Data Protection Road Map Policy

Adopted 3rd March 2026 Minute 247.25

1. Introduction

Tisbury Parish Council ("the Council") is committed to ensuring the protection of personal data in accordance with the requirements of the UK General Data Protection Regulation and the Data Protection Act 2018 and the Data (Use & Access) Act 2025.

The Council recognises its responsibilities as a Data Controller and acknowledges the regulatory oversight of the Information Commissioner's Office (ICO). This Road Map Policy sets out the structured programme by which the Council will achieve, demonstrate, and maintain compliance with data protection legislation and meet its compliance with the new Assertion 10 requirements set out the Council's Annual Governance & Accountability Return.

2. Scope

This policy applies to:

- All councillors.
- The Clerk and any employees.
- Contractors and volunteers acting on behalf of the Council.
- All personal data processed by the Council in paper or electronic form.

3. Objectives

The Council aims to:

- Process personal data lawfully, fairly, and transparently.
- Ensure data is collected for specified, explicit, and legitimate purposes.
- Limit data to what is necessary.
- Keep data accurate and up to date.
- Retain data only as long as necessary.
- Protect data through appropriate security measures.
- Demonstrate accountability.

4. Governance and Responsibilities

4.1 Data Controller

Tisbury Parish Council is the Data Controller for all personal data processed in carrying out its statutory functions. It is not required to appoint a statutory Data Protection Officer because Parish and Town Councils are not considered "public authorities" for that specific GDPR requirement.

4.2 Data Protection Lead

The Clerk to the Council acts as the Council's Data Protection Lead and shall:

- Maintain the Record of Processing Activities (ROPA).
- Act as primary contact for the ICO, including maintaining the Council's registration.
- Monitor compliance.
- Report data protection matters to the Council.

5. Implementation Roadmap

Phase 1 – Data Audit and Mapping

The Council shall maintain its Record of Processing Activities (ROPA) by:

- Identifying all categories of personal data held.
- Identifying processing activities.
- Establishing the lawful basis for each processing activity.

- Recording storage locations (paper, devices, cloud services and third parties).
- Identifying access control arrangements.
- Identifying data shared with third parties.

Phase 2 – Risk Management

Data storage and processing risks shall be incorporated into the Council's Risk Register and reviewed annually.

Risks may include:

- Email misdirection
- Loss or theft of devices
- Inadequate access controls
- Cybersecurity threats

Mitigation measures shall be documented, implemented and monitored.

Phase 3 – Policy Framework

The Council shall maintain and review the following policies:

- General Data Protection Policy
- Privacy Notice(s)
- IT and Email Policy
- Publication Scheme

All policies shall be formally adopted by resolution and reviewed annually.

Phase 4 – Training and Awareness

The Council shall:

- Provide annual data protection and processing training for councillors and staff.
- Deliver induction training for new councillors.
- Maintain training records.
- Promote awareness of breach reporting responsibilities.

Phase 4 – Data Processors

Where the Council engages third-party processors (e.g. payroll providers, IT support, website hosting providers), it shall ensure:

- A written contract is in place.
- Data processing clauses comply with UK GDPR.
- Systems backups are undertaken.
- Adequate security measures are confirmed.
- Breach notification requirements are specified.
- Data return or deletion is provided for at contract end.

6. Monitoring and Review

This Roadmap Policy shall be:

- Reviewed annually by the full Council.
- Updated following legislative change.
- Amended following any significant data breach.
- Formally re-adopted following review.
- Withdrawn when the actions within it have been delivered.