Three Rivers District Council

Data Retention Policy

2025 - 2028

THREE RIVERS DISTRICT COUNCIL

1. Introduction

Three Rivers District Council is committed to managing and storing information in a manner that complies with legal requirements and supports our operational needs. The purpose of this Data Retention Policy and Scheme is to ensure that Three Rivers District Council retains necessary information for as long as it is required to fulfil our operational, legal, and regulatory requirements. This policy outlines the guidelines and principles for the retention, storage, and disposal of data and outlines how long we keep different types of records and the procedures for their safe disposal.

2. Scope

This policy applies to all data and records created, received, or maintained by Three Rivers District Council in both electronic and paper formats. It covers all departments and services provided by the Council. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as "data".

3. Objectives

Through this policy, and our data retention practices, we aim to meet the following objectives:

- Ensure compliance with relevant legal and regulatory requirements.
- Provide clear guidelines on data retention periods.
- Promote efficient and systematic control of records.
- Ensure that data is available when needed.
- Prevent premature destruction of data.
- Facilitate the safe and secure disposal of data.
- Safeguard sensitive or confidential information from unauthorised access or disclosure.
- Mitigate risks associated with data breaches, privacy violations, or non-compliance.
- Facilitate effective records management practices, including organisation, indexing, and retrieval.
- Support Council services in decision-making by ensuring access to historical data.
- Reduce storage costs and optimise resource utilisation by eliminating unnecessary or obsolete records.
- Demonstrate accountability and transparency in handling and disposing of sensitive information.
- Foster trust and confidence among stakeholders, including customers, partners, and regulatory agencies, by adhering to data retention best practices.
- Establish a framework for regular review and update of retention policies to align with legal requirements and business needs.
- Enhance overall data governance and compliance instilling standardised procedures and protocols for managing data throughout its lifecycle.

4. Principles

Through this policy, and our data retention practices, we will meet the following commitments:

Minimisation: Only data that is necessary for specific purposes will be collected.
Retention Periods: Data will be retained for as long as necessary to fulfil those purposes.

Security: Data will be stored securely during its retention period.

Disposal: Data will be disposed of securely and in accordance with legal requirements.

Transparency: Clear and accessible information will be provided to individuals

regarding the purposes for which their data is collected, retained, and disposed of.

Accountability: Responsibility for ensuring compliance with data retention policies and procedures will be clearly assigned and upheld throughout the organisation.

Accuracy: Efforts will be made to ensure that retained data is accurate, up-to-date, and relevant for the intended purposes.

Accessibility: Individuals will have the right to access and review their data retained by the organisation, as well as request corrections or deletions where necessary.

Data Integrity: Measures will be implemented to safeguard the integrity of retained data, including protection against unauthorised modification, corruption, or loss.

Lawfulness: Data will only be retained where permitted by law for legitimate purposes.

Proportionality: The extent and duration of data retention will be proportionate to the purposes for which the data was collected and the associated risks and benefits.

5. Responsibilities

Data Owners: Ensure data is retained and disposed of according to this policy.

IT Department: Implement and manage technical controls for data retention and disposal.

All Staff: Comply with this policy and any specific instructions from the Data Protection Officer (DPO), IT Department and Legal Department.

6. Data Retention Schedule

The following schedule provides some examples of retention periods for various types of data, which will be adhered to at both Council and service levels. This list of not exhaustive. These retention periods are based on relevant legislation or accepted best practices.

Type of Record	**Minimum Retention Period**	**Reference**
Administrative Data		
Correspondence (general)	6 years	Local Government Act 1972
Council Meeting Minutes and Agendas	Permanent	Local Government Act 1972
Councillor Declarations of Interest	2 years from the end of a Councillor's term	Localism Act 2011
Documents provided to the “Proper Officer”	Permanent	Local Government Act 1972
Public Consultation Records	3 years	Local Government Act 2000
Financial and Human Resources Data		
Accounts and Financial Statements	7 years	*Recognised best practise*
Grants and Funding	7 years from the conclusion of their use	Charity Commission guidelines
Invoices and Receipts	7 years	Value Added Tax Act 1994
Bank Statements	7 years	Financial Services and Markets Act 2000
Employee Records	6 years after	*Recognised best practise*

	employment ends	
Payroll Records	7 years	The Income Tax (Pay As You Earn) Regulations 2003
Legal and Regulatory Data		
Contracts and Agreements	6 years after termination	Limitation Act 1980
Election Records	6 years	Representation of the People Act 1983
Freedom of Information (FOI) Requests	6 years after the request is closed	*Recognised best practise*
Health and Safety Records	5 years	Health and Safety at Work Act 1974
Legal Cases and Disputes	6 years after case resolution	Limitation Act 1980
Risk Assessments	5 years	Management of Health and Safety Regulations 1999
Service-Specific Data		
Asset Management Records	Permanent	Local Government Act 1972
Climate Change	5 years	Climate Change Act 2008
Community Engagement Records	5 years	Local Government Act 2000
Council Tax Records	7 years	Local Government Finance Act 1988
Housing Applications and Records	6 years after last contact	Housing Act 1985
Planning Applications and Permissions	Permanent	Town and Country Planning Act 1990
Property Records	Permanent	Land Registration Act 2002
Licensing Records	6 years after expiration	Licensing Act 2003
IT and Technical Data		
System Logs	1 year	*Recognised best practise*
Backups	1 year	*Recognised best practise*
User Access Records	1 year	*Recognised best practise*

7. Data Storage

Electronic Records: Stored in safe and secure databases, cloud services, and file systems with appropriate access controls.

Paper Records: Stored in secure physical locations with controlled access.

8. Data Encryption:

Electronic records containing sensitive or confidential information will be encrypted both in transit and at rest to mitigate the risk of unauthorised access or data breaches.

9. Data Backup

Regular backups of electronic records will be performed to ensure data resilience and availability in the event of system failures, disasters, or cyber-attacks.
Backup data will be stored safely and securely, with appropriate encryption and access controls, to prevent unauthorised access or tampering.

10. Data Disposal

Electronic data will be deleted using secure erasure methods to ensure data cannot be recovered.

Paper Data will be shredded or otherwise destroyed to ensure data cannot be reconstructed.

11. Compliance and Monitoring
Periodic reviews of data retention practices will be conducted to assess the ongoing relevance, accuracy, and necessity of retained data, and to ensure compliance with changing legal or regulatory requirements.

Retained data that is no longer required for legitimate business purposes will be promptly identified and securely disposed of in accordance with the data retention policy.
Regular audits will be conducted to ensure compliance with this policy. These audits will involve reviewing data retention practices, assessing the adequacy of data security measures, and verifying that all staff members are adhering to this policy.

Any breaches of this policy must be reported to the DPO immediately. A breach can include, but is not limited to, unauthorised access, loss of data, or failure to comply with the data retention schedule.

Upon receiving a report of a breach, the DPO will initiate an investigation within 24 hours. The investigation will include:

- Assessing the nature and scope of the breach: This will involve determining what data was compromised, how the breach occurred, and the potential impact on affected individuals.
- Identifying responsible parties: Understanding who was involved in the breach and any underlying factors contributing to the incident.

Following the investigation, the DPO will recommend actions to remedy the breach, which may include:

- Immediate corrective actions: These could include measures such as restricting access to compromised data, securing data storage systems, or informing affected individuals if necessary.
- Review and update of policies and procedures: Depending on the investigation's findings, policies and procedures may need to be revised to prevent future breaches. This can include additional staff training or enhanced security protocols.

All remedial actions should be completed within a timeframe of 30 days from the conclusion of the investigation, unless otherwise specified by the DPO based on the severity and complexity of the breach.

If a breach poses a risk to the rights and freedoms of individuals, the DPO will report the breach to the relevant supervisory authority within 72 hours of the Council becoming aware of it, in accordance with applicable data protection laws. Additionally, if necessary, affected individuals will be informed without undue delay.

All breaches and remedial actions taken will be documented. This documentation will be maintained for a period of at least three years and will be available for review by regulatory authorities as needed.

12. Training and Awareness:
Regular training will be available to all staff members to ensure understanding of data retention policies, procedures, and their respective roles and responsibilities.
Training will also cover the importance of data protection, privacy, and security measures to mitigate risks associated with data retention and disposal.

13. Contact Information
For questions or more information about this policy, please contact the Data Protection Officer.

14. Monitoring and Review
This policy will be formally reviewed every three years or when there are significant changes in the law or Three Rivers District Council procedures.

THREE RIVERS
DISTRICT COUNCIL