**CONTENTS**

1. **Introduction**
2. **Policy Statement**
3. **Scope**
4. **Data Protection Principles**
5. **Process / Procedure / Guidelines**
6. **Data Sharing**
7. **Responsibilities**
8. **Policy Compliance**
9. **Training**
10. **References**
11. **Introduction**

Fife Council provides a wide range of services, not only for people who live or work in Fife, but also for investors in Fife and for visitors who come here for pleasure or business. The Council also works in partnership with a wide range of public sector, commercial and voluntary sector organisations to provide services and support.

To deliver services effectively the Council needs to collect, process and hold, large volumes of personal information relating to current, past and prospective employees, suppliers, clients and customers. In addition, it may occasionally be required by law to process personal information to comply with the requirements of governmental departments and other agencies.

1. **Policy Statement**

Fife Council will seek to avoid personal data breaches by having a positive and proactive approach to data collection and management; ensuring we protect the information we collect; ensuring it is used and shared appropriately; actively managing it to ensure it is relevant and up-to-date; is fully compliant with legislation and best practice guidance from the ICO.

The Council recognises a personal data breach if not addressed in an appropriate and timely manner, can result in physical, material or non-material damage to individuals such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the individual concerned. Where personal data breaches do occur the Council will, without undue delay, seek to contain the harm to individuals, investigate the breach, report the breach to the Information Commissioner’s Office, where appropriate, and look to learn the lessons from any actual or suspected breaches.

1. **Scope**

This policy is applicable to all personal data held by Fife Council whether the information is held or accessed on Council premises or accessed remotely via mobile or home working or by using network access from partner organisations. Personal information held on removable devices and other portable media is also covered by this policy.

Personal data is anything which is capable of identifying a living individual, e.g. name, address, identification number, CCTV image, telephone call recording, e-mail address, location data, postcode, photograph etc. Special category data is information about racial and ethnic origin, political opinions, religious beliefs, physical and mental health, biometric data, sexual life, trade union membership and proceedings.

It applies to all employees, elected members, third party suppliers and any other individuals with access to the Council’s information and information systems. This policy also applies to Assessors and Fife Licencing Board, who are separate data controllers in their own right, but associated to Fife Council for the purposes of data protection. For Fife Council employees, compliance with the policy and associated procedures are a condition of employment. Violations of the policy may result in disciplinary action against an employee.

1. **Data Protection Principles**

The General Data Protection Regulations, together with the Data Protection Act 2018, (known as the Data Protection Legislation) requires organisations which handle personal data to collect, process and hold personal and confidential information securely and responsibly. This includes maintaining a data processing register of all information held and destroying the information safely when it is no longer required.

The Data Protection Legislation sets out six key principles:

* processed lawfully, fairly and in a transparent manner in relation to individuals;
* collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
* adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
* accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
* kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
* processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
1. **Process / Procedure / Guidelines**

To ensure compliance with the above data protection principles Fife Council will:

* Observe,the fair collection and use of personal data.
* Meet its legal obligations to specify the purposes for which data is used.
* Collect and process appropriate data, and only to the extent that it is required to fulfil operational needs or to comply with any legal requirements.
* Ensure the quality of the data used.
* Apply strict checks to determine the length of time the data is held.
* Take appropriate technical and organisational security measures to safeguard personal data.
* Ensure that personal data is not transferred outside the European Economic Area without suitable safeguards.
* Ensure that everyone managing and handling personal data is appropriately trained and supervised; and is fully aware of their data protection responsibilities.
* Regularly review and audit internal data handling processes and procedures.
* Ensure that rights of people about whom data is held can be fully exercised under the Data Protection Legislation . These include:
	+ The right to be informed that processing is being undertaken.
	+ The right to prevent processing in certain circumstances.
	+ The right to correct, rectify, block or erase data which is regarded as incorrect.
	+ The right of access to one’s personal data.
	+ The right to withdraw consent.

 Subject Access Requests

The Data Protection Legislation also allows people to find out what personal information is held by organisations about them by making a Subject Access Request (SAR). A SAR can include both electronic information and paper records. The organisation must provide the information to the individual, or their nominated representative within one month (there are some exceptions to this).

Individuals who wish to make a SAR to Fife Council will need to provide evidence of their identity. There is no charge for a SAR made by a data subject to Fife Council.

The Information Management and Requests Team are responsible for processing and managing Subject Access Requests on behalf of Fife Council. Employees must not process these requests, but should notify the Information Management and Requests Team upon receipt. The Information Management and Requests Team can be contacted at information.requests@fife.gov.uk

**6. Data Sharing**

 For the planned, regular sharing of personal information between Fife Council and other partners or agencies, appropriate information sharing agreement’s, protocols and supporting guidance materials must be agreed and in place. Information sharing agreements and other governance elements will be reviewed, amended and updated on a regular basis, and in accordance with operational requirements.

**7. Responsibilites**

 Fife Council has specific responsibility for agreeing, advising on and monitoring data protection practice within the organisation.

 The Executive Director, Finance and Corporate Services, has specific responsibility for data protection within Fife Council.

 Each Executive Director has responsibility for ensuring that the information under their control is collected, processed and held in accordance with this policy and the requirements of the Data Protection Legislation

 All employees, elected members, and any other individuals with access to the Council’s information must be familiar with the requirements of the Data Protection Legislation and have a responsibility to ensure that personal information is properly protected at all times. This requires continued compliance with the Council’s information policies, procedures and other guidance.

 Employees will only have access to personal information where that access is necessary to enable them to undertake work duties. Employees should discuss with their line manager any instance where access rights require clarification. Access rights must not to be regarded as permanent and are subject to change at any time dependent upon the nature of the duties being fulfilled by an employee.

 Employees should only record information about an individual which is relevant to the purpose or purposes that the information is being collected for, and should be aware that they may be required to justify what has been recorded and be aware that all recorded personal information may be released as part of a Subject Access Request.

 Any employee who is found to have inappropriately divulged personal information will be subject to investigation under the Council’s disciplinary procedure, which may result in dismissal and possible legal action.

 All users have a responsibility to report any observed or suspected breach of this Data Protection Policy or related information procedures and guidance.

 All personal data breach incidents must be reported immediately by e-mail to dataprotection@fife.gov.uk as the Council has a duty to report any personal data breach to the Information Commissioner’s Office (ICO) within 72 hours.

 The Council has a Data Protection team who can provide further advice and guidance in relation to security incidents. They can be contacted at dataprotection@fife.gov.uk

**8. Policy Compliance**

If any officer is found to have breached this policy, they may be subject to the Council’s disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

 If you do not understand the implications of this policy or how it may apply to you, seek advice from the Data Protection Officer or Senior Information Risk Owner.

**9. Training**

 Regular Data Protection training is mandatory for all Elected Members and employees of Fife Council. Training requirements will be assessed based on work role.

 Executive Directors are responsible for ensuring that employees within their Service are trained appropriately.

 The Council’s Data Protection team will assist Services in evaluating training needs and ensuring adequate resources are provided.

**10. References**

 This policy statement is underpinned by supporting policies, procedures and guidelines. The documents listed below are all available on FISH. The Data Protection and Freedom of Information Subject page is a good starting point.

National Code of Conduct for Councillors

Electronic Mail and Messaging Policy

Employee Code of Conduct

Employee Data Policy

Information Requests Policy

Information Security Policy

Information Security Incident Management Policy

Mobile Electronic Computing Devices & Removable Storage Media

Password Management Policy

Records Management Policy

System Access Policy for Non-Council Employees

Transfer of data out-with the EU

Privacy Impact Assessment Template and Guidance

Data Sharing Guidance

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**REVISION HISTORY**

Date: 30/11/10 Revision: 1 Created by: L Gauld

Update of the existing Data Protection Policy (created 2004) to ensure alignment with current business practices.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: 15/03/12 Revision: 2 Changed by: L Gauld

Update to ensure alignment with current business practices.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: 08/03/13 Revision: 3 Changed by: L Gauld

Updated to include references to new policies.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: 20/02/2017 Revision 4 Changed by: K Berry/K Welsh

Update to reflect current business practices.

Approved on 28-02-2017 by Eileen Rowand, Executive Director, Finance & Corporate Services.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: 26/07/2017 Revision 4.1 Changed by: K Berry/K Welsh

Update to reflect ICO audit recommendations.

Approved on 26-07-2017 by Martin Kotlewski, Solutions & Service Assurance Manager, BTS, Finance & Corporate Services.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: 22/08/2017 Revision 4.2 Changed by: K Berry/K Welsh

Update to reflect ICO audit recommendations.

Approved on 22-08-2017 by Martin Kotlewski, Solutions & Service Assurance Manager, BTS, Finance & Corporate Services.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: 01/05/2018 Revision 5 Changed by: K Berry/K Welsh

Update to reflect GDPR Legislation.

Approved on 01/05/18 by Eileen Rowand, Executive Director, Finance & Corporate Services.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: 20/12/2018 Revision 5.1 Changed by: K Berry/K Welsh

Updated to reflect Assessors and Fife Licennsing Board as separate Data Controllers.

Approved on 20/12/2018 by Fiona Stuart, Data Protection Officer, Finance & Corporate Servicees.