Fletton House
Fletton Way, Glapthorn Road
Oundle
Peterborough PE8 4JA
Tel: 01832 275433
E-mail: admin@volunteer-action.org.uk

Web Site: www.volunteer-action.org.uk

Data Protection Policy

Date this policy reviewed	**November 2025**
Next review	**November 2026**

Purpose

Volunteer Action (VA) needs to collect and process certain personal information about individuals in order to carry out its work effectively.

These individuals may include customers, suppliers, business contacts, employees, volunteers, and other people VA has a relationship with or may need to contact.

This Data Protection Policy sets out how personal data will be collected, handled, stored, and shared to comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

VA is also required to maintain information security policies to meet Safer Payments standards required by SquareUp Payments and data retention requirements as set by VA's selected insurers. This policy should be read in conjunction with VA's 'Acceptable Use of IT and Social Media Policy'.

This policy ensures that VA:

- Complies with data protection law and follows good practice
- Protects the rights of staff, volunteers, service users, customers, and partners
- Is transparent about how it stores and processes personal data
- Protects itself from the risks of a data breach or misuse of information

Scope

This policy applies to:

- The office of VA
- All staff, trustees, and volunteers
- Any third parties acting on behalf of VA

All staff and volunteers must read, understand, and comply with this policy and related procedures.

Information VA Collects

VA may collect, store, and use the following types of personal data:

- Names of individuals
- Postal addresses, email addresses, telephone numbers and age of individuals
- Information relating to individuals' mobility, health, and access needs
- Recruitment, payroll, and HR information
- Payment card details (processed securely but never stored)
- Information necessary to administer volunteering, employment, and core and additional services

How VA uses personal data

VA may use personal data to:

- Provide and manage core and additional services
- Administer volunteering and employment
- Process donations and claim Gift Aid
- Maintain contact records and communications
- Take and process payments securely
- Conduct surveys and evaluations

How VA collects information

VA may collect personal data in various ways, including:

- Directly from individuals (e.g. application forms, phone calls, or emails)
- From referral partners or agencies (with consent where appropriate)
- Through the website, donation forms, or membership documents

Lawful basis for processing

VA processes personal data under the following lawful bases:

- Legitimate Interests: Processing is necessary for the delivery of our services and organisational functions.
- Consent: Consent is obtained from all members of the core services to store data and recorded on the relevant data base system. In certain cases (e.g. marketing communications), we rely on explicit consent.
- Legal Obligation: For example, complying with HMRC requirements for Gift Aid or employment law.
- Contract: When processing is necessary for employment or volunteer agreements.

Data protection principles

VA adheres to the seven principles of data protection under the UK GDPR:

1. Lawfulness, fairness, and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

Staff and volunteer responsibilities

- Access to personal data is restricted to those who require it for their work/volunteering.
- Access rights are granted by the Chief Executive & Charity Manager (CE&CM) and withdrawn immediately upon leaving.
- Personal data must never be stored informally or written down unnecessarily (e.g. payment details must never be recorded on paper).
- Login details must never be shared.
- Requests for access to confidential information outside normal practice must be approved by the CE&CM.
- All staff and volunteers must sign a Confidentiality Agreement (Appendix 1).

Data storage and security

To ensure personal data is stored securely:

- Paper records are kept in locked cabinets and destroyed securely when no longer required.
- Electronic data is stored only on authorised drives and servers, protected by up-to-date antivirus software and firewalls.
- Removable media (e.g. USBs, CDs) must be securely stored and encrypted if used.
- Personal data must never be stored on personal or mobile devices unless authorised and securely deleted after use.
- Payment card details are never stored.
- We comply with the PCI DSS requirements, reviewed annually.
- Financial records are retained for 6 years.
- Service user information is archived and retained for up to 24 months after last use.
- Staff and volunteer records are retained as required by insurer safeguarding cover (up to 7 years).
- Exceptions may apply for ongoing complaints, legal claims, or HMRC requirements (e.g. Gift Aid – 6 years).
- Volunteer drivers must destroy personal information provided for journeys immediately after use.

Data accuracy

VA will take reasonable steps to ensure data is accurate and up to date.
Staff must verify details where possible and correct inaccuracies promptly.
Data should be kept in as few places as necessary to reduce duplication and risk.

Individual rights

Under UK GDPR, individuals have the right to:

- Access a copy of their personal information (Subject Access Request)
- Request correction of inaccurate data
- Request deletion of data where lawful
- Restrict or object to processing
- Withdraw consent (where applicable)
- Request data portability
- Not be subject to automated decision-making or profiling

Requests of the above nature should be directed to the CE&CM.
VA aims to respond within 14 days and does not normally charge a fee unless requests are excessive.
Identity verification will be required before releasing any data.

Data sharing and disclosure

VA will not share personal data with third parties unless:

- Required by law (e.g. HMRC, law enforcement)
- Necessary to deliver our services (e.g. volunteer coordination)
- Explicit consent has been obtained

Any disclosure to law enforcement agencies must be approved by the CE&CM and, where

necessary, the Board of Trustees and legal advisors.

Data breaches

Data breaches are managed in accordance with VA's Operational Risk Assessment, reviewed annually.

Any suspected data breach must be reported immediately to the CE&CM.

If a breach poses a risk to individuals' rights and freedoms, it will be reported to the ICO within 72 hours and to affected individuals as required.

Appendix 1: Confidentiality Agreement

- Volunteer Action needs to collect and process certain personal information about individuals in order to carry out its work effectively. These individuals may include customers, suppliers, business contacts, employees, volunteers, and other people the organisation has a relationship with or may need to contact.

- Between trustees, staff and volunteers, information about a client should only be disclosed to the extent that is necessary to enable individuals concerned to carry out their responsibilities to the client.

- Volunteer's information is confidential. By prior agreement with the volunteer, their mobile telephone number can be given to a beneficiary. We do not give out home addresses or telephone numbers of any of our trustees, staff or volunteers.

- Any known or suspected breach of information security or confidentiality must be reported to the Chief Executive immediately.

- Upon leaving Volunteer Action, all employees and volunteers must return or securely delete any personal information in their possession that relates to the organisation, its staff, volunteers, or beneficiaries.

- Signing this agreement confirms acceptance of and compliance with:

    1. The Acceptable Use of IT and Social Media Policy
    2. The Data Protection Policy

Name in Capitals_____

Signature_____ Date_____