WEST LOTHIAN COUNCIL

SPECIAL CATEGORY DATA POLICY

Data Label: Public

SPECIAL CATEGORY DATA POLICY
CONTENTS

1. INTRODUCTION

This policy has been developed by West Lothian Council ('the council') to meet the requirement in the Data Protection Act 2018 (DPA) for an appropriate policy document. The Policy details the lawful basis and conditions for processing along with safeguards the council has put in place when processing special category data, criminal offence data and sensitive processing for law enforcement purposes.

2. SCOPE

This policy covers:

- processing of special categories of personal data;
- processing for employment, social security, and social protection purposes;
- substantial public interest condition processing;
- processing for archiving, research, and statistical purposes;
- criminal offence data and
- sensitive processing for law enforcement purposes.

3. ACCOUNTABILITY

3.1. 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.

3.2. Heads of Service

Heads of Service are 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;
- Ensuring that CCTV installations adhere to this policy and associated procedures;
- Ensuring that the processing of special category data adheres to this policy and associated procedures;
- Resourcing the Information Liaison Officer role.

3.3. Data Protection Officer (DPO)

The council has appointed the Head of Corporate Services 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.

3.4. Governance and Risk 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 three Working Groups covering Governance, Risk Management and Information Management.

4. RESPONSIBILITIES

4.1. 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.

4.2. 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 and Risk Assessments associated with information systems and processes;
- Completing annual compliance reviews.

4.3. Performance and Improvement 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;
- Supporting the development of the council's information asset register and file plans;
- Providing advice and guidance on the completion of Data Protection Impact Assessments (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.

4.4. IT Service

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;
- Designing applying and managing a baseline security build and configuration for all approved hardware and devices;
- Security patch management;
- 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 Plus.

4.5. 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/sensitive data.

4.6. 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 councils Records Retention Schedules;
- Monitoring and reviewing the effectiveness of the Information Governance Policy and procedures.

4.7. 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:

- Identifying 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.

4.8. 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:

- Ensuring that they understand 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.

4.9. 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. Lawful basis for processing

The council is a government body with functions in accordance with statutory duties and powers. The council processes personal data under the following lawful bases provided in Article 6 of the General Data Protection Regulation (UK GDPR):

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

(g) processing is necessary for reasons of substantial public interest;

(h) processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of health care or treatment or the management of health or social care systems and services;

(i) processing is necessary for reasons of substantial public interest in the area of public health;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of UK GDPR.

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'. The details available 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.

The council's Information Governance Policy sets out the council's legal obligations in respect of processing personal data and this is available on the council's website.

5.2. Definition of special category and criminal offence data

Article 9(1) of the UK GDPR defines special category data as personal data which reveals:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health;
- Data concerning a natural person's sex life or sexual orientation.

Article 10 of the UK GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that 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'.

5.3. Conditions for processing special category and criminal offence data

The council processes special category data under the following paragraphs of Article 9(2) of the UK GDPR:

1. Article 9 2(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes.

    - Examples of our processing include staff dietary requirements and health in-formation we receive from our customers who require a reasonable adjustment to access our services.

2. Article 9 2(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Council or the data subject in the field of employment, social security, and social protection.

    - Examples of processing by the council based on this condition include the provision of social care services, revenue and benefits, housing functions and processing for HR purposes.

3. Article 9 2(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent.

    - An example of our processing would be using health information about a member of staff in a medical emergency.

4. Article 9 2(e) processing relates to personal data which are manifestly made public by the data subject.

5. Article 9 2(f) processing is necessary for the establishment, exercise, or defence of legal claims.

    - Examples of our processing include processing relating to any employment tribunal or other litigation.

6. Article 9 2(g) processing is necessary for reasons of substantial public interest.

    - Examples of our processing include the information the council seek or receive as part of a fraud investigation

7. Article 9 2(h) processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of health care or treatment or the management of health or social care systems and services.

    - Examples of our processing include, for the assessment of an employee's working capacity, the provision of social care services (including social work, personal care and social support services), the management of social care systems.

8. Article 9 2(i) processing is necessary for reasons of substantial public interest in the area of public health.

    - An example of processing by the council is the response to an epidemic or pandemic.

9. Article 9 2(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of UK GDPR.

    - An example would be archiving material from a conference by a council service

    Or

    - Conducting and longitudinal study which required regular data from client's health records to be fed in, where the data could not be fully anonymised.

To process criminal offence data the council must have both a lawful basis under Article 6 (see above) and either legal authority or official authority for the processing under Article 10 of the UK GDPR.

5.4. Description of data

The council processes special category data about its staff that is necessary to fulfil its obligations as an employer. This may include information about occupational health, wellbeing, ethnicity, photographs, and membership of trade unions. This may also include criminal offence data in relation to pre-employment checks.

Special category and criminal offence data are processed by the council relating to its customers and service users where there is a legal basis to do so. This may include information such as ethnicity, health, and criminal convictions. For example, in relation to housing needs, grants and revenue and benefits.

Sensitive law enforcement data is processed by the council in relation to criminal investigations and prosecutions where there is a legal basis to do so. This includes for example enforcement of housing standards, food health and safety, fly-tipping, licensing, and public protection anti-social behaviour.

5.5. Accountability principle

The council carries out Data Protection Impact Assessments (DPIA's) where appropriate in accordance with Articles 35 and 36 of the UK GDPR and section 64 of the DPA for law enforcement processing. This is to ensure data protection compliance by design and default.

The council Information Governance Policy is available to all staff and annual Data Protection training is carried out to all staff. The council maintains documentation relating to its processing activities in accordance with Article 30 of the UK GDPR in an Information Asset Register (IAR) which is reviewed and updated by the council's Information Liaison Officers in each service area. In relation to law enforcement processing the council follows the data protection principles set out in Article 5 of the UK GDPR, and Part 3, Chapter 2 of the DPA as detailed below:

5.5.1. Principle (a): lawfulness, fairness and transparency

The council provides clear, transparent information to those whose personal data it processes including information regarding their data rights.

The council provide service specific privacy notices on its website.

The council process data under a number of legal bases as set out above but will generally process personal data which is necessary for the performance of its public tasks with a basis in law in accordance with its statutory duties and powers (Article 6.1(e) of the UK GDPR).

Processing for any law enforcement processing will be necessary for the exercise of a function conferred upon the council for example enforcing housing standards and will be necessary for reasons of substantial public interest.

In the rare circumstances where the council seek consent as the only legal basis for processing it will make sure the consent is:

- unambiguous;
- freely given;
- given by an affirmative action;
- the data subject shall have a right to withdraw consent and anytime;
- consent is recorded as the condition for processing.

5.5.2. Principle (b): purpose limitation

The council does not process personal data for purposes that are incompatible with the purposes for which it is collected.

Purposes are set out in privacy notices where required.

When the council shares special category data or criminal offence data or law enforcement data with another controller or processor or partner the council ensures that the data transfers are compliant with relevant laws and regulations and uses appropriate data sharing agreements and contracts.

If the council plan to use personal data for a new purpose (other than a legal obligation or function set out in law) it checks that this is compatible with the original purpose or obtains specific consent and undertakes a Data Protection Impact Assessment where required. Data collected for law enforcement purpose will only be used for purposes other than law enforcement, where the council are authorised by law to process the data for the purpose.

5.5.3. Principle (c): data minimisation

The council collects personal data that is adequate, relevant, and limited to the relevant purposes for which it is processed. The council ensures that the information it processes is necessary and proportionate to its purpose. The council periodically reviews this and deletes any unnecessary data

5.5.4. Principle (d): accuracy

Personal data shall be accurate and, where necessary, kept up to date. If the council becomes aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, the council will take every reasonable step to ensure that data is erased or rectified without delay.

The council detail in its main privacy notice on the council's website how individuals exercise their right of erasure and rectification.

If the council decide not to either erase or rectify, the council will document their reason for the decision.

In relation to data collected for law enforcement purposes to the council, where relevant, and as far as possible, distinguish between personal data relating to different categories of data subject, such as:

- people suspected of committing an offence or being about to commit and offence;
- people convicted of a criminal offence;
- known or suspected victims of a criminal offence;

- witnesses or other people with information about offences.

The council only do this where the personal data is relevant to the purpose being pursued.

The council take reasonable steps to ensure that personal data, which is inaccurate, incomplete or out of date is not transmitted or made available for any of the law enforcement purposes.

5.5.5. Principle (e): storage limitation

The council retains special category data, criminal offence data and sensitive data for law enforcement processing in accordance with the council's retention and disposal schedules. These schedules are available on the council's website. Information Liaison Officers (ILO's) engage with their service manager to ensure that the data in the service area is deleted or disposed off in accordance with the retention and disposal schedules.

The council has a record retention schedule which sets out how long we keep records and the reason why.

5.5.6. Principle (f): integrity and confidentiality (security)

The council has put in place appropriate technical and organisational measures to safeguard and secure the information the council collects about individuals. The council has strict security standards, and all our staff who process personal data on the council's behalf receive training on induction and annual training about how to keep information safe. The council limits access to personal data to those employees, or third parties who have a business or legal need to access it.

Third parties or contractors that the council engages will only process personal data on the council's instructions or agreement, and where they do so they have agreed to handle the information confidentially and to keep it secure.

6. RETENTION AND ERASURE OF PERSONAL DATA

The council do 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.

There are a range of detailed guides on the council's intranet sit covering how to create, manage and dispose of records within council systems. Most records originate in electronic format.

The council has in place retention schedules segmented by service. These detail the record types created by the council and how long they should be kept for. The retention schedules are designed on the basis of the functions of the council and the activities carried out by each function. The retention schedules are published on the council's intranet site.

7. REVIEW

This policy 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.

8. APPENDIX 1: RELATED POLICIES

This policy supports the following council policies:

- Information Governance Policy;
- CCTV Policy.