



Telford and Wrekin

CVS

Involving, Inspiring, Supporting

Employees Privacy Standard Notice (GDPR)

1 April 2026

1. Who We Are (Data Controller)

Telford & Wrekin CVS is the **Data Controller** responsible for your personal data.

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

Data Protection Contact: Jeni Kuczynska, CEO

Email: jeni.kuczynska@tandwcvcs.org.uk

We are responsible for deciding how and why your personal data is processed.

2. Purpose of This Notice

This notice explains:

- What personal data we collect
- How and why we use it
- Who we share it with
- How long we keep it
- Your legal rights

This applies to employees, workers, contractors, and applicants.

3. Categories of Personal Data We Collect

We may collect and process the following categories:

a) Personal Identification Data

- Name, address, date of birth, NI number
- Contact details (email, phone)

b) Employment Data

- Job role, salary, performance records
- Training and disciplinary records

c) Financial Data

- Bank details
- Payroll, tax, and pension information

d) IT and Usage Data

- Login records, system usage
- Emails and communications (where appropriate)

e) Special Category Data (Sensitive Data)

- Health and medical information

- Equality data (e.g. ethnicity, disability)

f) Criminal Offence Data (where relevant)

- DBS checks or background screening

All personal data is defined under UK GDPR as information identifying an individual directly or indirectly.

4. How We Collect Your Data

We collect data from:

- You directly (e.g. employment forms)
- Recruitment agencies or referees
- Payroll and pension providers
- Public sources (e.g. professional profiles, where appropriate)

We ensure any third-party data is collected lawfully.

5. Lawful Bases for Processing

We process your data under the following legal bases:

- **Contract:** To fulfil your employment contract
- **Legal obligation:** To comply with laws (e.g. HMRC, employment law)
- **Legitimate interests:** For efficient business operations (balanced against your rights)
- **Consent:** Where required (e.g. certain sensitive data or marketing)

Sensitive data is processed only where additional legal conditions apply.

6. How We Use Your Data

We use your data to:

- Manage employment and HR processes
- Pay salaries and administer benefits
- Ensure health, safety, and wellbeing
- Meet legal and regulatory obligations
- Monitor performance and training
- Maintain IT systems and security

We will only use your data for the purposes it was collected unless legally permitted otherwise.

7. Data Sharing

We may share your data with:

Internal:

- Managers and HR staff (where necessary)

External:

- Payroll and pension providers
- IT service providers
- Legal and professional advisers
- Regulators (e.g. HMRC, ICO)

We only share data where:

- There is a lawful basis
- The recipient needs the information
- Appropriate safeguards are in place

8. International Transfers

We may transfer data outside the UK/EEA only where:

- The country provides adequate protection, or
- Approved safeguards (e.g. standard contractual clauses) are used, or
- Explicit consent is obtained

9. Data Retention

We retain personal data in line with our retention policy. Typical periods include:

- Employment records: **6 years after employment ends**
- Payroll/tax records: **6 years (HMRC requirement)**
- Recruitment records (unsuccessful candidates): **6–12 months**

Data is securely deleted or anonymised when no longer required.

10. Data Security

We protect personal data using:

- Access controls and authentication
- Secure IT systems and encryption
- Staff training and policies
- Regular audits and monitoring

Employees must follow all security procedures.

11. Automated Decision-Making

We **do not** make decisions based solely on automated processing that significantly affect employees.

If this changes, you will be informed and given the right to challenge decisions.

12. Your Rights

Under UK GDPR, you have the right to:

- Access your personal data
- Correct inaccurate data
- Request deletion (where applicable)
- Restrict or object to processing
- Withdraw consent at any time
- Request data portability
- Object to direct marketing
- Be informed about data breaches affecting you

Requests should be submitted to the data protection contact.

13. Complaints

If you are unhappy with how we handle your data, you can contact us first.

You also have the right to complain to:

Information Commissioner's Office (ICO)

Website: <https://ico.org.uk>

14. Data Breaches

All data breaches or suspected data breaches must be reported **immediately**.

Employees must:

- Report the breach **without delay to a member of the Senior Management Team (SMT)**
- Also notify the designated data protection contact where applicable
- Preserve any evidence and **not attempt to investigate independently**

The organisation will:

- Assess and investigate the breach
- Notify the Information Commissioner's Office (ICO) where required
- Inform affected individuals where there is a high risk to their rights and freedoms

15. Mandatory Data & Consequences

Some personal data must be provided to:

- Enter into an employment contract
- Meet legal obligations

Failure to provide required data may:

- Prevent employment
- Affect payroll or benefits
- Lead to legal non-compliance

16. Accountability & Governance

We ensure compliance through:

- Staff training
- Data protection policies
- Record keeping of processing activities
- Data Protection Impact Assessments (DPIAs)
- Regular audits and reviews

17. Changes to This Notice

We may update this notice periodically. The latest version will always be available to staff.

18. Employee Responsibilities

All staff must:

- Follow data protection policies
- Only access data when necessary
- Report breaches or concerns immediately

Failure to comply may result in disciplinary action.