent and ensure that consent is reviewed and updated;
- Avoid making consent a precondition of a service provision;
- Keep our requests for consent separate from other terms and conditions;
- Will be specific and 'granular' so that we get separate consent for separate things;
- Ensure that individuals provide a very clear and specific statement of consent.

The council apply particular protections to the collecting and processing of children's personal data because they may be less aware of the risks involved. Where we offer an online service, which is not a preventive or a counselling service, directly to a child, only children aged 13 or over are able to provide their own consent. For children under this age we may obtain consent from whoever holds parental responsibility for the child.

- **Providing Data in an Open Format**

  The council publish data freely and it is widely available via our web site. The council has adopted the UK government's approach to Open Standards. Council data is published in a format that meets, as a minimum, a rating of 3 stars from the Government's 5-star rating scheme. This means that council data is easily accessible and available to re-use as required under the Open Government Licence.

- **Access to Archives**

  The council also facilitate access to information through its Museums and Archives Service. The Museums and Archives Service preserves, and makes accessible, records relating to the history of West Lothian. The council provide facilities and finding aids to help people locate records held within the Archives, such as, a searchable online catalogue. Subject to conditions, all archive deposits held by the council are made widely available for public consultation.

5.3. The council ensure the security and confidentiality of information

The council is committed to preserving the confidentiality, integrity and availability of all physical and electronic information assets. The potential impact of damage or loss of council information includes disruption to services, risk to citizens, damage to reputation, legal action, personal distress, loss of confidence and may take considerable time and cost to recover. The council apply controls to prevent or minimise the impact of such events and reduce information related risks. These arrangements include:

- **Managing Information Security**

  Information security management within the council is concerned with protecting against unauthorised access to information, modification of information or loss of information by preserving:
  - **Availability** – protecting against loss or damage, ensuring maximum uptime and reducing service outages;
  - **Confidentiality** – ensuring confidential information is appropriately protected and that council arrangements are commensurate with legislation, regulations, standards and best practice;
  - **Integrity** – ensuring accuracy and completeness of information.

- **Maintaining Business Continuity Arrangements**

  The council has in place business continuity and contingency plans, including backup and recovery procedures, to ensure cyber resilience. The council's business continuity plans identify vital council information systems. In addition, a disaster recovery plan for the Council's archives is maintained.

- **Managing Breaches**

  A Data Protection Breach can occur through the theft or accidental loss of personal data, through the unauthorised use or accidental disclosure of personal data, or deliberate attacks on Council systems.

  The council has a number of arrangements in place to prevent information breaches. However, if this does happen, the council has in place a breach reporting procedure. Breaches are reported to the Investigating Officer, Heads of Service, IT Services, the DPO and Chief Solicitor. Where a breach is considered by the DPO likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours. Any staff who have identified a potential breach are required to report it to the IT Service Desk and their line manager without delay.

5.4. The council identify and mitigate information risks

The council has a number of controls in place to assess and mitigate information risks. These include:

- **Conducting and Maintaining Data Protection Impact Assessments**

  The council complete DPIAs when new technology is being introduced or where there are changes to the processing of personal data. The assessment identifies and assesses potential risks to the rights and freedoms of individuals and what steps can be taken to reduce risk whilst providing services. Where possible, the council consult users and will publish DPIAs on our website. The council treat DPIAs as living documents to be revised and updated whenever necessary.

- **Maintaining Information Registers**

  The council maintain an Information Asset Register that details the assets used to store and manage council information. Risk assessments are conducted on each asset.

  In addition, the council has established Records of Processing Activities (called a ROPA) which include information about processing of personal data, types of personal data, details about the data subjects, the purpose of the processing and any recipients of the data. The council has an Information Asset Register, Information Processing/Sharing Agreements, Privacy Notices and other contractual documentation.

5.5. The council train staff in good practice information governance

All staff are trained in good practice information governance, including, Information Security, Records Management, Freedom of Information and Data Protection. Staff who undertake specific roles relating to information governance are provided with additional training, such as, the Data Protection Officer, Records Manager, Information Security, Audit Risk and Counter Fraud Manager, Information Liaison Officers. Service Managers ensure an auditable record is maintained of all training.

5.6. The council regularly monitor and review performance

- **Regularly Assessing Record Keeping Arrangements**

  The council annually assess and review the Records Management Plan and record keeping arrangements. Evidence of improvements are submitted to the Keeper at the National Records of Scotland.

- **Monitoring Performance**

  The Governance and Risk Board operate with a forward plan and ensure effective arrangements are in place to improve information governance compliance. The board also monitor information governance and related risks. Reports are submitted by the Information Management Working Group, who have the remit for implementing information governance compliance arrangements.

- **Code of Corporate Governance Reporting**

  The Senior Information Risk Owner, the Data Protection Officer and the Head of Corporate Services will produce annual statements of compliance in accordance with the council's Local Code of Corporate Governance and related reporting procedures.

6. RETENTION AND ERASURE OF PERSONAL DATA

The council does not keep information for any longer than it is needed, and dispose of both paper and electronic records in a secure manner. The length of time the council need to keep information depends on the purpose for which it is collected. The Council has a record retention schedule which sets out how long we keep records and the reason why.

7. MONITORING AND REPORTING

Governance over this policy is built in to normal council processes e.g. line management, service management and project management. Formal governance over this policy is set out in the following table.

Group	Role	Frequency
Corporate Management Team	Scrutinise and review compliance and progress.	Quarterly
Information Management Working Group	Developing and implementing policies and procedures relating to the strategy and monitoring/ reporting progress across service areas.	Monthly
Governance and Risk Board	Reviewing and implementing policies, procedures and standards. Evaluating and monitoring projects in line with this policy.	Quarterly
Corporate Policy and Resources Policy Development and Scrutiny Panel	Scrutinise and review the policy and progress.	Annual
Council Executive	Approve policy and progress.	On significant update

8. REVIEW

This procedure will be reviewed as appropriate at least once every 5 years. The Head of Corporate Services may make minor and administrative changes when required, for example, to reflect internal council management structure changes, or new legislation or guidance.

9. APPENDIX 1: DEFINITIONS

Contracted Out Service – Certain functions of the council may be conducted under contract by a third party organisation.

Criminal Offence Data - Article 10 UK GDPR covers processing in relation to criminal convictions and offences or related security measures. This includes personal data relating to the alleged commission of offences, or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

Closed Circuit Television (CCTV) - also known as video surveillance, is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors.

Data Controller – The Data Controller is a legal person or organisation, which, alone or jointly with others, determines the purpose and manner by which personal data is processed. West Lothian Council and Elected Members are data controllers.

Data Processor – A Data Processor is a person or organisation, who process personal data on behalf of the Data Controller.

Data Protection Impact Assessment (DPIA) – This is a process that helps to identify and minimise data protection risks. More information on DPIAs can be found on the ICO Web Site.

Data Protection Law – Data Protection Law includes the General Data Protection Regulation 2016/679; the UK Data Protection Act 2018, UK GDPR and all relevant EU and UK Data Protection legislation.

Data Sharing Agreement - A data-sharing agreement is a formal contract that details the data being shared, how the data can be used, how it should be protected, how long it should be retained etc.

Data Subject – A Data Subject is any living individual to which personal data refers. Data Subjects must be identifiable, either directly from the data itself or indirectly by combining it with other data. Identifiable data can include, for example, name, identification number, location information, online identifier, or one or more factors specific to physical, physiological, genetic, mental, economic, cultural or social identity of individuals.

Format – Information can be in any form including (but not limited to): paper files, email, audio/visual, electronic documents, systems data, databases, digital images and photographs.

Information Asset Register (IAR) – This is a system that helps the council to understand and manage its information assets and risks to them. It provides detail on what information the council holds, and where it holds it, in order to protect it.

Information Governance – Information Governance is the process by which the council obtains and, provides assurance that, it is complying with its legal, policy and moral responsibilities in relation to the processing of information.

Memorandum of Understanding (MOU) – This is an agreement between two or more parties detailing, terms and conditions, responsibilities, and expectations etc.

Personal Data – Personal data means any information relating to a living individual who can be identified from that information or from other information for example, name, address, identification number, location data etc. Where this policy identified Personal Data, this should be read as including special category data and criminal offence data.

Processing Personal Data – Almost everything that can be done with personal data including obtaining, destroying, storing and using personal data amounts to processing personal data.

Record – A record is defined as information/data in any form, including those in systems, created or received in order to support and/or give evidence of an activity.

Record Keeping Systems – A system or procedure, by which records are created, captured, secured, maintained, reused, preserved and/or disposed of.

Records Management – The control of the records throughout their lifecycle, from creation to storage and retention until eventual archival or destruction.

Records of Processing Activities (ROPA) – This is how we document our processing activities.

Special Category Data – Some data has particular sensitivities, called Special Category Data. This includes data relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics or biometrics (such as finger prints), health, sex life or sexual orientation.

Staff – All council employees and workers, such as, contractors, consultants, volunteers and agency staff that have authorised access to council information/systems or process council information.

Third Party – Any external organisation that processes data on behalf of the council either in partnership or under contract or agreement.

10. APPENDIX 2: STANDARDS

This policy and the associated guidance have been developed within the context of national legislation, professional standards and codes of practice. As far as is practical, this policy will address the principles defined within:

Legislation:

- The Data Protection Act 2018;
- Freedom of Information (Scotland) Act 2002;
- Environmental Information (Scotland) Regulations 2004;
- Public Records (Scotland) Act 2011;
- Local Government etc. (Scotland) Act 1994;
- INSPIRE (Scotland) Regulations 2009;
- Re-use of Public Sector information Regulations 2015.

Standards:

- BS ISO/IEC 27001:2017 – Information technology. Security techniques. Information Security management systems.
- BS ISO/IEC 27032:2012 – Information technology. Security techniques. Guidelines for cybersecurity.
- BS ISO 15489 – Information and documentation. Records management.
- BS 10008:2014 – Evidential weight and legal admissibility of electronic information.
- *Code of Practice on Records Management* issued under section 61 of the Freedom of Information (Scotland) Act 2002.
- Archives Service Accreditation Standard of the UK National Archives.
- International Standards for Archival Description (ISAD(G)) and Archive Authority Files (ISAAR (CPF)).
- ISO 14721:2012 – Open Archival Information System (OAIS).
- BS 4971:2017 Conservation and care of archive and library collections.