Data Protection Policy

ENSURING COMPLIANCE WITH THE GENERAL DATA PROTECTION REGULATION AND THE DATA PROTECTION ACT 2018

Council of the ISLES OF SCILLY

May 2018 - Version 1.0

Revisions to Source Document

Version	1.0	Approving Committee	N/A
Date	11 May 2018	Ratified by Council	N/A
Responsible Officer	Simon Mansell, Data Protection Officer (DPO)	Review Date	May 2019

Version History

Date	Version	Author/Editor	Comments
11 May 2018	1.0	Jemma Pender	Draft for Approval by DPO

Equalities Impact Assessment Record

Date	Type of Assessment Conducted	Stage/Level completed (where applicable)	Summary of Actions Taken Decisions Made	Completed by.	Impact Assessment Review date

Document retention

Document retention period	Until superseded

CONTENTS

Revisions to Source Document 1
Version History 1
Equalities Impact Assessment Record 1
Document retention 1
Contents 2
Introduction 3
Background 3
Objective 4
Scope 5
Details 5
Document Information 9

If you require this document in an alternative language, in larger text, Braille, easy read or in an audio format, please contact the Council at diversity@scilly.gov.uk or telephone 0300 1234 105

Council of the Isles of Scilly
Town Hall
St Mary's
Isles of Scilly
TR21 0LW

Introduction

1.1 The General Data Protection Regulation 'GDPR' and the Data Protection Act 2018 (the 'Act') cover any information held about a living, identifiable individual.

1.2 GDPR and the Act gives individuals the right to know what information the Council holds about them, the right to have this data rectified if it is incorrect or incomplete and it gives an individual the right to have the data erased if it is out of date, or we are processing without the consent of the individual.

1.3 GDPR and the Act also provide a framework to ensure that the Council handles personal information properly.

1.4 GDPR and the Act applies only to information relating to a living person.

1.5 GDPR states that anyone who processes personal information must comply with six principles and must be able to show such compliance under the accountability requirement.

1.6 GDPR provides individuals with important rights, including the right to find out what personal information is held by the Council on computer and most paper records under the Right of Access, the right to have incorrect data erased or completed under the Right to Rectification and the right to have their data erased under the Right to Erasure if there is no longer a statutory reason to process the data, or if the individual has withdrawn consent.

1.7 Both GDPR and the Act also allows in certain circumstances two or more organisations sharing information between them and the sharing of information between the various parts of a single organisation, for example between the Council's various departments, but this right should not be taken as automatic.

Background

2.1 The sharing of up to date accurate information is fundamental to the Council's goal of delivering better and more efficient public services that are coordinated around the needs of our service users and in order to achieve this, when there are grounds to do so, the Council will seek to share information with its partners and the wider community. However, we recognise that the move we share information, the more important it is that people are confident that their personal data is kept safe and secure.

GDPR covers any information held about a living, identifiable individual. It gives individuals the right to know what information the Council holds about them and the ability to have this rectified or erased. It also provides a framework to ensure that the Council handles personal information properly.

GDPR and the Act builds on the rights that were created under the Data Protection Act 1998 for those who have their data stored, and places additional responsibilities on those who access and process personal data.

The six Data Protection Principles Article 5(1) of GDPR set out that personal information shall be:

a) "processed lawfully, fairly and in a transparent manner in relation to individuals;
b) 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 or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving 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
f) 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."

Article 5(2) then requires that:

"the controller shall be responsible for, and able to demonstrate, compliance with the principles."

OBJECTIVE

3.1 The purpose of this policy is to ensure the Council applies appropriate measures to comply with GDPR and in particular, but not solely, the six principles as summarised below. This will help the Council meet its statutory requirements and mitigate penalties imposed by GDPR and the Act which will be enforced by the Information Commissioner's Office.

The Council also wishes to ensure that the information it holds is both accurate and appropriate in order to facilitate good decision making. Holding out of date data is a breach of the data protection principles and could result in the Council receiving a fine and can lead to the Council making inaccurate decisions.

Personal information (data relating to a living individual):

- Must be processed fairly and lawfully
- Must be obtained for one or more specified and lawful purpose and only processed in a manner compatible with them
- Must be adequate, relevant and not excessive for the purposes defined
- Must be accurate and where necessary kept up to date
- Shall not be kept for longer than is necessary
- Must be processed in accordance with the data subject's rights

There are now separate restrictions on processing data outside the EEA that can be found in Articles 45 and 46 of GDPR.

SCOPE

4.1 This policy applies to personal and special categories of personal information held by the Council. Anyone who processes personal and special categories of information for the Council or on behalf of the Council either has to adopt this policy or prove that they have equivalent policies in place.

DETAILS

5.1 Policy

The Council of the Isles of Scilly regards the lawful and correct handling of personal information as essential to successful operations and to maintaining the confidence of those with whom we deal. We will always do our utmost to ensure that our organisation treats personal information lawfully and correctly.

To this end we fully endorse and adhere to the Data Protection Principles as set out in the GDPR.

5.2 Information Sharing

There are various types of information sharing. For example, organisations may share information between them. This could be achieved by giving access to each other's information systems or by setting up a separate shared database. This may lead to the specific disclosure of a limited amount of information, for example bulk matching name and address information in two databases. Another example involves the sharing of information between the various parts of a single organisation, for example between a local authority's various departments.

Where the Council intends to share personal information across departments or with other agencies, the relevant service shall ensure that an Information Sharing Agreement is in place which will govern how information will be shared. For further guidance on Information Sharing Agreements please contact the Data Protection Officer (DPO).

5.3 **Privacy Notices**

Processing personal data fairly includes being transparent about how we intend to use it, including who it will be shared with. In order to achieve this, clear privacy notices (also known as fair collection/processing notices/statements) must be made available when collecting personal data from our service users (data subjects). For further details please contact the DPO or see the Privacy Notice Guidance on the Information Commissioner's Office (ICO) website: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/your-privacy-notice-checklist/

5.4 **Consent Notices**

The GDPR is clearer that an indication of consent must be unambiguous and involve a clear affirmative action (an opt-in). It specifically prohibits pre-ticked opt-in boxes. It also requires distinct ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not be a precondition of signing up to a service.

You must keep clear records to demonstrate consent.

The GDPR gives a specific right to withdraw consent. You need to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time.

Public authorities, employers and other organisations in a position of power may find it more difficult to show valid freely given consent.

You need to review existing consents and your consent mechanisms to check they meet the GDPR standard. If they do, there is no need to obtain fresh consent.

5.5 **Management**

The Council's DPO is the designated Council owner of the Data Protection Policy and is responsible for the maintenance and review of the Data Protection Policy, Standards, Guidelines and Procedures in consultation with the Officer: Policy and Scrutiny.

CLT are responsible for overseeing day to day issues relating to data protection; developing and maintaining corporate data protection procedures, guidance and training

The Council's SIRO is responsible for managing corporate information risks, including maintaining and reviewing an information risk register.

The Council's Caldicott Guardian is responsible for protecting the confidentiality of service user personal information to ensure that standards are met when handling personal and sensitive personal information in health and social care.

The Council's DPO is responsible for compliance with the requirements of the General Data Protection Regulation.

Senior Managers and Officers are responsible for ensuring that staff are made aware of and comply with the Data Protection Policy, Standards, Guidelines and Procedures.

Users accessing Council information are required to adhere to the Data Protection Policy, Standards, Guidelines and Procedures.

It will be the responsibility of each Senior Manager (or delegated advisor) to:

- Ensure their Business Unit's compliance with the GDPR and the Act and implement agreed work and training programmes for Data Protection.
- Ensure any specific responsibilities for Data Protection are recorded in role profiles.
- Arrange for Requests for Rights of Access, Rectification and Erasure to be carried out within their Business Unit.
- Ensure that staff receive appropriate Data Protection and information security training and that training is monitored.
- Identify and record information asset owners within their Business Unit.
- Disseminate guidance to information asset owners within their Business Unit.
- Ensure that information asset owners are trained in the principles of the Act and the procedures for their implementation within the Council.
- Ensure that any contractor, consultant, partner or other persons who are providing goods or services on behalf of the Council are made aware of their obligations under this policy.
- Undertake other Data Protection tasks assigned by the DPO.
- Monitor compliance with this policy.

It will be the responsibility of each information asset owner to:

- Inform their Business Unit's Senior Manager and the DPO of the processing of personal data in their service to ensure that annual notification to the ICO is accurate.
- Ensure that they receive training on the GDPR and the Act
- Ensure that the information asset delegates assigned to their datasets are made aware of the standards applicable to their datasets and monitor their adherence.

It is everyone's responsibility to:

- Understand and implement the six Data Protection Principles
- Immediately report any breaches of the Data Protection Act using the Council's Information Security Incident Reporting Procedure.

All contractors, consultants, partners or other persons who provide goods or services on behalf of the Council must:

- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the Council, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the GDPR or the Act shall be grounds on which the Council may terminate the contract with that individual, company, partner or firm.

- Allow data protection audits by the Council of data held on its behalf (if requested).
- Indemnify the Council against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation arising out of a breach by them of the Act.
- All contractors who are users of personal information supplied by the Council will be required to confirm that they will abide by the requirements of the GDPR or the Act with regard to information supplied by the Council.

5.6 **Breaches and non-compliance**

The Employee Code of Conduct which forms part of your Contract of Employment includes a commitment to protecting personal and sensitive personal data you come into contact with in your role. Breaches of the GDPR or the Act could be regarded as gross misconduct and may result in disciplinary action up to and including dismissal.

There is also personal liability for breaches under your Contract of Employment and the GDPR and the Act.

Where external service providers, agents or contractors breach the policy, this should be addressed through contract arrangements.

If you see a breach of this policy, you must follow the Security Incident and Data Breach Policy and report it using the Security/Data Protection Breach Referral form.

5.7 **How the impact of the policy will be measured**

The DPO will monitor compliance with the policy. Indicators to monitor the performance on compliance with the GDPR and the Act are:

- Recording the number of requests for Rights of Access, Rectification and Erasure and any failures on the part of the Council or its contractors to comply with these rights.
- Recording statistics regarding information security incidents will form the basis for reports to the Senior Information Risk Owner (SIRO), Extended Leadership Team (ELT) and Corporate Leadership Team (CLT).
- Recording statistics regarding legislative compliance relating to Requests are reported to ELT on a monthly basis, and to CLT on a six monthly basis.

Potential risks will be regularly monitored and evaluated to ensure this policy is kept up to date.

5.8 **Evaluation and review**

This policy will be reviewed annually, or as demanded by business need, by CLT in consultation with the Council's DPO.

This policy will be signed off by the Council's DPO.

Document Information

6.1 Contacts

Policy prepared by the Council's DPO and reviewed by the Council's Officer: Policy and Scrutiny.

6.2 Further information

Users should read this policy in conjunction with the Council's Employee Code of Conduct, and information governance and information security policies, procedures and guidance:

Further information about this policy is available from the Council's DPO.

An online training programme on the Information Governance and GDPR is available to ensure that all staff are aware of their obligations around information rights legislation (Data Protection, Freedom of Information, etc.) and Records Management. Staff must complete the training programme every year.