Data Protection Policy

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

Council of the ISLES OF SCILLY

October 2025 - Version 2.3

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
8 September 2020	2.0	Jemma Pender & Tom Walton	Review and inclusion of confidentiality, data quality and records management to satisfy NHS Data Security and Protection Toolkit. To consider for future revisions: - Data protection by design and default should probably be captured elsewhere in the document as it doesn't only relate to data quality. - An equalities impact assessment has not been carried out – this should be considered at the next review.
18 May 2023	2.1	Jemma Pender & Tom Walton	Reviewed to reflect data processing by Cornwall Council
20 May 2025	2.2	Jemma Pender	Roles updated
20 October 2025	2.3	Jemma Pender	Roles updated

Equalities Impact Assessment Record

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

			Decisions Made		

CONTENTS

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 As a user of personal data, the Council is required to comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA), which cover any information held about a living, identifiable individual.

1.2 The UK GDPR is the UK General Data Protection Regulation (EU) 2016/679. It sets out the key principles, rights and obligations for most processing of personal data.

1.3 The DPA 2018 sets out the framework for data protection law in the UK. It sits alongside the UK GDPR, and tailors how the UK GDPR applies in the UK - for example by providing exemptions. It also sets out separate data protection rules for law enforcement authorities, extends data protection to some other areas such as national security and defence, and sets out the Information Commissioner's functions and powers.

1.4 The UK GDPR and the DPA give 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 the right to have the data erased if it is out of date/incorrect, or we are processing without the consent of the individual.

1.5 The UK GDPR and the DPA also provide a framework to ensure that the Council handles personal information properly.

1.6 The UK 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.

1.7 The UK 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.

1.8 Both the UK GDPR and the DPA also allow 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.

Data Protection Principles

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

1. "processed lawfully, fairly and in a transparent manner in relation to individuals;
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 or statistical purposes shall not be considered to be incompatible with the initial purposes;

3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
4. 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;
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 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 UK GDPR in order to safeguard the rights and freedoms of individuals; and
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."

Article 5(2) then requires that:

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

Purpose and Scope of this Policy

3.1 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 UK GDPR (as above).

3.2 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. This will help the Council meet its statutory requirements and mitigate penalties imposed by the UK GDPR and the DPA which will be enforced by the Information Commissioner's Office (ICO).

3.2 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.

Categories of data and Conditions of Processing

4.1 Personal Information

Personal data only includes information relating to living individuals who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.

This information:

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

4.2 Processing of personal information

The Council can only process personal data where at least one of the following applies:

- The individual has given the Council their clear consent
- It forms part of a contract or pre-contractual negotiations between the Council and the individual
- It is necessary for the Council to comply with a legal obligation (other than one imposed by a contract with the individual) and a privacy notice has been supplied
- It is in the vital interest of the data subject - applies only if it is a life or death situation
- The processing is necessary for:
    - administration of justice
    - the exercise of any functions conferred by or under any enactment
    - the exercise of any other public function in the public interest

4.2 Special Categories of Data

Personal data may also include special categories of personal data. These are considered to be more sensitive and you may only process them in more limited circumstances. Special categories of data are defined in the UK GDPR as information relating to an individual's:

- Racial or ethnic origin
- Political Opinions
- Religious or similar beliefs
- Trade Union membership
- Physical and mental health conditions

- Sexual life and sexual orientation
- Genetic data
- Biometric data (when processed to identify a person)

4.2 **Processing of Special Categories of Personal Data**

The Council can only process special categories of personal data, where at least one of the following conditions can be met:

- The individual has given the Council their clear and unambiguous consent
- The processing is necessary for performing any right or obligation imposed on the Council by law in connection with employment (e.g. where information is processed about employees with disabilities in compliance with the Equality Act 2010)
- The Council is protecting the vital interest of the data subject or another and consent cannot be given (e.g. where the data subject is physically or legally incapable) or reasonably sought (e.g. because the data subject cannot be located)
- The information has deliberately been made public by the data subject (e.g. a politician who has made public his political beliefs)
- The Council is processing information for:
    - the purpose of, or in connection with, legal proceedings
    - the purposes of obtaining legal advice
    - the purpose of establishing, exercising or defending legal rights.
- The processing is necessary for:
    - the administration of justice
    - the exercise of a function under an enactment
    - the exercise of a function of the Crown, a minister of the Crown or a government department
- You are processing for medical purposes and you are a health professional or someone who, in the circumstances, owes the same duty of confidence as is expected from a health professional - processing by the Council is not covered by this condition.
- The Council is processing the information in accordance with an order made by the secretary of state

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

INFORMATION SHARING

5.1 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.

5.2 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).

RESPONSIBILITIES

6.1 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 Senior Information Risk Owner (SIRO). The Council's DPO is also responsible for compliance with the requirements of the UK GDPR.

6.2 The Council's SIRO is responsible for managing corporate information risks, including maintaining and reviewing an information asset register. Individual Information Asset Owners (IAOs – normally a Senior Manager or Senior Officer) must be assigned and take responsibility for managing their own information assets.

6.3 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.

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

6.5 Everyone is responsible for overseeing day to day issues relating to data protection. Users accessing Council information are required to adhere to the Data Protection Policy. **Staff must complete the mandatory Information Governance online training on an annual basis.**

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

- Ensure their Business Unit's compliance with the UK GDPR and the DPA and implement agreed work 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 complete mandatory information governance training and any further training deemed necessary.
- Identify and record information asset owners within their Business Unit.
- Disseminate guidance to information asset owners within their Business Unit.
- 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.

6.7 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.
- Complete information governance mandatory training.
- Ensure that the information asset delegates assigned to their datasets are made aware of the standards applicable to their datasets and monitor their adherence.

6.8 It is everyone's responsibility to:

- Understand and implement the six Data Protection Principles
- Immediately report any breaches of the DPA 2018 using the Council's Security Incident and Data Breach Procedure.
- Complete information governance mandatory training.

6.9 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 DPA. Any breach of any provision of the UK GDPR or the DPA 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 DPA.
- 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 UK GDPR and the DPA with regard to information supplied by the Council.

PRIVACY NOTICES

7.1 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/business/create-a-privacy-notice/

7.2 The Council has an overarching privacy notice which explains our approach to data handling for the whole organisation and our customers' rights in relation to their data. You must still have service specific notices in place for the data you handle.

Consent Notices

8.1 The UK GDPR specifies that 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.

8.2 Consent is required only in the following circumstances:

- When collecting information to provide a non-statutory service. The council does not need consent to collect personal information to provide a statutory service i.e. a service the council is required by law to provide.
- If the personal information is used or shared for any purpose not related to that which it was collected for. This includes sharing with other teams in the council or with another third party.

8.3 Third parties are those you will pass the personal information to, for instance a data processor or partner such as the NHS. When seeking consent, you must name any third parties who will rely on this consent and record how, when and what was said.

8.4 You must keep clear records to demonstrate consent. Records of gaining consent are necessary in case you need to provide this as evidence at a later date. You must also record details if consent is withheld.

8.5 Remember that consent can be withdrawn at any time. The UK 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.

Breaches and Non-Compliance

9.1 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 within your role. Breaches of the UK GDPR or the DPA could be regarded as gross misconduct and may result in disciplinary action up to and including dismissal. Rarely, and in deliberate or highly negligent cases, this could also result in personal prosecution.

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

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

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

CONFIDENTIALITY

10.1 Confidential information includes information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including service user information, employee records, occupational health records, etc. It also includes the Council's confidential business information e.g. commercially sensitive contracts, trade secrets and procurement information, which should also be treated with the same degree of care.

10.2 Confidentiality relates to the internal and external sharing, by whatever means of personal, sensitive or identifiable information about individuals or organisations (commercial in confidence information), which comes into the possession of the Council through its work. This definition applies to all data that is known to officers or contractors regardless of whether this is recorded data or not.

10.3 The Council of the Isles of Scilly is committed to making sure that it protects the data of its service users and staff and to ensure compliance with the UK GDPR and the DPA. By adhering to these legislative requirements, we can ensure that the common law duty of confidentiality and the right to privacy under the Article 8 of the Human Rights Act 1998 will be adhered to at all times.

10.4 The following confidentiality principles must be adhered to:

- Personal or confidential information must be effectively protected against improper disclosure when it is received, stored, transferred (by whatever means) or disposed of.
- Access to personal or confidential information must be on a need-to-know basis and the minimum amount necessary should be used.
- Disclosure of personal or confidential information must be limited to the purpose for which it is required.

10.5 Staff must always take sufficient steps check the identity of the recipient and never assume someone is who they say they are. All staff have a legal duty of confidence to keep personal or confidential information private and must not intentionally divulge confidential information to a recipient they know is not entitled to it.

10.6 Recipients of information must always be made aware that it is given to them in confidence.

10.7 Staff must remember that in some circumstances the duty to share information can be as important as the duty to protect information - if in doubt ask.

10.8 If the decision is taken to disclose or share information, either internally with other Council Services, or externally with stakeholders/partners, that decision must be justified and documented and the grounds for sharing recorded. An information sharing agreement should be considered for routine information sharing. Contact the information governance team, either jemma.pender@scilly.gov.uk or tom.walton@scilly.gov.uk if you think an information sharing agreement may be required.

10.9 In certain circumstances it may help to ensure confidentiality if personal information is anonymised or pseudonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data.

In order for data to be truly anonymised under the UK GDPR, it must be stripped of sufficient elements (e.g. name, address, date of birth) that the individual can no longer be identified. However, if anyone could at any point use any reasonably available means to re-identify the individuals to which the data refers, that data will not have been effectively anonymised but will have merely been pseudonymised.

The UK GDPR defines pseudonymisation as "…the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

Pseudonymised data is still considered personal data under UK GDPR, anonymised data is not.

10.10 Confidential or personal information can be shared or disclosed if it is required by law or under a court order – if you receive such an order or a request from the police to share data please contact the DPO at dpo@scilly.gov.uk.

10.11 Identifiable personal information can be shared or disclosed in safeguarding proceedings if it is considered that the information required is in the public or vulnerable persons' interest under UK GDPR Regulation 6(1)(d) and Article 9(2)(c) vital interests, and agreed information sharing agreements where applicable.

10.12 Confidential or personal information can be shared or disclosed where disclosure can be justified for another purpose. This can be, for example, for the protection of the public and in this scenario, it is likely to be in relation to the prevention and detection of serious crime under Schedule 2 of the Data Protection Act 2018. If you consider there may be grounds for the sharing of data in this manner you should seek advice from the DPO at dpo@scilly.gov.uk.

10.13 Staff must ensure that appropriate standards and safeguards are in place and followed in respect of dealing with all information, including office conversations, telephone enquiries, emails, faxes and mail and follow the Council's Confidentiality Guidelines and Information Sharing guidance in relation to methods of communication and transfer.

This includes any additional procedures that relate to specific information e.g. role-based access to information and systems.

10.14 Transferring personal or confidential information by email or file sharing to anyone outside the Council network may only be undertaken if it has been captured in the appropriate documentation and approved by the information governance team or someone with an appropriate formal delegation

10.15 Sending confidential or personal information via email to service users is permissible, provided the risks of using unencrypted email have been explained to them and they have given their consent and the information only relates to them. **If you use the auto fill to pick the email address in outlook you MUST ensure that the right address is selected**.

10.16 When working in and away from the office environment, staff must ensure that their working practice complies with the Council's policies and procedures.

10.17 If it is necessary to take home/remove paper documents that contain personal or confidential information from Council premises you must ensure that only the minimum required is taken and that it is transported and stored securely. You must ensure at all times that any paper documents, or electronic medium that is used to store data is not left in a vulnerable position, such as in a car, overnight.

10.18 It is strictly forbidden for employees to knowingly browse, search for or look at any information relating to themselves, their own family, friends or other persons, without a legitimate purpose. Action of this kind will be viewed as contrary to the requirements of confidentiality as set out in the Employee Code of Conduct and will be a breach of confidentiality in respect of the UK GDPR and of the Data Protection Act 2018.

10.19 Staff may be held personally liable for a breach of confidence.

10.20 Any concerns about compliance with these principles must be discussed with either your Line Manager or the Democratic and Corporate Team

Data Protection by Design and Default

11.1 All processes must be designed by adopting a data protection by design approach. All staff responsible for setting up or commissioning new services or procuring new systems must ensure that a Business and Privacy Impact Assessment (BPIA) is completed as early as possible in the planning phase to identify and minimize data protection risks and enable a data protection by design approach

Data Quality

12.1 The UK GDPR places an emphasis on the quality of data. Good quality, up to date data helps to ensure the Council's decisions are sound and legally compliant. To achieve this all data handled by the Council must be held and disposed of in accordance with the law.

12.2 There is also a need to ensure that we do not hold inaccurate data or retain data for any longer than necessary. There are strict retention periods that the Council is required to adhere to and after this retention period the data should be disposed of in a secure manner, unless there is a particular reason for keeping the data in agreement with the DPO.

12.3 Anyone who processes data for the Council, or on behalf of the Council must either abide by this policy or prove that they have equivalent policies in place.

12.4 By adhering to the third, fourth and fifth Data Protection Principles from Article 5(1) of UK GDPR (set out in the 'Data Protection Principles' section at the top of this policy) which relate to data quality, we can ensure the Council handles data in a legally compliant way. These principles articulate that all data we handle should be:

- "adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed." **This is sometimes referred to as 'data minimisation.'**
- "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"
- **"**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 UK GDPR in order to safeguard the rights and freedoms of individuals." **This is referred to as 'storage limitation.'**

12.5 When designing and reviewing data creation, collection or retention processes, the following characteristics of data quality, should be considered. An appropriate balance made between the different characteristics to ensure the needs of the users of the data are met.

- Relevant – data that it is collected by the Council is collected for specified and explicit purposes and is not used beyond these purposes;
- Accurate – Data should be accurate, kept up to date thereby ensuring it is current;
- Valid – Data should only be collected in an agreed format and should only be used for the purposes which it is collected for, or in connection with these purposes;
- Complete – All data should be captured should be as complete as is necessary for the purpose which it was captured for, based on the information needs of the Council;
- Secure – Data should be stored securely and confidentially;
- Accessible – Data should be easily available to those who need it, and produced in a suitable format, with accompanying explanations where appropriate;
- Reliable – By ensuring that all data used by the Council meets the above criteria we can ensure that it is reliable.

12.6 In ensuring that the Council maintains a high standard of data quality there needs to be ownership of the data at all levels. Ensuring good data quality can be as simple as checking that an email address is typed into Outlook correctly, or managers verifying that travel claims have been completed correctly.

Retention and Disposal

13.1 **Retention Procedures**

In order to ensure that the data we hold is current, and therefore of good quality, there is a need for all data owners to adhere to the Council's corporate data retention schedule.

13.2 In order to ensure that we are legally compliant with recognised guidelines for retention, the Council uses the Batchelor Retention Schedule, and this must be adhered to for all information that is held by the Council.

13.5 **Disposal Procedures**

Data must not be retained beyond its retention period and must be disposed of in a manner which makes it impossible to then recover.

13.6 The best practise is to have a properly managed disposal process. This has the following benefits for the Council:

- It avoids unnecessary storage costs, either electronic or physical;
- It is legally compliant; and
- Finding and providing information is quicker as there is less to search.

13.7 It is for the Information Asset Owners within each service to ensure that their data handling procedures are compliant in terms of retention and disposal. It is also up to the IAOs to communicate these procedures to all users.

12.8 Disposal schedules can be created in any medium. It is important that they are maintained on a regular basis and retained so the council can demonstrate, if required to do so, what data has been disposed of and is therefore no longer available.

12.9 Records of disposal decisions should clarify which of the following apply:

- That all the information should be destroyed
- That part of the information should be retained. You will need to explain which part of the information is to be retained and why. You will also need to state the disposal date of the retained information.
- That all of the information should be retained.
- That the information needs to be transferred to archive.

How the impact of the policy will be measured

13.1 The DPO and the SIRO will monitor compliance with the policy. Indicators include:

- Mandatory training completion rate.
- Information Asset Register completion.
- Privacy notices in place.
- Data flows recorded for relevant data collection activity.
- Evidence of compliance via spot checks.
- Statistics regarding information security incidents will form the basis for reports to the SIRO who will report further if necessary.
- Recording statistics regarding legislative compliance relating to requests are reported regularly to the management team.

13.2 This policy will be updated and informed by lessons learned from reports of near misses and data breaches and by any risks identified relating to data protection.

Evaluation and Review

14.1 This policy will be reviewed annually.

14.2 This policy will be signed off by the Council's DPO and endorsed by the SIRO.

Contacts

15.1 **Contacts**

Data Protection Officer: Simon Mansell, dpo@scilly.gov.uk
Senior Information Risk Owner: Russell Ashman, russell.ashman@scilly.gov.uk
Caldicott Guardian: Sue Ross, sue.ross@scilly.gov.uk