Beaudesert & Henley-in-Arden Joint Parish Council

Data Protection Policy

(Aligned with UK GDPR, the Data Protection Act 2018, NALC model guidance, and AGAR Assertion 10)

Adopted	02.03.26
Review Date Policy reviewed every 2 years or upon legislative change	Reviewed and amended 08.04.26
Version	1.1

1. Introduction

The Joint Parish Council (JPC) is committed to protecting the personal data it holds and processes. This policy sets out how the Council complies with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the principles of good information governance.

This policy also supports the Council's compliance with Assertion 10 of the Annual Governance & Accountability Return (AGAR), which requires the Council to act lawfully regarding personal data, protect it from unauthorised access, and ensure appropriate controls are in place.

Freedom of Information and Publication Scheme

The Council complies with the Freedom of Information Act 2000 and has adopted the ICO Model Publication Scheme. Information is proactively published in accordance with the Scheme, supporting the Council's obligations under AGAR Assertion 10.

Requests for information not routinely published will be handled under the Freedom of Information Act.

2. Scope

This policy applies to:

- All personal data processed by the Council
- All councillors
- The Clerk and any other employees
- Volunteers, contractors and anyone acting on behalf of the Council

It covers all formats, including electronic files, emails, paper records, photographs, CCTV (if applicable), and data held on personal devices used for council business.

3. Data Protection Principles

The Council will ensure that personal data is:

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 only for as long as necessary
6. Processed securely, protecting it against unauthorised or unlawful access, loss or damage

These principles underpin the Council's approach to data protection and are embedded in its procedures.

4. Lawful Bases for Processing

The Council will only process personal data where a lawful basis exists, including:

- Legal obligation (e.g., financial records, governance documents)
- Public task (e.g., responding to residents, managing council services)
- Contract (e.g., employment contracts)
- Consent (e.g., mailing lists, photographs)

- Legitimate interests (rarely used by councils but available where appropriate)

Special category data will only be processed where a lawful condition applies.

5. Roles and Responsibilities

The Council

- Acts as the Data Controller
- Ensures compliance with UK GDPR and this policy
- Reviews data protection arrangements annually (supporting AGAR Assertion 10)

The Clerk

- Acts as the Council's Data Protection Lead
- Manages day-to-day data protection compliance
- Maintains records, retention schedules and security measures
- Ensures councillors follow this policy

Councillors

- Must handle personal data responsibly and securely
- Must use council-provided or council-approved systems for data
- Must not store personal data unnecessarily or share it inappropriately

6. Data Security

The Council will ensure that personal data is protected through:

- Password-protected devices and accounts
- Secure email practices
- Locked storage for paper records
- Controlled access to data
- Regular backups of electronic data
- Use of .gov.uk or council-approved email accounts
- Avoidance of personal devices unless authorised and secured

These measures support AGAR Assertion 10 by ensuring data is “protected from unauthorised access”.

7. Data Retention and Disposal

The Council will retain personal data only for as long as necessary, following:

- NALC’s Local Council Document Retention Guidelines
- Legal requirements (e.g., financial records for 6 years)
- Operational needs

Data will be securely destroyed when no longer required.

8. Rights of Individuals

The Council will uphold the rights of individuals under UK GDPR, including:

- Right to be informed
- Right of access (Subject Access Requests)
- Right to rectification
- Right to erasure (where applicable)
- Right to restrict processing
- Right to data portability (rarely relevant to councils)
- Right to object

Requests will be handled within statutory timescales.

9. Freedom of Information Requests

The Council will respond to Freedom of Information (FOI) requests in accordance with the Freedom of Information Act 2000. FOI requests will be acknowledged and responded to within statutory timescales. Exemptions will be applied where appropriate, and applicants will be informed of their rights to review or appeal.

This supports the Council’s obligations under AGAR Assertion 10.

10. Data Breaches

A data breach includes loss, unauthorised access, accidental disclosure or destruction of personal data.

The Council will:

- Record all breaches
- Assess the risk to individuals
- Report serious breaches to the ICO within 72 hours
- Notify affected individuals where required
- Review procedures to prevent recurrence

This process directly supports AGAR Assertion 10.

11. Sharing Data

The Council will only share personal data where:

- There is a lawful basis
- It is necessary for council functions
- The individual has given consent (where required)
- A data processing agreement is in place (for contractors)

The Council will never sell personal data.

12. Councillor Use of Personal Data

Councillors must:

- Use council-approved email accounts
- Store data securely
- Delete personal data when no longer needed
- Not use personal data for political or personal purposes

This ensures compliance with both UK GDPR and the Code of Conduct.

13. Privacy Notices

The Council will publish Privacy Notices explaining:

- What personal data it collects
- Why it is processed
- The lawful basis for processing

- Individuals' rights

Privacy Notices will be reviewed regularly and made available on the Council's website.

13. Training and Awareness

The Council will ensure that:

- The Clerk receives appropriate data protection training
- Councillors are briefed on their responsibilities
- Policies are reviewed regularly

13. Review

This policy will be reviewed every two years, or sooner if legislation or guidance changes.