Three Rivers District Council

Data Protection Policy

2025 - 2028

THREE RIVERS DISTRICT COUNCIL

Contents

1. Introduction 2
2. Scope 2
3. Definitions 2
4. Data Protection Principles 2
5. Lawful Basis for Processing 3
6. Rights of Data Subjects 3
7. Data Collection 4
8. Data Processing 4
9. Data Security 5
10. Data Retention 6
11. Data Disposal 6
12. Data Breach Management 7
13. Data Sharing and Transfers 7
14. Data Protection Impact Assessments 8
15. Training and Awareness 8
16. Monitoring and Audit 9
17. Record Keeping 9
18. Responsibilities 9
19. Complaints 10
20. Policy Review 10

1. Introduction

Three Rivers District Council (the Council) is committed to protecting the privacy and security of personal data. This Data Protection Policy outlines how the Council collects, uses, stores, and protects personal data in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) (together referred to as the 'Data Protection Legislation').

2. Scope

This policy applies to all employees, contractors, agents, volunteers, and other individuals who handle personal data on behalf of the Council. It covers all personal data the Council processes, regardless of the medium in which it is held or whether it relates to past or present employees, contractors, agents, volunteers, or any other Data Subject.

3. Definitions

Data Breach: Any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. An accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data is a Data Breach.

Data Controller: The entity that determines the purposes and means of processing personal data.

Data Processor: The entity that processes personal data on behalf of the Data Controller.

Data Subject: A living identified or identifiable individual whose personal data is being processed by the Council.

Joint Controller: If two or more Data Controllers jointly determine the purpose and means of Processing the same personal data, they are joint controllers.

Personal data: Any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access, including Special Category Data.

Processing or Processes: Any operation or set of operations performed on personal data, whether or not by automated means.

Special Category Data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, or data concerning a natural person's sex life or sexual orientation.

4. Data Protection Principles

The Council adheres to the following principles when Processing personal data: Lawfulness, Fairness, and Transparency: personal data must be Processed lawfully, fairly, and in a transparent manner.

Purpose Limitation: personal data must be collected for specified, explicit, and legitimate purposes and not further Processed in a manner incompatible with those purposes.

Data Minimisation: personal data must be adequate, relevant, and limited to what is

necessary for the purposes for which it is Processed.

Accuracy: personal data must be accurate and, where necessary, kept up to date.
Storage Limitation: personal data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data is Processed.

Integrity and Confidentiality: personal data must be Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful Processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

Accountability: An overarching principle that the Council is responsible for and must be able to demonstrate compliance with these principles.

5. Lawful Basis for Processing

The Council will only Process personal data where there is a lawful basis for doing so. The lawful bases include:

- The Data Subject has given their consent.
- The Processing is necessary for the performance of a contract with the Data Subject.
- To meet our legal compliance obligations.
- To protect the Data Subject's vital interests.
- Performance of a task carried out in the public interest or in the exercise of official authority
- Legitimate interests allow the Council or a third party to Process personal data for purposes deemed necessary, provided they do not override the Data Subject's rights or freedoms.
- For Special Category Data, legitimate interests alone are not enough. Additional legal conditions, such as explicit consent or public interest, must be met.
- Processing of Special Category Data or criminal conviction data also requires extra safeguards to ensure the protection of Data Subject's rights.

6. Rights of Data Subjects

Data Subjects have the following rights regarding how TRDC handles their personal data:

Right to be informed: Data Subjects have the right to be informed about the collection and use of their personal data the Council holds. This will usually be in electronic form if the Data Subject has made the request electronically, unless they agree otherwise.

Right of access: Data Subjects have the right to access their personal data the Council holds and obtain information about how it is Processed, including through a Subject Access Request (SAR), which allows Data Subjects to request a copy of their personal data held by the Council.

Right to rectification: Data Subjects have the right to have inaccurate personal data corrected or completed if it is incomplete. Where the Council has disclosed the personal data to a third party it must also inform that third party of the right to rectification where possible.

Right to erasure: Data Subjects have the right to have their personal data erased in certain circumstances.

Right to restrict Processing: Data Subjects have the right to request the restriction or suppression of their personal data in certain circumstances.

Right to data portability: Data Subjects have the right to obtain and reuse their personal data for their own purposes across different services.

Right to object: Data Subjects have the right to object to the Processing of their personal data in certain circumstances.

Rights in relation to automated decision-making and profiling: Data Subjects have the right not to be subject to a decision based solely on automated processing, including profiling and using algorithms, which produces legal effects or significantly affects them.

7. Data Collection

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes. The Council collects personal data for a variety of purposes.
Service delivery: To provide services to residents, businesses, and visitors.

Human resources management: To manage employment relationships, including recruitment, payroll, performance management, and employee development.

Financial transactions: To process payments, grants, and other financial activities.

Community engagement: To involve residents in Council decision-making and community activities.

Legal compliance: To fulfil legal obligations and exercise statutory functions.
Public health and safety: To protect the health, safety, and welfare of the public.

The Council collects various types of personal data, including:
Contact information: Name, address, telephone number, email address.

Demographic information: Age, gender, marital status.

Identification information: National Insurance number, passport number, driving licence number.

Employment information: Job title, employment history, qualifications, performance records.

Financial information: Bank account details, payment history, tax information.

Health information: Medical history, health status, disabilities.

Communication records: Correspondence, call recordings, emails.

Visual images: Photographs, CCTV footage.

Should the Council wish to use personal data for a new or different purpose from that for which it was obtained, the DPO will provide advice on how to do this in compliance with both the Data Protection Legislation and this policy.

8. Data Processing

The Council Processes personal data for the following activities:
Service provision: Managing and delivering Council services to residents and businesses.
Administrative tasks: Record-keeping, correspondence, report generation.

Decision-making: Assessing eligibility for services, benefits, and grants.

Communication: Informing residents about council activities, events, and services.

Compliance: Ensuring adherence to legal and regulatory requirements.

Monitoring and enforcement: Investigating complaints, conducting audits, enforcing regulations.

Research and analysis: Conducting surveys, evaluating programs, improving services.

Processing Special Category Data requires additional safeguards due to its sensitive nature. The Council will only Process Special Category Data when:
Explicit consent has been obtained from the Data Subject.

Processing is necessary for employment, social security, or social protection law.

Processing is necessary to protect the vital interests of the Data Subject or another person where the Data Subject is physically or legally incapable of giving consent.

Processing is allowed by a not-for-profit organisation with a political, philosophical, religious, or trade union purpose, as long as it pertains to members or former members and is not disclosed outside the organisation with the Data Subject's consent.

Processing relates to personal data which are manifestly made public by the Data Subject.

Processing is necessary for legal claims or whenever courts are acting in their judicial capacity.

Processing is necessary for reasons of substantial public interest, based on domestic law, proportionate to the aim, and with safeguards to protect the Data Subject's rights and interests.

Processing is necessary for preventive or occupational medicine, employee capacity assessment, medical diagnosis, healthcare provision, or management of health/social care services, based on domestic law or a contract with a health professional, and subject to relevant conditions and safeguards.

Processing is necessary for public health reasons.

Processing is necessary for archiving purposes in the public interest, scientific or historical research, or statistical purposes.

9. Data Security

The Council implements appropriate technical and organisational measures to protect personal data against unauthorised or unlawful Processing, access, loss, destruction, or damage. These measures include:
Access controls: Only authorised personnel have access to personal data.

Encryption: personal data is encrypted where necessary to protect its confidentiality.

Network security: Firewalls, intrusion detection systems, and other security measures are in place to protect the Council's network.

Physical security: personal data is stored in secure facilities with access controls.

Training and awareness: Employees receive regular training on data protection and security.

Incident response: Procedures are in place for responding to Data Breaches and security incidents.

The Council will follow all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction. The Council may only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

10. Data Retention

The Council maintains a Data Retention Policy that outlines the retention periods for different categories of personal data. The retention periods are based on:
Legal and regulatory requirements: Compliance with statutory obligations and guidelines.

Business needs: Operational requirements for service delivery and administration.

Contractual obligations: Terms and conditions of contracts and agreements.

Data Subject rights: Balancing the need for data retention with the rights and expectations of Data Subjects.

The Council will ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Council's Data Retention Policy.

11. Data Disposal

The Council ensures that personal data is disposed of securely to prevent unauthorised access, loss, or misuse. You will take all reasonable steps to destroy or erase from the Council's systems all personal data that we no longer require in accordance with the Council's applicable policies. Secure disposal methods include:
Shredding: Paper documents are shredded using cross-cut shredders to render them unreadable.

Incineration: Sensitive documents are incinerated in a controlled environment to ensure complete destruction.

Secure Deletion: Electronic records are securely deleted using software that overwrites data to prevent recovery.

Degaussing: Magnetic media, such as hard drives and tapes, are degaussed to erase data.

Physical Destruction: Storage devices, such as hard drives and USB drives, are physically destroyed to prevent data retrieval.

Special Category Data requires additional safeguards during disposal. The Council will:
Ensure Special Category Data is separated from other records during disposal.

Use higher security measures, such as incineration or physical destruction, for Special Category Data.

Maintain records of the disposal process, including the date, method, and personnel involved.

12. Data Breach Management

All employees, contractors, and third-party users must report any suspected Data Breach to the Data Protection Officer immediately.

A data breach is defined as; '*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data, transmitted, stored or otherwise processed*'.

In the event of a Data Breach, the Council will:

Contain and mitigate the Data Breach: Take immediate steps to contain the Data Breach and mitigate its impact.

Assess the risk: Evaluate the risks to Data Subjects and the severity of the Data Breach.

Notify the ICO: Notify the Information Commissioner's Office within 72 hours if the Data Breach poses a risk to Data Subjects' rights and freedoms.

Notify Data Subjects: Inform affected Data Subjects without undue delay if the Data Breach is likely to result in a high risk to their rights and freedoms.

Review and Improve: Investigate the cause of the Data Breach and implement measures to prevent recurrence.

13. Data Sharing and Transfers

The Council will only share personal data with third parties when a lawful basis from the legislation can justify that sharing, where it is necessary to achieve a clear purpose and, with that purpose in mind, it is fair and proportionate to do so.

The Council may share personal data with third parties, including:

- Government bodies and regulatory authorities
- Law enforcement agencies
- Service providers and contractors
- Partner organisations

Data sharing will be conducted in accordance with Data Protection Legislation and the Council's data sharing agreements, ensuring that appropriate safeguards are in place to protect the personal data.

Purpose: Data Sharing Agreements (DSAs) outline the terms under which personal data is shared between organisations, ensuring both parties understand the purpose of the data sharing, including the aims of the data sharing and the benefits it will bring.

Legal Compliance: DSAs must comply with Data Protection Legislation, specifying the lawful basis for data sharing and ensuring the rights and freedoms of Data Subjects are protected.

Transparency: We must provide privacy notices to Data Subjects explaining who their personal data will be shared with.

Roles and Responsibilities: The DSA clearly defines whether the parties involved are Data Controllers or Joint Controllers and outlines their respective responsibilities and obligations.

Security Measures: DSAs must include provisions on how the personal data will be

secured, specifying technical and organisational measures to prevent unauthorised access or Data Breaches.

Data retention and disposal: DSAs should define how long the shared personal data will be retained and outline the processes for securely disposing of personal data once it is no longer required.

Oversight by the DPO: All DSAs must be approved by the DPO, who maintains a register of these agreements and monitors compliance.

The Council uses Data Processors to process personal data on behalf of the Council. These could be service providers and contractors. When using Data Processors, the Council will ensure it complies with Data Protection Legislation:

Data Processing Agreement: Data processing agreements (or data protection clauses in contracts) must meet the requirements of Article 28 of the UK GDPR and set out specific requirements, including requirements to only process personal data on the instruction of the Council as the Data Controller.

Security Measures: Ensuring Data Processors provide sufficient guarantees of the appropriate technical and organisational measures they will put in place to protect personal data.

The Council will not transfer personal data outside the UK unless:
The destination country provides an adequate level of data protection as determined by the UK government.

Appropriate safeguards are in place, such as standard contractual clauses or binding corporate rules.

The transfer is necessary for the performance of a contract, with the Data Subject's consent, or for other specified reasons permitted by law.

Contractors of the Council will not transfer personal data outside of the UK, without prior agreement

14. Data Protection Impact Assessments
The Council will conduct Data Protection Impact Assessments (DPIAs) for Processing activities that are likely to result in a high risk to Data Subjects' rights and freedoms.
The DPIA process involves:
Identifying the need: Determining when a DPIA is required.

Describing the Processing: Outlining the nature, scope, context, and purposes of the Processing.

Assessing necessity and proportionality: Evaluating whether the Processing is necessary and proportionate to achieve its aims.

Identifying and assessing risks: Identifying potential risks to Data Subjects and assessing their likelihood and severity.

Mitigating risks: Identifying measures to mitigate identified risks.
Documenting and reviewing: Documenting the DPIA and reviewing it regularly.

15. Training and Awareness
The Council provides regular training and awareness programs to ensure that

employees understand their responsibilities under Data Protection Legislation and this policy. The e-learning the Council provide to all staff is mandatory and is recertified every two years. Training covers topics such as:

- Data protection principles
- Data Subject rights
- Data security
- Incident response
- Data sharing and transfers

16. Monitoring and Audit

The Council regularly monitors and audits its data protection practices to ensure compliance with this policy and relevant laws. This includes:

- Regular reviews of personal data Processing activities.
- Audits of personal data security measures.
- Monitoring of personal data access and usage.
- Compliance checks against data protection laws.

17. Record Keeping

The Council maintains comprehensive records of its Processing activities in the form of a record of processing activities, including details of:

- Purposes of Processing.
- Categories of Data Subjects and personal data.
- Recipients of personal data.
- Retention periods.
- Data protection impact assessments.
- Data sharing and data processing agreements.

18. Responsibilities

Data Protection Officer: The Council has appointed a Data Protection Officer (DPO) who is responsible for overseeing this policy and ensuring compliance with Data Protection Legislation. Please contact the DPO with any questions about the operation of this policy or Data Protection Legislation, or if you have any concerns this policy is not being, or has not been, followed.

Deputy Data Protection Officer: This Officer will support the Data Protection Officer in their role as well as colleagues across the Council with advice and practical guidance.

Employees: All Council employees, including agency staff, who handle or collect personal data are responsible for ensuring their own compliance with the Data Protection Legislation. Employees must ensure that personal data is securely stored and processed in accordance with Data Protection Legislation, this policy, and the Staff Code of Conduct.

Heads of Service, Managers, and Team Leaders: Are responsible for ensuring that Council staff, volunteers, and work experience students under their supervision comply with the Data Protection Legislation, this policy, and are provided with appropriate training and inductions.

Failure to comply with this policy by any employee may result in disciplinary action, up to and including dismissal, and could also lead to criminal prosecution under Data Protection Legislation, as well as potential civil liability for compensation claims.

Elected Members: All elected members who handle or collect personal data are individually responsible for ensuring compliance with Data Protection Legislation. Elected members must ensure that personal data is securely stored and processed in

accordance with the Data Protection Legislation, this policy, and the Members' Code of Conduct.

Failure to comply with this policy by any elected member may result in formal action and could lead to criminal prosecution under Data Protection Legislation, in addition to potential civil liability for compensation claims.

19. Complaints

Data Subjects who have concerns about the way the Council is handling their personal data can raise a complaint with the DPO or directly with the UK data protection regulator, the Information Commissioner's Office (ICO).
Complaints can be made via the Corporate Compliments or Complaints policy.

Complaints should be submitted for the attention of the DPO and will be acknowledged within five working days. The DPO will investigate the complaint and respond within 30 days.

If the complainant is not satisfied with the response, they may escalate the complaint to the ICO.

Contact Information for ICO:

Email: icocasework@ico.org.uk
Telephone: 0303 123 1113
Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF,
Website: https://ico.org.uk/

20. Policy Review

This policy will be formally reviewed every three years or when there are significant changes to data protection laws or the Council's processing activities.

THREE RIVERS
DISTRICT COUNCIL