DUNSTABLE TOWN COUNCIL

DATA PROTECTION POLICY

Introduction

This policy outlines how Dunstable Town Council complies with its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It applies to all councillors, employees, contractors, volunteers, and anyone else who processes personal data on behalf of the council.

Purpose and Scope

The purpose of this policy is to ensure that personal data is handled responsibly, securely, and in accordance with the law. It supports the council's commitment to transparency, accountability, and the protection of individual privacy rights.

This policy applies to all personal data processed by the council, whether held electronically or in paper form, and includes data relating to residents, staff, contractors, and service users.

Data Protection Principles

The council will ensure that personal data is:

- Processed lawfully, fairly, and transparently
- Collected for specified, explicit, and legitimate purposes
- Adequate, relevant, and limited to what is necessary
- Accurate and kept up to date
- Kept only for as long as necessary
- Processed securely to prevent unauthorised access, loss, or damage

Lawful Basis for Processing

The council will identify and document the lawful basis for processing personal data, which may include:

- Consent
- Contractual necessity
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

Date Adopted: 22 September 2025
Last Reviewed: -
Minute No: FGP 209/25

Rights of Data Subjects

Individuals have the following rights under UK GDPR:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision-making and profiling
- Requests to exercise these rights should be submitted in writing and will be responded to within one calendar month.

Data Security

The council will implement appropriate technical and organisational measures to protect personal data, including:

- Password protection for electronic files
- Secure storage for paper records
- Regular backups
- Restricted access to sensitive data
- Staff training on data protection

Data Breaches

Any data breach must be reported immediately to the Clerk or Data Protection Lead. The council will assess the breach and, if necessary, report it to the ICO within 72 hours. A personal data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Breaches can occur whether data is held electronically or in paper form.

Examples of Data Breaches Include:

- Loss or theft of devices containing personal data (e.g., laptops, USB drives, mobile phones)
- Sending personal data to the wrong recipient via email or post
- Unauthorised access to personal data by staff or third parties
- Accidental deletion of personal data without backup
- Failure to redact personal information in documents released to the public

- Hacking or malware attacks that compromise council systems
- Leaving paper records or screens displaying personal data unattended in public areas
- Incorrect disposal of confidential waste (e.g., not shredding paper documents)

Data Breach Response Procedures

In the event of a personal data breach, Dunstable Town Council will follow a structured response process to mitigate harm, comply with legal obligations, and prevent recurrence.

1. **Identification and Reporting**

   Any staff member, councillor, or contractor who becomes aware of a potential data breach must report it immediately to the Clerk or Data Protection Lead. Reports should include details of what happened, when, and what data may be affected.

2. **Containment and Recovery**

   The Clerk or Data Protection Lead will assess the breach and take steps to contain it, such as:

   - Isolating affected systems
   - Recovering lost data
   - Changing access credentials
   - Notifying IT support if technical intervention is needed

3. **Risk Assessment**

   The council will evaluate:

   - The type and sensitivity of the data involved
   - The number of individuals affected
   - Potential consequences for those individuals
   - Whether the data was encrypted or protected

4. **Notification**

   If the breach is likely to result in a risk to individuals' rights and freedoms, the council will:

   - Notify the Information Commissioner's Office (ICO) within 72 hours
   - Inform affected individuals without undue delay, providing clear guidance on steps they can take

5. **Documentation**

   All breaches will be recorded in the council's Data Breach Register, including:

- Date and time of breach
- Nature of the breach
- Individuals affected
- Actions taken
- Outcome and lessons learned

6. **Review and Prevention**

   The council will conduct a post-incident review to:

   - Identify root causes
   - Update policies and procedures
   - Provide additional staff training if necessary

Data Retention

Personal data will be retained only for as long as necessary and in accordance with the council's Document Retention Policy. Data no longer required will be securely deleted or shredded.

Data Sharing

Personal data will only be shared with third parties when there is a lawful basis to do so. The council will ensure that appropriate data sharing agreements are in place.

Training and Awareness

All staff and councillors will receive regular training on data protection responsibilities. Awareness will be maintained through updates and guidance.

Review and Updates

This policy will be reviewed annually or when significant changes occur in legislation or council operations.

Contact

For questions or concerns about this policy or data protection matters, please contact:

Data Protection Lead / Clerk: Paul Hodson
Paul.hodson@dunstable.gov.uk
01582 513000

Date Adopted: 22 September 2025
Last Reviewed: -
Minute No: FGP 209/25

Data Subject Access Requests (DSARs)

Under the UK GDPR, individuals have the right to access their personal data held by the council. This is known as a Data Subject Access Request (DSAR).

Making a Request:

- Requests must be made in writing (including email) and should include sufficient information to identify the individual and the data requested.
- Requests can be submitted to the Clerk or Data Protection Lead at the council's main office or via the council's official email address.

Verification:

- The council may request proof of identity before processing the request to ensure data is not disclosed to the wrong person.

Response Time:

- The council will respond to DSARs within one calendar month of receipt.
- This period may be extended by a further two months if the request is complex or numerous. The individual will be informed of any extension and the reasons for it.

Scope of Access:

Individuals are entitled to:

- Confirmation that their data is being processed
- Access to their personal data
- Other supplementary information (as outlined in Article 15 of the UK GDPR)

Exemptions:

Some data may be withheld if an exemption applies under the Data Protection Act 2018 (e.g., data relating to crime prevention or legal privilege).

Record Keeping:

The council will maintain a log of all DSARs received, including the date of receipt, the nature of the request, and the date of response.

Date Adopted: 22 September 2025
Last Reviewed: -
Minute No: FGP 209/25