St Davids City Council
Information and Data Protection Policy

Date Approved by Council: 18 May 2026

Date due for review: May 2027

1. Introduction and Purpose

St Davids City Council ("the Council") is committed to protecting the privacy and security of personal data. This policy sets out how the Council will comply with its obligations under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Data (Use and Access) Act 2025.

The Council processes personal data to deliver services to residents, manage its operations, and fulfil its statutory functions. This policy ensures that personal data is handled lawfully, fairly, and transparently.

This policy applies to all Councillors, employees, contractors, volunteers, and any other individuals who process personal data on behalf of the Council.

2. Legal Framework

The Council must comply with the following legislation:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Privacy and Electronic Communications Regulations 2003 (PECR)
- Freedom of Information Act 2000
- Environmental Information Regulations 2004

The Information Commissioner's Office (ICO) is the UK's independent supervisory authority for data protection. The Council is registered with the ICO as a data controller.

3. The Data Protection Principles

The Council will ensure that all personal data is processed in accordance with the seven data protection principles set out in Article 5 of the UK GDPR:

1. **Lawfulness, fairness and transparency:** Personal data shall be processed lawfully, fairly, and in a transparent manner.
2. **Purpose limitation:** Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
3. **Data minimisation:** Personal data shall be adequate, relevant, and limited to what is necessary.
4. **Accuracy:** Personal data shall be accurate and, where necessary, kept up to date.
5. **Storage limitation:** Personal data shall be kept for no longer than is necessary for the purposes for which it is processed.
6. **Integrity and confidentiality:** Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.
7. **Accountability:** The Council shall be responsible for, and be able to demonstrate compliance with, these principles.

4. Lawful Bases for Processing

The Council will only process personal data where there is a lawful basis to do so. The lawful bases available under UK GDPR Article 6 are:

- **Consent:** The individual has given clear consent for processing.
- **Contract:** Processing is necessary for the performance of a contract.
- **Legal obligation:** Processing is necessary for compliance with a legal obligation.
- **Vital interests:** Processing is necessary to protect someone's life.
- **Public task:** Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.
- **Legitimate interests:** Processing is necessary for legitimate interests pursued by the Council or a third party, except where overridden by the interests of the data subject.

For most Council functions, the lawful basis will be 'public task' as the Council exercises official authority vested in it as a local authority.

5. Individual Rights

The UK GDPR provides the following rights for individuals:

1. **Right to be informed:** Individuals have the right to be informed about the collection and use of their personal data through privacy notices.
2. **Right of access:** Individuals can request access to their personal data (Subject Access Request).
3. **Right to rectification:** Individuals can request correction of inaccurate personal data.
4. **Right to erasure:** Individuals can request deletion of their personal data in certain circumstances.
5. **Right to restrict processing:** Individuals can request the restriction of processing of their personal data.
6. **Right to data portability:** Individuals can request their personal data in a commonly used format.
7. **Right to object:** Individuals can object to processing in certain circumstances.
8. **Rights related to automated decision-making:** Individuals have rights in relation to automated decision-making and profiling.

The Council will respond to requests within one calendar month. Requests should be made in writing to the Clerk.

6. Roles and Responsibilities

6.1 The Council

The Council is the Data Controller and is responsible for ensuring compliance with data protection legislation. The Council will ensure appropriate policies, procedures, and training are in place.

6.2 The Clerk

The Clerk is responsible for the day-to-day management of data protection compliance, acting as the primary point of contact for data protection matters, responding to data subject requests, maintaining the Council's data protection records, and reporting data breaches.

6.3 Councillors

All Councillors must comply with this policy when handling personal data in their capacity as Council members. Councillors should only access personal data necessary for Council business and must keep such data secure.

7. Data Security

The Council will implement appropriate technical and organisational measures to ensure personal data is kept secure. These measures include:

- Password protection on all devices and systems containing personal data
- Encryption of sensitive data where appropriate
- Secure storage of paper records in locked cabinets
- Use of official Council email addresses for Council business
- Regular data backups
- Secure disposal of personal data no longer required
- Staff and Councillor training on data protection

The ICO provides a checklist 'How secure is your personal data?' which the Council will use to review its security measures regularly.

8. Data Breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

In the event of a data breach, the Council will:

1. Assess the nature and severity of the breach
2. Take immediate steps to contain the breach and recover any data
3. Report the breach to the ICO within 72 hours if it is likely to result in a risk to individuals' rights and freedoms
4. Notify affected individuals without undue delay if the breach is likely to result in a high risk to their rights and freedoms
5. Document all breaches and the actions taken

9. Data Retention

The Council will only retain personal data for as long as necessary for the purposes for which it was collected. The Council maintains a retention schedule setting out how long different categories of data will be kept.

When personal data is no longer required, it will be securely destroyed or anonymised.

10. Data Sharing

The Council may share personal data with third parties where there is a lawful basis to do so, such as with other public authorities in the performance of statutory duties, contractors providing services on behalf of the Council (who act as data processors), and where required by law or court order.

Where the Council engages data processors, appropriate contracts will be in place to ensure the processor complies with data protection requirements.

11. Privacy Notices

The Council will provide clear and transparent information to individuals about how their personal data is used through privacy notices. Privacy notices will be published on the Council's website and made available on request.

12. Complaints

Individuals who are dissatisfied with how the Council has handled their personal data may raise a complaint with the Clerk in the first instance. The Council has a formal complaints procedure in place for handling data protection complaints.

If the matter is not resolved satisfactorily, individuals have the right to complain to the Information Commissioner's Office:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF
Telephone: 0303 123 1113
Website: https://ico.org.uk

13. Training

The Council will ensure that all Councillors and staff receive appropriate training on data protection. Training will be provided upon induction and refreshed as necessary.

14. Policy Review

This policy will be reviewed annually or sooner if there are changes to legislation or guidance from the Information Commissioner's Office. Any changes will be approved by the full Council.

15. Related Policies and Guidance

This policy should be read in conjunction with the following:

- St Davids City Council Privacy Notice
- Information Technology Policy
- Document Retention Policy
- Freedom of Information Publication Scheme
- ICO Guide to Data Protection

16. Further Information

For guidance on data protection, the following resources are available from the Information Commissioner's Office:

- Guide to Data Protection: https://ico.org.uk/for-organisations/guide-to-data-protection/
- Data Protection Principles: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/
- Security Checklist - 'How secure is your personal data?': https://ico.org.uk/for-organisations/advice-for-small-organisations/information-security/data-security-advice/how-secure-is-your-personal-data/
- Data (Use and Access) Act 2025 guidance: https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/