Telford and Wrekin

CVS

Involving, Inspiring, Supporting

Data Retention Policy (GDPR)

1 April 2026

1. INTRODUCTION

This Data Retention Policy sets out how Telford & Wrekin CVS ("the Organisation") retains, manages, and disposes of personal data in compliance with:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Data (Use and Access) Act 2025 (DUAA)

Under the UK GDPR, personal data must be:

"kept in a form which permits identification of data subjects for no longer than is necessary."

This is known as the **storage limitation principle**.

This policy applies to all personal data processed by the Organisation, including special category data.

2. AIMS AND OBJECTIVES

The aims of this policy are to:

- Ensure personal data is not retained longer than necessary
- Define clear and justified retention periods
- Ensure secure disposal or anonymisation of personal data
- Support compliance with legal and regulatory obligations
- Demonstrate organisational accountability

3. SCOPE

This policy applies to:

- All employees, volunteers, trustees, and contractors
- All personal data processed by the Organisation
- All storage formats, including:
    - Electronic systems
    - Paper records
    - Third-party systems

4. DATA PROTECTION PRINCIPLES (RETENTION)

The Organisation adheres to the UK GDPR principles by ensuring personal data is:

- Processed lawfully, fairly, and transparently
- Collected for specified, explicit purposes
- Adequate, relevant, and limited
- Accurate and up to date
- Not retained longer than necessary

- Processed securely

All retention decisions are:

- Documented
- Justified
- Reviewed regularly

5. DATA SUBJECT RIGHTS

Individuals have the right to:

- Access their data (Subject Access Requests)
- Rectify inaccurate data
- Request erasure (“right to be forgotten”)
- Restrict or object to processing

The Organisation will respond to all requests in accordance with UK GDPR requirements.

6. LEGAL AND REGULATORY CONTEXT

This policy reflects current UK data protection legislation, including:

- UK GDPR
- Data Protection Act 2018
- Data (Use and Access) Act 2025

The Organisation recognises that:

- UK GDPR requirements remain in force following Brexit
- The Data (Use and Access) Act 2025 introduces updates to processing and compliance requirements
- ICO guidance is subject to ongoing review

The Organisation will update this policy as required to reflect legislative and regulatory changes.

7. RETENTION PRINCIPLES

7.1 General Rule

Personal data will only be retained:

- For as long as required to fulfil its purpose
- To meet legal, regulatory, or contractual obligations

7.2 Determining Retention Periods

Retention periods are determined based on:

- Legal obligations
- Business needs
- Contractual requirements
- Risk to individuals
- Data subject expectations
- Lawful basis for processing

Each retention category must include:

- Purpose of processing
- Retention period
- Justification
- Disposal method

8. RETENTION SCHEDULE

The Organisation maintains a Retention Schedule which:

- Lists all categories of personal data
- Defines retention periods
- Documents justification
- Specifies disposal outcomes

The schedule is:

- Reviewed annually
- Updated when processing changes
- Owned by a designated responsible person

9. DATA DISPOSAL

At the end of the retention period, personal data will be securely disposed of.

Electronic Data

- Secure deletion
- Removal from backups where feasible

Paper Records

- Cross-cut shredding
- Confidential waste disposal

Alternative Actions

- Anonymisation
- Secure archiving (where legally permitted)

10. ROLES AND RESPONSIBILITIES

10.1 Data Protection Officer (DPO)

The Organisation has appointed a **Data Protection Officer (DPO)** who is responsible for overseeing compliance with this Data Retention Policy and all applicable data protection legislation, including the UK GDPR, Data Protection Act 2018, and Data (Use and Access) Act 2025.

Current DPO: Jeni Kuczynska
Contact Email: jeni.kuczynska@tandwcvs.org.uk
Telephone: 01952 916081

The DPO is responsible for:

- Monitoring compliance with this policy and relevant legislation
- Maintaining and reviewing the retention schedule
- Providing advice on data retention and lawful processing
- Acting as the primary contact for data protection queries and requests
- Liaising with the Information Commissioner's Office (ICO) where required

The Organisation will ensure that DPO contact details are:

- Kept up to date
- Easily accessible to staff and data subjects
- Published in relevant privacy notices and communications

10.2 Managers

Managers are responsible for:

- Ensuring that personal data within their area is retained and disposed of in accordance with this policy
- Reviewing data holdings regularly
- Escalating any retention or compliance concerns to the DPO

10.3 Staff and Volunteers

All staff and volunteers must:

- Comply with this policy
- Only retain personal data where necessary
- Ensure secure handling and disposal of data
- Report any risks, breaches, or concerns promptly

11. ACCOUNTABILITY AND DOCUMENTATION

The Organisation demonstrates compliance by:

- Maintaining Records of Processing Activities (RoPA)
- Linking retention to lawful bases
- Documenting retention decisions
- Keeping deletion and audit records

12. REVIEW AND GOVERNANCE

This policy will be reviewed:

- Annually
- Following legislative or regulatory updates
- When new processing activities are introduced

The Organisation will ensure ongoing alignment with ICO guidance.

APPENDIX A: RETENTION SCEDULE

Data Type	Retention Period	Justification (Legal / Business Need)	Disposal Action
Job applications & interview records (unsuccessful)	6 months after decision	Employment tribunal limitation period; equality claims defence	Secure deletion or shredding
Personnel & training records	Employment duration + 6 years	Limitation Act 1980 (legal claims)	Secure deletion
Contracts of employment & variations	Employment duration + 6 years	Legal claims, contractual evidence	Secure deletion
Working time opt-out forms	2 years	Working Time Regulations 1998	Secure deletion
Working Time Regulations compliance records	2 years	Working Time Regulations 1998	Secure deletion
Annual leave records	6 years	Employment law compliance; audit trail	Secure deletion
Payroll records (unincorporated businesses)	5 years after 31 January following tax year	HMRC statutory requirements	Secure deletion
Payroll records (companies)	6 years from financial year-end	HMRC / Finance Act requirements	Secure deletion
PAYE records	Minimum 3 years (recommended 6 years)	HMRC Income Tax Regulations 2003	Secure deletion
Collective workforce agreements	Permanent	Ongoing legal and organisational reference	Secure archive (restricted access)
Board of Trustee meeting minutes	Permanent	Governance, legal, and historical record	Secure archive
Maternity records	3 years after tax year end	Statutory Maternity Pay Regulations	Secure deletion
Current bank details (staff/service users)	Duration of use only	Operational necessity; data minimisation principle	Immediate deletion when no longer needed
Employee loan/advance records	Employment + 6 years after repayment	Financial audit; legal claims	Secure deletion
Death benefit nomination forms	Employment + 6 years post-payment	Benefits administration; legal claims	Secure deletion
Accident, injury and RIDDOR reports	Minimum 3 years	RIDDOR 2013 legal requirement	Secure deletion or archive if required

Data Type	Retention Period	Justification (Legal / Business Need)	Disposal Action
Wage and hours records (NMW compliance)	3 years	National Minimum Wage legislation	Secure deletion
Consent records (data processing)	Duration of processing + 6 years	Evidence of consent; accountability requirement	Secure deletion
DBS checks and criminal record data	Retained only as necessary; normally deleted after decision	ICO guidance; safeguarding vs minimisation	Immediate deletion; retain decision record only
Immigration/right-to-work checks	2 years after employment ends	Immigration, Asylum and Nationality Act 2006	Secure deletion