



Telford and Wrekin

CVS

Involving, Inspiring, Supporting

Data Protection Policy (GDPR)

1 April 2026

1. Organisation Details

Organisation: Telford & Wrekin CVS

Data Protection Lead: Jeni Kuczynska, CEO

Contact Email: jeni.kuczynska@tandwcvcs.org.uk

Address: Suite 12 & 15 Hazledine House, Central Square, Telford Centre, Telford, Shropshire, TF3 4JL

2. Purpose

This policy explains how the organisation collects, uses, stores, and protects personal data. It ensures compliance with the UK GDPR and Data Protection Act 2018.

3. Scope

This policy applies to all personal data processed by the organisation, including data relating to employees, volunteers, service users, suppliers, and other individuals.

4. Responsibility

The Data Protection Lead is responsible for overseeing compliance. All staff, volunteers, and contractors must comply with this policy.

5. Key Definitions

- **Personal data:** Information that identifies a living individual.
- **Special category data:** Sensitive data such as health, ethnicity, religious beliefs, or political opinions.
- **Processing:** Any use of personal data (e.g., collecting, storing, sharing, deleting).

6. Data Protection Principles

The organisation follows UK GDPR principles:

- Personal data is processed lawfully, fairly, and transparently.
- Data is collected for specified, explicit, and legitimate purposes.
- Data is adequate, relevant, and limited to what is necessary.
- Data is accurate and kept up to date.
- Data is retained only as long as necessary (see separate retention policy).
- Data is processed securely.

7. Lawful Basis

Personal data is processed only where a lawful basis applies, including:

- Consent
- Contract

- Legal obligation
- Legitimate interests
- Vital interests
- Public task (where applicable)

Details of the lawful basis used for specific processing activities are set out in the organisation's privacy notices.

8. Special Category and Criminal Data

Where special category or criminal records data is processed, the organisation ensures:

- An appropriate lawful basis under UK GDPR Article 6; and
- An additional condition under Article 9 and / or Schedule 1 of the Data Protection Act 2018;
- Appropriate safeguards are in place to protect this data.

9. Individual Rights

Individuals have the right to:

- Access their personal data
- Rectify inaccurate data
- Request erasure (where applicable)
- Restrict processing
- Object to processing
- Data portability (where applicable)
- Lodge a complaint with the Information Commissioner's Office (ICO)

Individuals are encouraged to raise concerns with the organisation first using the contact details above.

10. Subject Access Requests (SARs)

- Requests must be responded to within one month.
- Identity verification may be required.
- Requests may be refused or charged where manifestly unfounded or excessive.

11. Data Storage and Retention

- Data is stored securely in electronic and / or paper formats.
- Retention periods are managed in line with the organisation's separate Data Retention Policy.
- Personal data is securely deleted when no longer required.

12. Data Security

The organisation implements appropriate technical and organisational measures, including:

- Access controls
- Password protection
- Encryption where appropriate
- Secure storage and disposal procedures

Third-party processors must:

- Act on written instructions
- Maintain confidentiality
- Implement appropriate security measures

13. Data Breaches

All data breaches must be reported immediately to the Data Protection Lead. Reportable breaches will be notified to the ICO within 72 hours where required.

14. International Transfers

Personal data may be transferred outside the UK/EEA only where appropriate safeguards are in place, such as adequacy regulations or approved contractual clauses.

15. Accountability and Governance

The organisation demonstrates compliance by:

- Maintaining records of processing activities (ROPA)
- Conducting Data Protection Impact Assessments (DPIAs) where required
- Implementing appropriate policies and procedures

16. Staff Responsibilities

Anyone handling personal data must:

- Only access data when authorised
- Use data only for legitimate purposes
- Keep data secure
- Not disclose data without authority
- Report breaches or concerns promptly

Failure to comply may result in disciplinary action.

17. Training

All staff and volunteers receive data protection training. Additional role-specific training is provided where necessary.

18. Confidentiality

Confidential information must be protected:

- Do not disclose without authorisation or legal requirement
- Keep all materials secure
- Return all data upon leaving the organisation

19. Review and Governance

Review Frequency: Annually or sooner where appropriate

Last Reviewed: April 2026