

Alnwick Town Council

Policy Title: Data Protection Policy

Policy Type: Governance & Legal

Adopted: February 2026

Last Reviewed: 26th February 2026

Next Review Due: February 2027

Approved By: Finance & Policy Committee

Minute Reference: FP25/41

Policy Owner: Town Clerk

Related Policies: Freedom of Information Policy; Records Management Policy.

Code of Conduct for Members – Index of Contents		
Section	Topic	Page
1	Introduction & Purpose	2
2	Data Protection Principles	2
3	Lawful Basis and Consent	2
4	Roles and Responsibilities	3
5	Data Security	3
6	Processing Children’s Data	3
7	Third Party Processors	4
8	Data Audits	4
9	Training and Guidance	4
10	Privacy Notice	4
11	Data Breach Reporting	5
12	Data Protection Impact Assessment (DPIAs)	5
13	Data Retention and Disposal	5-6
14	Data Subject Rights	6
15	Monitoring and Review	6

1. Introduction and Purpose

This Data Protection Policy sets out how the Town Council (“the Council”) complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

The Council is committed to ensuring that personal data is handled lawfully, fairly, and transparently, and that individuals’ rights are protected.

This policy applies to all councillors, employees, volunteers, contractors, and anyone processing personal data on behalf of the Council.

Alnwick Town Council is registered with the Information Commissioner’s Office (ICO) as a Data Controller.

2. Data Protection Principles

2.1 In accordance with the UK GDPR, the Council shall ensure that all personal data is:

- a. **Processed lawfully, fairly and in a transparent manner**
- b. **Collected for specified, explicit and legitimate purposes** and not processed in ways incompatible with those purposes
- c. **Adequate, relevant and limited** to what is necessary
- d. **Accurate and kept up to date**, where necessary
- e. **Kept in a form which permits identification for no longer than necessary**
- f. **Processed securely**, protecting against unauthorised or unlawful processing, accidental loss, destruction, or damage
- g. **Accountability** — the Council is responsible for, and must be able to demonstrate, compliance with the above principles.

These principles apply to all stages of data handling.

3. Lawful Basis and Consent

3.1 Personal data must only be processed where a lawful basis exists under Article 6 of the UK GDPR.

3.2 Where consent is used as the lawful basis, the Council shall ensure that:

- Consent is freely given, specific, informed, and unambiguous
- Individuals can withdraw consent easily
- Records of consent are maintained

3.3 The Council will **not** rely on consent where an alternative lawful basis is more appropriate, particularly when exercising its official duties as a public authority. As a public authority, the Council recognises that consent is unlikely to be freely given and will only use consent where individuals have a genuine choice.

4. Roles and Responsibilities

4.1 Data Controller

Alnwick Town Council is the Data Controller and has overall responsibility for ensuring compliance with data protection law.

4.2 Data Protection Lead

The Council has determined that, due to its size and processing activities, it is not required to appoint a statutory Data Protection Officer. The Town Clerk acts as the Council's Data Protection Lead and contact point for data protection matters, including liaison with the Information Commissioner's Office.

4.3 All Staff and Members

All councillors, employees, and volunteers must:

- Handle personal data in accordance with this policy
- Complete required training
- Report data breaches immediately
- Follow internal procedures and retention guidance Failure to comply may result in disciplinary action or suspension of system access.

5. Data Security

5.1 The Town Clerk shall ensure that appropriate technical and organisational measures are in place to protect personal data. These measures include, but are not limited to:

- Access controls based on role and necessity
- Secure password and authentication requirements
- Encryption of data where appropriate
- Secure disposal of physical and electronic data
- Use of secure council email accounts for all official business
- Prohibition on storing personal data on personal devices unless authorised

5.2 All staff must follow security procedures and report any suspected weaknesses.

6. Processing Children's Data

6.1 Personal data relating to a child under the age of 13 will not be processed without verified parental or guardian consent.

6.2 Privacy notices for children will be written in clear and age-appropriate language.

6.3 The Council does not normally process children's personal data as part of its core functions

7. Third-Party Processors

7.1 The Council shall ensure that any third-party processing personal data on its behalf provides sufficient guarantees regarding security, confidentiality, and breach reporting.

7.2 These requirements shall be written into all contracts and reviewed periodically.

7.3 Where required by Article 28 UK GDPR, a formal written data processing agreement shall be in place with the third-party processor.

8. Data Audits

8.1 The Town Clerk shall ensure that a Data Audit / Record of Processing Activities (ROPA), proportionate to the Council's size and activities, is reviewed at least annually. The audit will provide an overview of:

- What data is held
- Where it is stored
- Why it is processed
- Who it is shared with
- Applicable retention periods

9. Training and Guidance

9.1 All councillors and employees will receive data protection training as part of induction and at regular intervals thereafter.

9.2 The Town Clerk shall maintain an up-to-date Data Protection Guidance Note for easy reference by staff and members.

10. Privacy Notices

10.1 The Town Clerk shall prepare and maintain Privacy Notices explaining how personal data is used by the Council.

10.2 Privacy Notices will:

- Be published on the Council's website
- Be provided at the point of collection where practical
- Explain why data is collected, how long it is kept, how it will be used, and details of any third-party sharing
- Be reviewed annually

10.3 Notices will be clear, concise, and compliant with ICO guidance.

11. Data Breach Reporting

11.1 A personal data breach is any breach of security resulting in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

11.2 The Town Clerk shall maintain breach reporting procedures and ensure staff know how to report concerns.

11.3 All breaches must be reported immediately to the Town Clerk.

11.4 The Town Clerk will determine, with reference to ICO guidance, whether the breach must be reported to the ICO within 72 hours and whether affected individuals must be notified.

11.5 Where a breach is likely to result in a high risk to individuals' rights and freedoms, affected individuals will be informed without undue delay.

11.6 All breaches, regardless of severity, will be logged.

12. Data Protection Impact Assessments (DPIAs)

12.1 DPIAs will be used to identify and minimise risks arising from data processing activities, especially where processing may result in high risk to individuals.

12.2 The Town Clerk shall maintain procedures for determining when a DPIA is required and ensure it is carried out before the processing begins.

13. Data Retention and Disposal

13.1 The Council will not retain personal data for longer than necessary.

13.2 The Council determines retention periods based on legal requirements, operational need, and accountability requirements.

13.3 Before disposal, the following questions must be considered:

- a. Is retention required to fulfil a statutory obligation?
- b. Is retention required for operational needs?
- c. Is retention required as evidence for disputes?
- d. Does the document have historical or archival value?

13.4 All personal data must be destroyed securely once retention periods expire.

13.5 Items of historic significance may be transferred to the County Archive at Woodhorn Museum, where appropriate.

13.6 Retention periods may be extended by statutory or regulatory requirements, litigation, audit, or other formal holds.

13.7 Retention periods are set out in the Council's Document Retention Policy.

14. Data Subject Rights

14.1 Individuals have the following rights under the UK GDPR:

- a. Right to access their information
- b. Right to rectification
- c. Right to erasure
- d. Right to restrict processing
- e. Right to object
- f. Right to data portability
- g. Right to withdraw consent (where used as a basis for processing)
- h. Right to lodge a complaint with the Information Commissioner's Office

14.2 Requests to exercise rights should be submitted to the Town Clerk and will be handled within statutory timescales.

14.3 Subject Access Requests will normally be responded to within one calendar month.

15. Monitoring and Review

15.1 This policy shall be reviewed periodically, and at least annually, taking into account:

- Operational experience
- Feedback from data subjects
- Changes in legislation or ICO guidance

15.2 Updated versions of this policy shall be approved by the Council.