DATA PROTECTION & INFORMATION SECURITY POLICY

Date Adopted/Revised	Minute Ref	Review Cycle
15/04/26	25/220	Annually

1. Purpose

This policy sets out how Acton Bridge Parish Council ("the Council") complies with the Data Protection Act 2018, UK General Data Protection Regulation (UK GDPR), and related legislation.

It establishes principles and controls for the secure handling of personal data and Council information.

This policy should be read alongside:
- Freedom of Information Policy
- Document Retention Policy
- IT Policy
- Risk Management Strategy
- Code of Conduct

2. Scope

This policy applies to:
- All Councillors
- The Clerk and Responsible Financial Officer (RFO)
- Employees and contractors
- Any third party processing personal data on behalf of the Council

It covers:
- Paper records
- Electronic records
- Emails
- Portable devices
- Cloud systems
- Audio/visual recordings

3. Data Protection Principles

The Council processes personal data in accordance with UK GDPR principles. Personal data shall be:

1. Processed lawfully, fairly and transparently
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary
4. Accurate and kept up to date
5. Kept no longer than necessary
6. Processed securely
7. Accountable and demonstrable in compliance

4. Lawful Bases for Processing

The Council processes personal data primarily under:

- Public task (exercise of official authority)
- Legal obligation
- Contract
- Legitimate interests (where appropriate)
- Consent (where required)

Special category data will only be processed where a lawful basis and condition under Article 9 UK GDPR applies.

5. Roles and Responsibilities

5.1 Council

The Council is the Data Controller.

5.2 Clerk / RFO

The Clerk acts as the Council's Data Protection Lead and is responsible for:

- Handling Subject Access Requests (SARs)
- Managing data breaches
- Maintaining compliance records
- Liaising with the ICO where required
- Ensuring retention schedules are followed

5.3 Councillors

Councillors must:

- Process personal data only for Council purposes
- Use Council-approved systems
- Not retain personal data on personal devices beyond what is strictly necessary
- Delete casework data once no longer required
- Immediately report any suspected data breach

6. Information Security

The Council will implement proportionate technical and organisational measures including:

- Secure password standards
- Multi-factor authentication (where available)
- Anti-virus and system updates
- Restricted access based on “need to know”
- Secure email usage
- Encryption where appropriate
- Secure disposal (cross-shredding / certified destruction)

Personal data must not be stored long-term on personal email accounts or personal cloud storage.

All information must be stored within approved Council systems in accordance with the Document Retention Policy.

7. Data Retention & Disposal

Retention periods are governed by the Council’s Document Retention Policy.

Personal data shall:

- Be reviewed periodically
- Not be retained longer than necessary
- Be securely deleted or destroyed when no longer required

8. Subject Access Requests (SARs)

Individuals have the right to access their personal data.

- Requests must be responded to within one calendar month of receipt.
- No fee will normally be charged.
- Fees may only be charged where requests are manifestly unfounded or excessive (as permitted under UK GDPR).

Identity verification may be required before disclosure.

All SARs must be referred immediately to the Clerk.

9. Freedom of Information Requests

FOI requests are handled under the Freedom of Information Policy.

Where requests involve personal data, the Council will apply relevant exemptions under the Freedom of Information Act 2000.

The statutory response timeframe is 20 working days.

10. Data Breaches

A personal data breach includes:

- Loss or theft of data
- Unauthorised access or disclosure
- Accidental deletion
- Cyber attack

All breaches or suspected breaches must be reported immediately to the Clerk.

The Clerk will:

1. Assess severity and risk
2. Record the incident
3. Notify the ICO within 72 hours where required
4. Notify affected individuals if high risk
5. Implement corrective measures

A breach log will be maintained.

11. Third-Party Processors

Where external providers process data on behalf of the Council:

- Written agreements must be in place
- Providers must implement appropriate security measures
- Compliance assurances may be requested

12. Risk Management

Data protection and information security risks form part of the Council's Risk Management Strategy.

The Council will:

- Review cyber and data risks annually
- Consider information risks when introducing new systems
- Review this policy annually

13. Training & Awareness

Councillors and staff will receive periodic awareness updates on:

- Data protection responsibilities
- Cyber security risks
- Secure handling of information

14. Monitoring & Review

This policy will be reviewed annually or sooner if:

- Legislation changes
- ICO guidance updates
- A significant breach occurs
- Systems or processes materially change

15. Consequences of Non-Compliance

Failure to comply with this policy may:

- Constitute a breach of the Code of Conduct
- Result in internal disciplinary action
- Require reporting to regulatory authorities