West Lothian Council

WEST LOTHIAN COUNCIL
DATA PROTECTION ACT 1998
POLICY

Version 3.0

DATA PROTECTION ACT 1998 POLICY

CONTENTS

DATA PROTECTION ACT 1998 POLICY

1. INTRODUCTION

In order to operate efficiently, West Lothian Council has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information in order to fulfil its statutory requirements.

This personal information must be handled and dealt with appropriately, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means there are safeguards within the Act to ensure this.

The council regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the council and those with whom it carries out business. The council will ensure that it treats personal information lawfully and correctly.

To this end the council fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998.

The Data Protection Act 1998 regulates the processing of information relating to living persons in the UK. It requires that data controllers be registered with the UK Information Commissioner and comply with the **eight principles** which are legally enforceable. The Principles require personal data files to be up-to-date and accurate and that procedures are established which enable the Council (the **data user**), to answer fully enquiries from persons (**data subjects**), about the manual or computerised data which the Council holds about them.

This document contains technical terms which must be used such as **data user** and **data subject** already referred to above. To assist, a number of the most commonly used terms are defined in Appendix 1.

The provisions of the Act are set out in Section 2 and are then used as a framework for the General Policy statement in Section 3. Section 4 deals with non-compliance with the Act. Section 5 summarises the role of the elected members. Sections 6, 7 and 8 complete the document by outlining arrangements for providing control, advice, training and up-dating.

2. PROVISIONS OF THE ACT

The Act provides for an independent Information Commissioner who maintains a public register containing sufficient information for an individual to be aware of who holds **personal data** of which he/she could be subject.

The following obligations are imposed on the Council by the Act;

(a) to make the requisite entries in the Public Register describing all the **personal data** held by the council; and

(b) to use the described **data** only for the registered purposes; and

(c) not to disclose the **data** to persons other than those described in the Register; and

(d) to maintain the accuracy of the **data**; and

(e) to maintain adequate **data** relevant to the purpose; and

(f) not to keep **data** for too long; and

(g) to supply copies of all **data** referring to an individual at the request of that individual except where access to the **data** is exempted by the Act; and

(h) to take appropriate security measures to guard against the loss, accidental destruction or unauthorised **disclosure** of the **data**; and

(i) ensure that personal data is not transferred to a country outwith the European Economic Area, unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3. SCOPE

This policy covers all personal information in all areas of councils business. The policy covers all methods of acquiring, creating, accessing, processing, storing, transferring, archiving and disposing of council information. This includes:

- Manually stored data such as paper records, folders, files etc.
- Data held in computer applications and databases
- Data held and processed on council owned and operated websites (including cookies)
- Data from CCTV and other audio or visual recording systems
- Data held in records archive storage
- Data stored on any media such as tapes, CD/DVD, computer disk drives and memory cards, USB drives etc.

3.1 The council observes its duty of confidentiality towards citizens, customers, suppliers, partners and staff. Council employees, contractors, consultants, agency staff, contracted 3rd parties and volunteers, have a responsibility to ensure compliance with the Act and this policy when handling council information. Managers and staff have a responsibility to develop and encourage good working practices within their areas of responsibility. All users of council owned personal information have a responsibility to ensure that they process the data in accordance with the 'eight principles' of the Act and the other conditions set down in the Data Protection Act.

3.2. **Information Sharing** - In line with this policy, where personal and/or sensitive information is being shared systematically between organisations working together in a partnership or contracting arrangement, the involved services will ensure that a Data Processing Agreement, Data Sharing Agreement and/or Third Party Access Agreement(s) are in place. All contracts for the supply of services will include a standard clause relating to Data Protection and any additional requirements for the continued compliance with the Act.

Copies of all Contracts and Agreements are maintained in the council's Electronic Documents and Records Management system.

3.3. The council will inform **data subjects** of its commitment to Data Protection through the publication of its **Information Charter (Appendix 2)**

4. GENERAL POLICY STATEMENT

4.1 West Lothian Council is registered as the **Data Controller** with the Office of the Information Commissioner.

4.2 Under the Council Scheme of Delegation the Head of Corporate Services is the Council's Data Protection Officer.

4.3 West Lothian Council promotes compliance with the Data Protection Act 1998 and seeks observance of its principles by maintaining the confidentiality of all **personal data** held on **computers** and in relevant **manual filing systems**.

4.4 This policy applies to all employees and elected members of the Council.

4.5 The Chief Executive has overall responsibility for the administration and implementation of the Council's policy for Data Protection. The Chief Executive is the Senior Information Risk Officer for the council. Each Depute Chief Executive will retain executive authority for the compliance of employees within their areas of responsibility.

4.6 **Personal data** held on **computer or in relevant manual files** will be as accurate as possible in respect of matters of fact. Opinions will be carefully and professionally expressed.

4.7 The council will ensure that processes are in place to update data with amendments requested by **Data Subjects**.

4.8 The council will ensure that procedures are in place to assist requests for access to **data** from **data subjects, clearly indicating where** a fee may be applied,

4.9 The authorisations of the Depute Chief Executive, or his/her nominated representative, is necessary where the employees use their privately owned **computers** to process data belonging to the Council subject to the provisions of 4.11 below.

4.10 **Computers, files and data** will be maintained in an appropriately controlled environment and the requirements are set down in the Council's Information Security Policy and Information Handling Procedure.

4.11 The council will ensure that Data Protection Principles are applied to all systems handling personal information. All changes, upgrades and new implementations will be risk assessed to ensure the continued protection of personal information.

4.12 When employees use the Council's **computers** for any purpose, such users are subject to the Council's Information Security Policy, Information Handling Procedure and Employees Code of Conduct.

4.13 **Personal data** must not be disclosed to persons other than those referenced in the Data Protection Register entry for the Council or otherwise where the data subject has explicitly consented to the data being disclosed (or the disclosure is permitted by statute).

4.14 The council will inform users of any personal information collected via websites using **cookies**. A cookie notice will inform users on what cookies are used, what information is collected and why. Users will be informed on how to switch off non-essential cookies and the impact of doing so.

4.15 **Sensitive Personal data** must not be disclosed to persons other than those referenced in the Data Protection Register entry for the Council and only where the data subject has explicitly consented to the data being disclosed (unless the disclosure is permitted by statute.

4.16 Contracts and agreements for agency, bureau, voluntary, unpaid and contract staff will contain a clause to cover their employees' obligation to observe the Council's Data Protection policy.

4.17 The Council will ensure that **data** held by it for a registered purpose are adequate, relevant, not excessive and not held for longer than necessary.

4.18 All breaches or potential breaches of this policy are handled in accordance with the incident handling policy. All incidents are recorded, risk assessed and corrective measures put in place to ensure the continued protection of personal data. The Chief Solicitor is the council's contact with the Information Commissioner's Office.

4.19 Any employee deliberately breaching the Council's Data Protection Policy will be subject to the established disciplinary procedures.

5. NON-COMPLIANCE WITH THE ACT

To protect the Council, elected members and the employees of the Council from inadvertent breaching of the Act, general guidelines will be issued by the Head of Corporate Services. Operational procedures for service areas will be put in place by Heads of Service to supplement the guidelines published.

6. ROLE OF ELECTED MEMBERS

This Act affects elected members in three different capacities:

(a) as a member of a committee or the Council; and, therefore subject to the same rights, responsibilities and penalties as employees of the Council;

(b) acting on behalf of a member of the public; and

(c) personally when the rights of data subjects apply.

The Data Protection Act and this Policy statement do not change any duties, rights or responsibilities imposed by any other enactment.

With regard to (a) and (c), the rules which apply to employees also apply to elected members of the council.

Members of the Council will only seek access to data when knowledge of such data is essential for them to undertake their Council responsibilities or where the data subject has authorised the access ((b) above).

7. GOVERNANCE

Governance over Data Protection 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 table below.

Data Protection Policy Governance Structure		
Group	**Governance/Scrutiny Role**	**Reporting Frequency**
Information Management Working Group	Developing and implementing policies and procedures relating to the strategy and monitoring/reporting progress across service areas	6 weeks
ICT Programme Board	Reviewing and implementing policies, procedures and standards. Evaluating and monitoring projects in line with this policy	Quarterly
Partnership and Resources Policy Development and Scrutiny Panel	Scrutinise and review the policy and progress	Annual
Council Executive	Approve policy and progress	Annual

8. ADVICE AND TRAINING

The council will provide training and guidelines for employees to comply with this policy. This includes additional measures for highly sensitive or confidential information

9. ISSUE AND REVIEW

Each Head of Service shall ensure that a copy of this Policy will be brought to the attention of the employees within their Service.

It will be reviewed periodically and will be revised to comply with any alteration to the legislation. This will be carried out by the Information Management Working Group and reported to Corporate Management Team and elected members as required.

Previous Review Date: **April 2017**
Next Review Date: **April 2018**

APPENDIX 1 - Definitions

Computer

Any equipment which can process data automatically; and therefore includes PCs, servers, any equipment with micro-processor chips which can execute instructions automatically.

Data

Recorded information including information held in a form which can be processed by computer.

Personal Data

*"*personal data*"* means data which relate to a living individual who can be identified—
(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

Sensitive Personal Data

The Act defines categories of sensitive personal data, namely, personal data consisting of information as to:-

(a) the racial or ethnic origins of the data subject;
(b) his political opinions
(c) his religious beliefs or other beliefs of a similar nature
(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992;
(e) his physical or mental health or condition;
(f) his sexual life;
(g) the commission or alleged commission by him of any offence; and
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Data Controller

"…. A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed".

"…. It shall be the duty of a data controller to comply with the Data Protection Principles in relation to all personal data with respect to which he/she is the data controller."

A data controller must be a “person” i.e. a legal person. This term comprises not only individuals but also organisations such as companies and other corporate and unincorporated bodies of persons.

Data subject

An individual who is the subject of **personal data**.

Data User

A legal entity, e.g. West Lothian Council, who controls the use and contents of one or more collections of **personal data**. Normally the employees of the Council will not be regarded as **data users** themselves since they are acting on behalf of the Council, but if an officer owns **data** for his/her own private use, i.e. **data** which has no relation to his/her work for the Council, then he/she is a **data user**.

Disclosing

Giving a copy of some or all of the **personal data** relating to an individual to another individual or organisation. The means by which the information is given e.g. paper copy, magnetic media or over a network etc. is not important.

Registered

The reason for which the Council processes **data** and **purpose** which has been accepted by the Information Commissioner as lawful.

Information Sharing

‘Information sharing’ is the sharing of sensitive and/or personal information in a closed way between or within organisations as part of integrated working or service delivery. The Council encourages lawful information sharing undertaken in line with best practice, both within the Council and with relevant third parties.

SIRO

Senior Information Risk Officer (SIRO)

West Lothian Council

West Lothian Council - Information Charter

We need to handle personal information about you so that we can provide services for you. This is how we look after that information:

When we ask you for personal information, we undertake:

- to make sure you know why we need it;
- to only ask for what we need, and not to collect too much or irrelevant information;
- to protect it and make sure nobody has access to it who shouldn't;
- to let you know if we share it with other organisations to give you better public services, and if you can say no;
- to make sure we don't keep it longer than necessary; and
- not to make your personal information available for commercial use without your permission.

In return, we ask you to:

- give us accurate information; and
- tell us as soon as possible if there are any changes, such as a new address.

This helps us to keep your information reliable and up to date.

You can get more details on:

- how to find out what information we hold about you and how to ask us to correct any mistakes;
- agreements we have with other organisations for sharing information;
- circumstances where we can pass on your personal information without telling you, for example, to prevent and detect crime or to produce anonymised statistics;
- our instructions to staff on how to collect, use and delete your personal information;
- how we check the information we hold is accurate and up to date; and
- how to make a complaint.

For more information, please contact:
The Contact Centre
West Lothian Civic Centre
Howden South Road
Livingston
Telephone : 01506 280000
Email: ContactCentre@westlothian.gov.uk

When we ask you for information, we will keep to the law. If you consider that your information has been handled incorrectly you can contact the Information Commissioner for independent advice about Data Protection, privacy and data sharing issues. You can contact the Information Commissioner at: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Telephone: 08456 30 60 60 or 01625 54 57 45 Fax: 01625 524510 Website: www.ico.gov.uk