Data Protection Policy

(Including Direction and Process)

Created: 2026
Review Date: 27.04.2026

Next review Date: April 2027

Introduction

Denbigh Town Council is committed to protecting the rights and freedoms of data subjects while ensuring the secure and lawful processing of their data in accordance with legal obligations. We hold personal data about elected members, employees, volunteers, clients, contractors, and other individuals for various purposes.

This policy outlines how we protect personal data and ensures compliance with relevant data protection regulations. In particular, all elected members, employees, and volunteers must consult the Data Protection Officer (DPO) before initiating any significant new data processing activity to ensure compliance measures are met. *(See attached Direction and Process for further details.)*

Scope

This policy applies to all elected members, employees, volunteers, consultants, and advisors. All individuals subject to this policy must be familiar with its terms and comply accordingly.

This policy supplements other adopted policies relating to Internet use, email use, and document retention. We may amend or supplement this policy, with any new versions circulated before adoption. Upon adoption of an updated version, previous versions must be deleted or destroyed.

Data Protection Principles

Denbigh Town Council adheres to the principles of data protection as outlined in the EU General Data Protection Regulation (GDPR). We strive to comply with these principles in all data processing activities. The principles are:

1. **Lawfulness, Fairness, and Transparency** – Data must be collected lawfully, fairly, and transparently, with clear information on how it will be used.
2. **Purpose Limitation** – Data must be collected for specific, explicit, and legitimate purposes.
3. **Data Minimisation** – Only data that is necessary for the intended purpose should be collected.
4. **Accuracy** – Data must be kept accurate and up to date.
5. **Storage Limitation** – Data should not be stored longer than necessary.
6. **Integrity and Confidentiality** – Data must be processed securely to protect against unauthorised access, loss, or damage.

Definitions

Purposes for Processing Personal Data

Personal data may be processed for the following purposes:

- Compliance with legal, regulatory, and contractual obligations
- Delivery of council services
- Operational functions, including recruitment, training, security vetting, payroll, and administration
- Investigating complaints and responding to inquiries
- Ensuring safe working practices and monitoring access to systems and facilities
- Managing employee, volunteer, and elected member conduct and disciplinary matters

Personal Data

Personal data refers to any information that identifies an individual, either directly or indirectly, including but not limited to:

- Name, contact details (phone, email, home address)
- Educational background, employment history, financial details
- Nationality, marital status, CV, and skills information

Special Categories of Personal Data

Special categories of personal data include:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Physical or mental health status
- Criminal offences or related proceedings
- Genetic and biometric data

Processing of special category data must be strictly controlled and in accordance with this policy.

Data Controller

The data controller is the entity that determines the purposes and means of processing personal data. In some cases, this is defined by law.

Data Processor

A data processor is an individual or organisation that processes personal data on behalf of the data controller.

Processing

Processing refers to any operation performed on personal data, including collection, recording, organisation, storage, retrieval, use, disclosure, erasure, or destruction.

Supervisory Authority

The **Information Commissioner's Office (ICO)** is the designated regulatory body responsible for overseeing data protection compliance.

Policy Review

This policy, along with its attached guidance, will be reviewed annually.

Date: 27.04.2026
Next Review Date: April 2027

To be reviewed Annually

Data Protection: Direction and Process

Fair and Lawful Processing

We must process personal data fairly and lawfully, ensuring compliance with individuals' rights under the First Principle. This means that personal data should not be processed unless a lawful basis is established.

If no lawful basis applies (as outlined below), processing the data would be unlawful. Data subjects have the right to request the deletion of any unlawfully processed data.

Data Controller

Denbigh Town Council is classified as a data controller and also processes data. We are required to maintain appropriate registration with the Information Commissioner's Office to lawfully control and process data.

If you have any concerns regarding data handling, please contact the Data Protection Officer (DPO) for guidance.

Lawful Basis for Processing Data

Before processing personal data, a lawful basis must be established. It is your responsibility to ensure that any data you manage has a documented and DPO-approved lawful basis.

At least one of the following conditions must be met when processing personal data:

1. **Consent** – The individual has given clear, explicit, and informed consent for their data to be processed for a specific purpose.
2. **Contract** – Processing is necessary to fulfil or prepare a contract with the individual.
3. **Legal Obligation** – Processing is required to comply with a legal obligation (excluding contractual obligations).
4. **Vital Interests** – Processing is necessary to protect someone's life or in a medical situation.

5. **Legitimate Interest** – Processing is required for the organization's legitimate interests, provided that these do not override the individual's rights and freedoms.

Determining the Appropriate Lawful Basis

When assessing the lawful basis for processing data, ensure that:

- The processing is necessary and directly supports the intended purpose.
- There is no reasonable alternative to achieving the same purpose.
- The processing benefits the organization without disproportionately affecting individuals.

Consider the following questions and document your answers:

- What is the purpose of processing the data?
- Can the objective be achieved in a different way?
- Is processing the data optional or mandatory?
- Who benefits from the processing?
- Would the data subject reasonably expect this processing?
- What impact does the processing have on the individual?
- Does the organization hold a position of power over the data subject?
- Is the individual considered vulnerable?
- Could the individual object to the processing?
- Can the processing be stopped upon request, and is there a mechanism for doing so?

Our commitment to the First Principle requires us to document this process and justify our decisions. Individuals must be informed of the lawful basis for processing their data, as well as its intended purpose, through a privacy notice. This applies whether the data was collected directly from the individual or from another source.

If you are responsible for assessing the lawful basis and implementing the privacy notice for a processing activity, ensure that the DPO reviews it.

Special Categories of Personal Data

What are Special Categories of Personal Data?

Previously referred to as “sensitive personal data,” this category includes information requiring additional protection due to the higher risk it poses to individuals' rights and freedoms. Examples include:

- Race
- Ethnic origin
- Political beliefs
- Religious beliefs
- Trade union membership
- Health information

In most cases, processing special categories of personal data requires explicit consent from the data subject unless legal obligations or exceptional circumstances apply (e.g., ensuring workplace health and safety). Consent must clearly specify the type of data being processed, the reason for processing, and any third parties involved.

The processing of special categories of personal data must always comply with legal requirements. If a lawful basis does not exist, processing must cease immediately.

Data Protection: Direction and Process

Responsibilities

Our Responsibilities

- Analysing and documenting the type of personal data we hold
- Ensuring procedures cover all individual rights
- Identifying the lawful basis for processing data
- Ensuring consent procedures comply with legal requirements
- Implementing and reviewing processes to detect, report, and investigate personal data breaches
- Secure data securely
- Assessing risks to individual rights and freedoms in the event of data compromise

Your Responsibilities

- Fully understand your data protection obligations
- Ensure data processing activities comply with our policy and are justified

- Avoid unlawful use of data
- Store data correctly and securely to prevent breaches
- Comply with this policy at all times
- Raise concerns, report breaches, errors, or anything suspicious promptly

Responsibilities of the Data Protection Officer

- Keeping the council informed about data protection responsibilities, risks, and issues
- Regularly reviewing data protection policies and procedures
- Reviewing data inventory
- Conducting internal audits to ensure GDPR compliance
- Addressing data protection inquiries from elected members, employees, volunteers, and councillors
- Checking and approving data processing agreements with third parties
- Supporting the completion of Privacy Impact Assessments
- Investigating and reporting data breaches

IT Security Responsibilities

- Ensuring all systems, services, software, and equipment meet security standards
- Regularly checking and scanning security hardware and software
- Researching third-party services, such as cloud storage solutions, before use

Accuracy and Relevance

We ensure that all processed personal data is accurate, adequate, relevant, and not excessive for its intended purpose. Data will not be used for unrelated purposes without consent or reasonable expectation.

Individuals may request corrections to inaccurate personal data. If a dispute arises regarding accuracy, record the concern and inform the DPO.

Data Security

Personal data must be protected from loss or misuse. Any third-party organization processing data on our behalf must have a contract that includes data security provisions.

Storing Data Securely

- Printed data must be stored securely and shredded when no longer needed per the Document Retention Policy
- Digital data must be password-protected with strong passwords, preferably managed via a password manager
- Portable storage devices (CDs, memory sticks, external drives) must be encrypted or password-protected and securely stored
- Cloud storage must be approved by the DPO
- Servers containing personal data must be located in secure areas and protected with security software
- Regular backups must follow council backup procedures
- Personal data should never be saved directly to mobile devices (laptops, tablets, smartphones)
- All reasonable technical measures must be implemented to secure data

Data Retention

Personal data must be retained only as long as necessary, based on the reason it was obtained. Retention periods must align with the council's data retention policy.

Transferring Data Internationally

Transferring personal data outside the EEA is restricted. Secure approval from the DPO before making any international data transfers.

Rights of Individuals

Individuals have rights concerning their data, which we must uphold:

1. **Right to be Informed**
    - Provide clear, concise, and accessible privacy notices
    - Maintain records to demonstrate compliance
2. **Right of Access**
    - Enable individuals to access their data and supplementary information
    - Allow individuals to verify the lawfulness of processing
3. **Right to Rectification**
    - Correct or amend inaccurate or incomplete personal data upon request

    - Act without delay, within one month (extendable to two months with DPO approval)

4. **Right to Erasure**
    - Delete or remove personal data upon request unless compelling reasons justify retention
5. **Right to Restrict Processing**
    - Comply with requests to restrict, block, or suppress data processing
    - Data may be stored but not further processed
6. **Right to Data Portability**
    - Provide individuals with their data in a commonly used, machine-readable format
    - Transfer data to another controller upon request
7. **Right to Object**
    - Respect objections to processing based on legitimate interests or public interest tasks
    - Respect objections to direct marketing and profiling
    - Respect objections to data processing for research and statistics
8. **Rights Related to Automated Decision-Making and Profiling**
    - Allow individuals to object to automated processing
    - Explain automated decisions and enable human intervention upon request

Privacy Notices

When to Provide a Privacy Notice

A privacy notice must be supplied:

- At the time of data collection if obtained directly from the individual
- Within one month if obtained from another source
- Before using the data for communication
- Before disclosing the data to another recipient

What to Include in a Privacy Notice

Privacy notices must be concise, transparent, and easily accessible. They should include:

- Identity and contact details of the data controller and DPO
- Purpose of processing and the lawful basis
- Legitimate interests of the controller or third party (if applicable)
- Right to withdraw consent (if applicable)
- Categories of personal data (if not obtained directly from the subject)
- Recipients or categories of recipients of the data
- Details of any international data transfers and safeguards in place
- Retention period or criteria for determining retention
- Right to lodge a complaint with the ICO
- Source of personal data (if not obtained directly from the subject)
- Existence of automated decision-making or profiling, including logic and potential consequences
- Any legal or contractual obligations to provide data and possible consequences for failure to do so

This updated document ensures comprehensive coverage of responsibilities and compliance measures while maintaining clarity and conciseness.

Subject Access Requests

What is a Subject Access Request? Individuals have the right to:

- Confirm whether their data is being processed.
- Access their personal data and supplementary information (as outlined in a privacy notice).

Handling Subject Access Requests

- Requests must be fulfilled free of charge within one month.
- Where possible, data should be provided in a commonly used electronic format or through a secure remote system.
- If the request is complex or numerous, the deadline may be extended by two months with DPO approval. The individual must be informed of the extension within one month.

- Requests may be refused if manifestly unfounded or excessive. In such cases, a fee may be charged with DPO approval.
- If a large volume of data is requested, individuals may be asked to specify the required information.
- Once a request is received, no data should be altered or deleted. Doing so is a criminal offence.

Right to Erasure

What is the Right to Erasure? Individuals can request their data be erased when:

- The data is no longer necessary for its original purpose.
- Consent is withdrawn.
- The individual objects to processing with no overriding legitimate interest.
- The data was unlawfully processed or breached data protection laws.
- Compliance with a legal obligation is required.
- The data relates to a child.

Processing Right to Erasure Requests

Requests may only be refused when:

- Required to exercise freedom of expression and information.
- Necessary to comply with legal obligations, public interest tasks, or contractual obligations.
- Needed for public health or research purposes.
- Required for legal claims.
- If personal data has been shared with third parties, they must be notified of the erasure request.

Right to Object Individuals can object to data processing based on their specific circumstances. Processing must stop unless:

- There are overriding legitimate grounds for processing.
- The processing is necessary for legal claims.

Individuals must be informed of their right to object in the privacy notice and given an online means to exercise this right.

Right to Data Portability

- Data must be provided in a structured, commonly used, and machine-readable format.
- Data should be sent to the individual or a specified data controller, free of charge, within one month.
- If complex, the deadline may be extended by two months with DPO approval.

Third-Party Data Processors

Using Third-Party Controllers and Processors

- Written contracts must be in place with all third-party processors, outlining responsibilities and obligations.
- Processors must provide GDPR-compliant guarantees.
- Processors must act only on documented instructions and protect data subjects' rights.

Contracts with Data Processors Contracts must include:

- Processing only under written instructions.
- Confidentiality obligations for those handling data.
- Security measures for data protection.
- Sub-processors only with prior approval.
- Support for subject access requests and GDPR compliance.
- Secure deletion or return of data at contract end.
- Audit and compliance obligations.

Criminal Offence Data Criminal record checks must be justified by law and cannot be conducted based solely on consent. Such data must be handled as a special category of personal data.

Audits, Monitoring, and Training

Data Audits Regular audits will assess data management risks and inform the data inventory. Audits must be documented and shared with the DPO.

Monitoring The DPO will conduct periodic internal audits to ensure compliance. Any breaches must be reported to the DPO immediately.

Training

- Elected members and employees must complete data protection training relevant to their role.

- If role changes occur, additional training must be requested.
- The DPO is available for data protection inquiries.

Reporting Breaches

- Any breach must be reported immediately.
- The organisation must report data breaches to the ICO within 72 hours.
- Elected members and employees must report suspected breaches to facilitate investigation and compliance.
- Failure to report a breach may result in disciplinary action.

Failure to Comply Non-compliance with this policy can lead to disciplinary action. Protecting data is a shared responsibility, and failure to adhere to this policy may put individuals and the organisation at risk.