SHERE PARISH COUNCIL

Shere Parish Council – Data Protection Policy

1. Introduction

1.1 Shere Parish Council holds and processes information about employees, councillors, residents, contractors, service users, and other data subjects for administrative, statutory, and operational purposes.

1.2 When handling such information, the Council and all those acting on its behalf must comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and any subsequent amendments or replacement legislation.

1.3 This policy is based on current law and will automatically adapt to any future legislative changes.

2. Data Protection Principles

In accordance with the UK GDPR, personal data must be:

1. Lawfulness, fairness and transparency – Processed lawfully, fairly, and in a transparent manner.
2. Purpose limitation – Collected for specified, explicit, and legitimate purposes and not further processed in ways incompatible with those purposes.
3. Data minimisation – Adequate, relevant, and limited to what is necessary.
4. Accuracy – Accurate and, where necessary, kept up to date. Inaccurate personal data will be rectified or erased without delay.
5. Storage limitation – Kept in a form that permits identification for no longer than is necessary, unless required for archiving, research, or statistical purposes under appropriate safeguards.
6. Integrity and confidentiality – Processed securely to protect against unauthorised access, loss, destruction, or damage.
7. Accountability – The Council must be able to demonstrate compliance with these principles.

3. Roles and Responsibilities

3.1 Data Controller: Shere Parish Council is the Data Controller and is responsible for ensuring compliance with data protection law.

3.2 Data Protection Officer (DPO):
The appointed DPO is Ciaran Ward.
Contact: **Ciaran Ward**
Head of Information Governance
Guildford Borough Council

Direct Line: 01483 444072
Ciaran.Ward@guildford.gov.uk or contact clerk@shereparishcouncil.gov.uk for more information

The DPO is responsible for:

- Observing conditions for the fair collection and lawful use of information.
- Specifying the purposes for which data is used.
- Ensuring personal data collected is relevant and not excessive.
- Maintaining data accuracy and quality.
- Applying strict checks to determine retention periods.
- Enabling individuals to exercise their rights under the law.
- Implementing appropriate technical and organisational security measures.
- Preventing transfers outside the UK without lawful safeguards.
- Ensuring councillors, staff, and volunteers handling personal data:
  - Understand their legal responsibilities.
  - Receive regular training and supervision.

3.3 All councillors, employees, and volunteers are responsible for compliance with this policy.

4. Storage, Security, and Retention

4.1 Personal data is held in secure paper-based systems and/or on password-protected electronic systems/cloud storage with regular security updates.

4.2 Access to personal data is restricted to those who require it for their role.

4.3 Retention periods are set out in the Council's Document Retention Scheme, available on request. Key examples:

4.4 At the end of the retention period, data will be securely destroyed (shredded, securely wiped, or otherwise made irrecoverable).

5. Rights of Data Subjects

5.1 Individuals have the right to:

- Ask what personal data the Council holds about them.
- Request access to a copy of their data (Subject Access Request).
- Know why and how their data is used, and with whom it is shared.
- Request correction of inaccurate or incomplete data.
- Request deletion of their data where it is no longer required for lawful purposes.
- Restrict or object to processing in certain circumstances.
- Request data portability (where applicable).

5.2 Requests will be responded to without undue delay and within one month of receipt. This period may be extended by up to two months for complex or multiple requests, with notification to the requester.

5.3 The Council may require proof of identity before releasing data.

6. Data Breach Procedure

6.1 A personal data breach is any incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

6.2 All breaches must be reported immediately to the DPO.

6.3 The DPO will assess the risk and, if required, report to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach.

6.4 Where the breach is likely to result in a high risk to individuals, those affected will be informed without undue delay.

7. International Data Transfers

7.1 Personal data will not be transferred outside the UK unless:
- The destination country is covered by a UK "adequacy decision"; or
- Appropriate safeguards are in place, such as Standard Contractual Clauses; and
- Individuals' rights are protected and enforceable.

8. Privacy by Design and Default

8.1 The Council will ensure that data protection principles are considered in the design of new systems, processes, and projects, and that only the minimum necessary personal data is collected and processed.

9. Data Sharing

9.1 The Council will only share personal data with third parties where necessary and lawful, and subject to a written Data Sharing Agreement or contractual clause ensuring compliance with UK GDPR.

10. Training and Awareness

10.1 All councillors, employees, and relevant volunteers will receive data protection training at induction and annual refresher training thereafter.

11. Complaints

11.1 Complaints about how personal data has been handled should be made to the Clerk in the first instance.

11.2 If unresolved, complaints can be escalated to the Information Commissioner's Office:
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.
Tel: 0303 123 1113 | Website: www.ico.org.uk

12. Policy Review

This policy will be reviewed annually or sooner if required by changes in law, best practice, or operational needs.

Adopted: 2nd September 2025
Next Review: September 2026 or earlier if required by law or operational changes