ORKNEY
ISLANDS COUNCIL

Data Protection Policy

All our written information can be made available, on request, in a range of different formats and languages. If you would like this document in any other language or format, please contact Corporate Services on 01856873535 or email corporateservices@orkney.gov.uk.

Contents

1. Policy Statement 3
2. Introduction 4
3. Definitions 4
4. Roles and Responsibilities 5
5. Lawful Bases for Processing Personal Information 7
6. Rights of Individuals 8
7. The Data Protection Principles 8
8. Notifying the Information Commissioner 9
9. Processing Personal Information 9
10. Training 9
11. Information Security 10
12. Complaints 10
13. Breaches of Security 10
14. Monitoring and Reporting 10
15. Related Policies and Procedures 10
16. Further Information and Guidance 11

1. Policy Statement

To operate efficiently, Orkney Islands Council must 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 to comply with the requirements of government.

Orkney Islands Council regards respect for the privacy of individuals and the lawful and careful 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 proportionately.

To this end Orkney Islands Council is committed to protecting the rights and privacy of individuals including those rights set out in the General Data Protection Regulation and other data protection legislation.

The Council's principal aim is to ensure that all personal data processing carried out by the Council, or on its behalf, complies with the six data protection principles and other key legislative requirements.

This Policy applies to all employees and elected members as well as consultants, volunteers, contractors, agents or any other individual performing a function on behalf of the Council.

2. Introduction

The Council increasingly depends on computer systems and paper records (paper files) to carry out much of its normal business. In 1998, when the previous Data Protection Act 1998 was enacted by Parliament, the internet was in its infancy, social media and smart telephones had not been invented and the way we shared information was very different. The General Data Protection Regulation protects the rights of individuals in these new circumstances. This policy sets out how the Council will protect the rights of individuals and comply with the law.

To comply with the current legislation, all employees, elected members, consultants, volunteers, contractors and other agents of the Council who use its computer facilities or paper files to hold and process personal information must comply with the Policy.

3. Definitions

3.1 Personal Data

This is data which relates to a living individual ("data subject") who can be identified:

- From the data.
- From the data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

This includes the name, address, telephone number, national insurance number as well as 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.

3.2 Special Category Data

This is personal data consisting of information as to any of the following:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetics.
- Biometrics (where used for ID purposes).
- Health.
- Sex life.
- Sexual orientation.

Special category personal data is subject to much stricter conditions of processing.

3.3 Record

A record is recorded information, in any form, including data in systems created, received and maintained by the Council and kept as evidence of such activity.

3.4 Vital Record

This is a record without which an organisation would be unable to function or to prove that a key activity had taken place.

3.5 Format

A record can be in any format including (but not limited to) paper files, e-mail, audio/visual, electronic documents, systems data, databases, digital images and photographs.

3.6 Records Management

The control of the Council records during their lifetime, from creation to storage until archiving or destruction.

3.7 Record Keeping System

A system or procedure by which the records of the Council are created, captured, secured, maintained and disposed.

3.8 Processing

The definition of processing covers everything from obtaining and gathering in information to using the information and, eventually, destroying the information.

3.9 Data Controller

A Data Controller is a person or organisation who decides how any personal information can be held and processed, and for what purposes. Orkney Islands Council is a Data Controller.

3.10 Joint Data Controllers

These are people or organisations (for example, Orkney Islands Council, NHS Orkney or Police Scotland) who jointly process and share information.

3.11 Data Processor

This role is carried out by any person other than a Council employee (for example, contractors and agents) who process personal information on behalf of the Council.

4. Roles and Responsibilities

4.1 Information Asset Owners

The Information Asset Owners (IAOs) are the members of the Senior Management Team. Their role is to understand what information is held by their service, what is added and what is removed, how information is moved, and who has access and why. Through their Heads of Service and management teams they must ensure that written procedures are in place and followed relating to these activities, risks are assessed, mitigated and the risk assessment processes are audited. IAOs will appoint Information Asset Administrators to provide advice to members of staff.

Overall responsibility and accountability for ensuring that all staff and associated third parties comply with information legislation, this Policy and associated policies and procedures, lies with the Senior Management Team.

4.2 Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) has overall strategic responsibility for governance in relation to data protection risks. The SIRO:

- Acts as advocate for information risk at the Senior Management Team.
- Provides written advice to the Chief Finance Officer for the Annual Governance Statement relating to information risk.
- Drives culture change regarding information risks in a realistic and effective manner.
- Oversees the reporting and management of information incidents.
- In liaison with the Chief Executive and the Executive Directors, ensures the Information Asset Owner and Information Asset Administrator roles are in place to support the SIRO role.

The Council's SIRO is the Executive Director of Corporate Services.

4.3 Data Protection Officer

The role of the Data Protection Officer (DPO) is to:

- Inform and advise the Council and its employees about their obligations to comply with the General Data Protection Regulation and other data protection laws.

- Monitor compliance with the General Data Protection Regulation and other data protection laws, including the assignment of responsibilities, awareness raising, and training of staff involved in the processing operations and related audits.

- Provide advice about data protection impact assessments and monitor their performance;

- Co-operate with the supervisory authority (the Information Commissioner's Office).

- Act as the contact point for the Information Commissioner's Office on issues related to the processing of personal data.

The Council's DPO is the Head of Legal Services.

4.4 Information Asset Administrators

Each Executive Director has nominated one or more Information Asset Administrator(s) to the Council's Information Governance Group. They are responsible for providing routine advice on data protection to their respective services.

4.5 Information Governance Officer

The Information Governance Officer (IGO) is responsible for developing, delivering and maintaining a comprehensive information governance and security framework for the Council. He/she will help ensure compliance with legislative frameworks governing the access to, retention, sharing and disposal of information.

The Information Governance Officer is responsible for reporting all personal information held by the Council to the Information Commissioner.

The IGO will collect information to identify the Council's processing activities, analyse the processing activities and provide information to the DPO so he or she can inform, advise and issue recommendations to the Council.

The IGO will assist services in the carrying out of data protection impact assessments where required.

4.6 Information Security Officer

The Information Security Officer is responsible for creating, implementing and maintaining the Council's security policy and procedures to reflect changing local and national requirements. This includes requirements arising from legislation, security standards and national guidance.

The Information Security Officer will support service areas on achieving best practice and compliance with security requirements.

4.7 Archivist

The Archivist will ensure that policies and procedures are compatible with legislation, particularly in relation to the transfer of records to the archive and their subsequent storage and access.

4.8 Individual Members of Staff and Elected Members

Individual members of staff and elected members are responsible for protecting personal information held or processed on computer, or held in paper records, within their care.

4.9 Information Governance Group

The Council's Information Governance Group (IGG), among its various functions in relation to information management, assists the Council to implement the Policy. The members of the IGG are the Data Protection Officer, the Information Governance Officer, the Information Security Officer, the Archivist and the Information Asset Administrators. The IGG is chaired by the Information Governance Officer.

5. Lawful Bases for Processing Personal Information

The lawful bases for processing are set out in the General Data Protection Regulation. At least one of these must apply whenever the Council processes personal information:

- **Consent**: the individual has given clear consent for the Council to process his/her personal data for a specific purpose.
- **Contract**: the processing is necessary for a contract that the Council has with the individual, or because the individual has asked the Council to take specific steps before entering into a contract.
- **Legal obligation**: the processing is necessary for the Council to comply with the law (not including contractual obligations).
- **Vital interests**: the processing is necessary to protect someone's life.

- **Public interest**: the processing is necessary for the Council to perform a task in the public interest or in the exercise of official authority vested in the Council.
- **Legitimate interests**: the processing is necessary for the purposes of legitimate interests pursued by the Council or a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. However, this basis is not available to processing carried out by the Council in the performance of its official tasks; it can only apply to the Council when it is fulfilling a different role.

6. Rights of Individuals

The General Data Protection Regulation provides individuals with the following rights regarding their personal information:

- The right to be informed about how their information will be used.
- The right of access to their personal information.
- The right to rectification, which is the right to require the Council to correct any inaccuracies.
- The right to request the erasure of any personal information held by the Council where the Council no longer has a basis to hold the information.
- The right to request that the processing of their information is restricted.
- The right to data portability.
- The right to object to the Council processing their personal information.
- Rights in relation to automated decision making and profiling.

The Council will publish detailed information for the public that will set out what these rights are and how these can be exercised.

7. The Data Protection Principles

The General Data Protection Regulation sets out six principles for the processing of personal information which are legally binding on the Council. The personal information must be:

7.1.

Processed lawfully, fairly and in a transparent manner in relation to the data subject.

7.2.

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.

7.3.

Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

7.4.

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.

7.5.

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 General Data Protection Regulation in order to safeguard the rights and freedoms of the data subject.

7.6.

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.

8. Notifying the Information Commissioner

The Council must advise the Information Commissioner's Office that it holds personal information about living people.

9. Processing Personal Information

The Council will hold and process personal information only to support those activities it is legally entitled to carry out.

The Council may on occasion share personal information with other organisations. In doing so, the Council will comply with the provisions of the Information Commissioner's Data Sharing Code of Practice.

The person the personal information is collected from must be advised of the purpose for which the information will be held or processed and who the information may be shared with.

10. Training

All staff will be provided with training in basic data protection law and practice as soon as reasonably practicable after starting to work for the Council. All staff (including supply/relief) have a confidentiality clause in their contracts of service. They also sign an Information Security User Acceptance for the Information Security User Guidance.

Staff who work on computer systems that hold or process personal information, or who use the information associated with those systems, will receive relevant training. If written procedures for using such systems are not yet in place, staff will be trained in legitimate ways of finding and providing information and told which information must not be recorded.

Any new Information Asset Administrators will be trained in data protection relating to their responsibilities for their business area.

Managers may wish to request in-depth training for their staff, particularly if they are dealing with Special Category Data. In these circumstances they should contact the relevant Information Asset Administrator in the first instance to enable appropriate arrangements to be made.

Local training modules can be put in place for service areas who routinely deal with more sensitive personal and/or confidential information.

Elected Members will be provided with training in basic data protection law and practice as soon as reasonably practicable after they are elected.

11. Information Security

The Council's approach to Information Security is set out in its Information Security Policy and in the 'Orkney Islands Council Information Security Staff Guidance' document.

12. Complaints

Any complaints received by, or on behalf of, a member of the public containing allegations of inappropriate disclosure of information will be dealt with in the normal way through the Council's Complaints Handling Procedure in the first instance.

If an individual does not feel that the Council is treating their data appropriately or has not answered their complaint they can contact the Information Commissioner.

13. Breaches of Security

Organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. Despite the security measures taken to protect personal data held by the Council, a breach can happen.

If a breach occurs the IGO must immediately be informed who will put into place a Breach Management Plan. Where an IT security breach occurs, this will be reported to the Information Security Officer who will respond to it in accordance with the provisions of the Information Security Policy.

More information on breach management can be found on Information Commissioner's Office Guidance on Data Security Breach Management.

14. Monitoring and Reporting

This policy will be reviewed annually by the Information Governance Officer.

Proposed changes to information governance policies or procedures will be considered by the Information Governance Group in the first instance.

A review of the Council's compliance with relevant legislation and best practice will be reported to Elected Members on an annual basis.

15. Related Policies and Procedures

- Orkney Islands Council Records Management Policy.

- Orkney Islands Council Information Security Policy.
- Orkney Islands Council Records Retention Schedule.
- Orkney Islands Council Freedom of Information Policy.
- Orkney Islands Council Personal Information – Your Rights.
- Orkney Islands Council Complaints Handling Procedure.

16. Further Information and Guidance

Information Governance Officer
Corporate Services
Orkney Islands Council
Council Offices
Kirkwall
KW15 1NY

E-mail: corporateservices@orkney.gov.uk

Tel: 01856873535, extension 2210.

Further information is also available from the Information Commissioner's website.

Document control Sheet

Review/Approval History

Date	Name	Position	Version Approved
9 April 2018	Gavin Mitchell	Head of Legal Services	V1.0 Council 1 May 2018

Change Record Table

Date	Author	Version	Status	Reason

Status Description

Final – The document is complete and is not expected to change significantly. All changes will be listed in the change record table.