



Wealden Volunteering Data Protection Policy

Approved by the Board: July 2026

Next Review date: July 2028

Chair Signature:

A handwritten signature in blue ink, appearing to read 'Paul P. K.', is written on a light yellow rectangular background.

1. Purpose

Wealden Volunteering (WV) is committed to protecting the privacy and personal data of all individuals we engage with, including volunteers, beneficiaries, staff, trustees, and partners.

We recognise that individuals trust us to handle their information responsibly. This policy explains how we meet our legal obligations and ensure personal data is processed safely, lawfully, and transparently in line with the UK GDPR and Data Protection Act 2018.

2. Scope

This policy applies to:

- All staff, volunteers, trustees, contractors, and partners
- All personal data processed by WV in delivering its services

3. Legal Framework

This policy is based on:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018

WV will comply with the data protection principles, ensuring that personal data is:

- Processed lawfully, fairly and transparently
- Collected for specific, explicit purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date
- Retained only as long as necessary
- Processed securely
- Accountable and demonstrable

4. Key Definitions

- **Data Controller:** WV deciding how/why data is processed

Example: Managing volunteer records

- **Data Processor:** WV processing data on behalf of another organisation

Example: Delivering services under contract for a partner or funder

- **Personal data:** Information relating to an identifiable individual (“data subject”)
- **Special category data:** Sensitive data (e.g. health, disability, safeguarding-related information)

Wealden Volunteering acts as both a Data Controller and, in some cases, a Data Processor.

5. Roles and Responsibilities

Board of Trustees

- Overall accountability for data protection compliance
- Oversight of risk and governance

CEO (Data Protection Lead)

- Day-to-day responsibility for compliance
- Managing breaches, risks, and data subject rights
- Ensuring training and procedures are in place

WV is not required to appoint a formal Data Protection Officer but ensures appropriate oversight.

Staff and Volunteers

- Must follow this policy and complete training
- Must handle data securely and report concerns

6. Lawful Basis

WV identifies a lawful basis for all data processing activities, including:

- Consent – e.g. communications and marketing
- Contract – delivering volunteering services
- Legal obligation – safeguarding or reporting requirements

- Legitimate interests – managing services and relationships
- Vital interests – protecting life

A record of processing activities is maintained to demonstrate compliance.

7. Special Category Data

WV may process sensitive data (e.g. health, vulnerability, safeguarding-related information).

This will only occur where:

- Explicit consent is provided, or
- It is necessary for safeguarding, support, or legal obligations

Additional safeguards include:

- Restricted access
- Secure storage
- Limited sharing

8. Processing Personal Data

All staff and volunteers must:

- Only use data for authorised purposes
- Minimise the data they collect and use
- Ensure information is accurate
- Not share data without proper authority
- Use secure systems in line with IT policy

Personal data must never be used for personal purposes or stored improperly

8.1 Privacy Notices

WV provides clear privacy notices explaining:

- What data is collected
- Why it is collected
- How it is used
- How long it is retained
- Individuals' rights

Privacy notices are provided at point of data collection and reviewed regularly.

9. Data Sharing

WV will only share personal data where necessary:

- To deliver services
- To meet legal obligations
- For safeguarding purposes

Data protection will not prevent appropriate information sharing where there is a risk of harm, in line with safeguarding responsibilities.

All third parties must:

- Have a written agreement
- Process data only on WV instructions
- Maintain appropriate security
- Report breaches promptly

10. International Transfers

Personal data will not be transferred outside the UK unless appropriate safeguards are in place, such as:

- UK adequacy regulations
- Standard contractual clauses

11. Data Retention

Data is only kept as long as necessary.

Retention periods will be based on:

- Legal requirements
- Safeguarding considerations
- Operational need

Examples:

- Volunteer records – retained for defined periods after engagement
- Financial records – minimum 7 years

- Safeguarding records – retained in line with statutory guidance

Retention Schedule:

- Owned by CEO
- Reviewed annually
- Updated following changes to law or practice

12. Individual Rights

Individuals have the right to:

- Access their personal data
- Request correction of inaccurate data
- Request erasure (where applicable)
- Restrict processing
- Object to processing
- Data portability

All requests must be:

- Reported immediately to the CEO
- Responded to within one calendar month

WV will ensure requests are handled promptly and appropriately.

13. Data Breaches

A data breach includes loss, unauthorised access, or accidental disclosure of personal data.

All breaches must be reported immediately.

WV will:

- Assess risk to individuals
- Report serious breaches to the ICO within 72 hours
- Inform affected individuals where risk is high
- Record and review all breaches

Reporting Procedure:

- Must be reported immediately to CEO (Data Protection Lead)
- Report via email or phone as soon as identified
- Include details of what happened, data affected and individuals involved

WV will:

- Assess risk
- Contain and investigate breach
- Record incident
- Report to ICO within 72 hours if required
- Inform affected individuals where risk is high

14. Confidentiality

Personal data will be handled sensitively and securely.

However, confidentiality cannot be guaranteed:

- Where there are safeguarding concerns
- Where disclosure is required by law
- Where sharing is necessary to protect individuals

15. Privacy by Design

WV will consider data protection at the outset of all activities, services, and systems to:

- Minimise risks
- Ensure compliance
- Protect individuals' rights

16. Training and Awareness

All staff, volunteers, and trustees will:

- Receive data protection training
- Understand their responsibilities

- Know how to report incidents

17. Monitoring and Governance

WV will:

- Maintain records of data processing
- Monitor compliance
- Review risks regularly
- Report issues to the Board of Trustees

Serious incidents may be reported to the Information Commissioner's Office (ICO) and, where relevant, to the Charity Commission.

18. Review

This policy will be reviewed every two years or sooner if required due to:

- Changes in legislation
- Organisational learning
- Updates to safeguarding or IT policies