

Data Protection Policy Template

(UK GDPR Compliant Template for VCSE sector)

1. Overview

[Name of Organisation] collects and uses personal information in order to carry out its work and deliver services. We are committed to handling personal data lawfully, fairly, and transparently, and to respecting the rights and privacy of individuals.

This policy explains how we meet our obligations under the UK GDPR and the Data Protection Act 2018.

2. Scope

This policy applies to everyone involved in [Name of Organisation], including trustees, staff, volunteers, sessional workers, students, and anyone acting on behalf of the organisation.

It covers all personal data processed in connection with our activities, whether held electronically or in paper form.

3. Roles and Responsibilities

Overall responsibility for data protection sits with the Board of Trustees, who ensure the organisation meets its legal obligations.

Day-to-day responsibility is delegated to a designated lead (for example, a Data Protection Lead, Manager, or Coordinator), who oversees compliance, supports good practice, and acts as the main point of contact for data protection matters.

This includes ensuring that personal data is handled appropriately, monitoring risks, supporting improvements in practice, and managing any data breaches where they arise.

All staff and volunteers are expected to follow this policy. Failure to do so may result in action being taken.

4. What is Personal Data?

Personal data is any information that can identify a living individual, either on its own or when combined with other information. This includes basic details such as names and contact information, as well as records relating to staff, volunteers, and service users.

Some types of information are classed as “special category data” and require additional protection. This includes information about health, ethnicity, religion or beliefs, sexual orientation, or criminal convictions.

5. Data Protection Principles

We follow the core principles of UK data protection law. This means personal data is used lawfully, fairly, and transparently, and is only collected for specific and legitimate purposes.

We ensure that data is limited to what is necessary, kept accurate and up to date where possible, stored securely, and retained only for as long as needed. We also ensure that individuals' rights are respected at all times.

6. Lawful Basis for Processing Data

We only process personal data where we have a valid lawful basis to do so. This may include consent, the delivery of a service or contract, a legal obligation, or legitimate interests where appropriate and balanced.

Where personal data is collected, we will explain clearly why it is being collected and how it will be used through appropriate privacy information. We will not use data for new purposes without first ensuring this is lawful.

7. Transparency and Consent

We are committed to being open and transparent about how personal data is used. Individuals will be informed about what data is collected, why it is needed, how it will be used, and who it may be shared with.

Where consent is required, it must be freely given, informed, and specific. Individuals can withdraw consent at any time. Where special category data is processed, additional safeguards and conditions will apply in line with the UK GDPR.

8. Data Security and Storage

We take appropriate measures to protect personal data from loss, misuse, or unauthorised access. This includes secure IT systems, password protection, restricted access, and secure storage of paper records.

When data is no longer required, it will be disposed of securely, for example through shredding or secure deletion.

9. Data Retention

We only keep personal data for as long as it is necessary for the purpose for which it was collected.

The organisation maintains a retention approach that ensures data is regularly reviewed and securely deleted or anonymised when no longer needed.

10. Sharing Information

We may share personal data with relevant organisations such as local authorities, funders, or partner agencies where necessary to deliver services or meet legal obligations.

We will only share the minimum amount of information required, ensure that sharing is lawful, and where appropriate, inform individuals about how their data may be shared.

In some circumstances, information may be shared without consent where there is a legal requirement or a safeguarding concern.

11. International Transfers

Personal data will not normally be transferred outside the UK. Where this is required, appropriate safeguards will be put in place in line with UK data protection requirements.

12. Individual Rights

Individuals have rights in relation to their personal data. These include the right to access their data, request corrections, request deletion in certain circumstances, object to or restrict processing, and request portability where applicable.

We will respond to valid requests within one calendar month, in line with legal requirements under the UK GDPR.

13. Subject Access Requests

Individuals may request access to the personal data we hold about them. Requests should be made in writing, including by email where appropriate.

We will take steps to verify identity before releasing any information and will provide responses free of charge in most cases. We will also make reasonable adjustments where needed to support access.

14. Data Breaches

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

Where a breach occurs, we will take immediate steps to assess and contain it, record it appropriately, and determine whether it must be reported to the Information Commissioner's Office within 72 hours, in line with legal requirements.

Where there is a high risk to individuals, we will also inform those affected without delay.

15. Training and Awareness

All staff and volunteers will receive appropriate training in data protection. This will be provided at induction and refreshed regularly, with additional support where needed depending on role and responsibilities.

16. Complaints and Contact

Any concerns about how personal data is handled should be raised with the organisation's designated data protection contact.

Individuals also have the right to complain to the Information Commissioner's Office if they are unhappy with how their data has been managed.

17. Review

This policy will be reviewed regularly to ensure it remains accurate, effective, and compliant with changes in legislation or organisational practice.

Adoption and Review

Adopted by: [Board of Trustees / Management Committee]

Date: _____

Signed: _____

Name: _____

Position: _____

Issue Number: _____

Next Review Date: _____