Charity 501
SC501001

Data Protection Policy

0.1 | Draft for board approval

Document Control

Document title	Data Protection Policy
Version	0.1
Status	Draft for board approval
Owner	
Approved by (name and role)	
Date approved	
Next review due	
Classification	

Version History

Version	Date	Author	Summary of changes
0.1			

Before adoption

Confirm every field above and every placeholder in this document (such as [INSERT NAME] or [INSERT DATE]) has been completed before the board adopts it. Then read the whole document against the charity's own circumstances: every statement about what the charity holds, has decided, has arranged or has already done must be true, and anything that is not must be changed before adoption.

- [CHARITY TO CONFIRM: the name and job title of the Data Protection Lead (clause 7.2)]
- [CHARITY TO CONFIRM: the name and job title of the Deputy Data Protection Lead (clause 7.2)]
- [CHARITY TO CONFIRM: the name of the nominated trustee who handles concerns involving the Chair (clause 7.6)]
- [INSERT CONTACT METHOD for data subject requests (clause 8.10), for example a dedicated email address or postal address]
- [CHARITY TO CONFIRM: our ICO registration status has been checked using the self-assessment tool at ico.org.uk/registration, and the outcome and fee tier have been recorded in our ICO registration / data protection fee status document]
- [CHARITY TO CONFIRM: our Record of Processing Activities (Article 30) has been prepared or updated and covers all current processing activities, including special category data, criminal offence data, and PVG information]
- [CHARITY TO CONFIRM: the retention periods for each category of personal information, including the specific period for child protection and safeguarding records, have been set by the board and recorded in the Record of Processing Activities]

- [CHARITY TO CONFIRM: a Privacy Notice has been prepared for each audience group (service users and beneficiaries; staff and volunteers) and is being provided at the point of data collection]
- [CHARITY TO CONFIRM: written data processing agreements are in place with all third-party processors named in our Record of Processing Activities]

Important: These are draft outputs from a Charity Compliance Engine advisory session. They require trustee review, adaptation to your specific circumstances, and formal board approval before adoption. They do not constitute legal advice. Independent professional advice should be sought for complex or high-risk areas.

Contents

Document Control 2
Version History 2
Before adoption 2
Contents 4
Data Protection Policy 5
1. Purpose and Scope 5
2. Legal Framework 5
3. The Data Protection Principles 5
4. Lawful Basis for Processing 6
5. Special Category Data and Criminal Offence Data 7
6. Children's Data 7
7. Data Protection Lead — Who Is Responsible 8
8. Individual Rights 8
9. Retention and Storage Limitation 9
10. Personal Data Breaches 10
11. High-Risk Processing and Data Protection Impact Assessments 11
12. Data Sharing and Third-Party Processors 11
13. ICO Registration 11
14. Security 12
15. Related Policies and Documents 12
Reference Materials 14

A DIAGRAM FROM THIS POLICY

Choosing a lawful basis

Shown in full. In the policy it sits beside the text it supports.

REFERENCE **UK GDPR: Which Lawful Basis Applies?**

Every time your organisation processes personal data, one of the seven lawful bases must apply. Choose the basis that most accurately reflects the reason for processing, and do not stack multiple bases as a precaution. Consent is not always the right choice.

1. Consent

Freely given, specific, informed and unambiguous

Use for newsletters, marketing, optional data collection, and photography. Must be as easy to withdraw as to give. Cannot be bundled with service provision.

Usually inappropriate for service users or staff: where someone depends on your organisation for support or employment, the power imbalance often means consent cannot be truly free, and it can be withdrawn at any time. Another basis (commonly legitimate interests) is usually more appropriate for routine beneficiary processing. This is a strong caution, not an absolute ban.

2. Contract

Necessary to perform a contract with the individual

Use for processing employee or contractor data necessary to manage their employment, pay salary, or fulfil contractual obligations.

Processing must be genuinely necessary for the contract — not just convenient.

3. Legal Obligation

Required by UK law or a court order

Use for payroll and PAYE records (HMRC), PVG and disclosure checks (Disclosure Scotland), statutory reporting to OSCR, and compliance with court orders.

The specific legal obligation must be identified — "we have to" is not sufficient.

4. Vital Interests

Necessary to protect someone's life

Use in genuine emergencies where the person cannot consent and life is at risk. Sharing health information with emergency services when a service user is unconscious or in immediate danger.

Last resort only — not for routine health data processing.

5. Legitimate Interests

Necessary for your legitimate interests or a third party's

Use for internal record-keeping, fraud prevention, network security, processing volunteer contact details, and most routine administrative processing where individuals would reasonably expect it.

Requires a Legitimate Interests Assessment (LIA) documenting: (1) the legitimate interest pursued; (2) why processing is necessary for it; (3) that the individual's rights do not override yours. Keep the LIA on record. Most routine charity administration passes this test, but document your reasoning.

6. Public Task

Necessary for a task carried out in the public interest

Primarily for public authorities. May apply to charities delivering commissioned public services where the task or authority has a basis in law: for example, a charity delivering adult social care under a statutory function.

Rarely applies to independent charities. A public-sector contract alone does not create it: the task or authority must be grounded in law.

7. Recognised Legitimate Interests

A narrow, pre-approved public-interest basis (Annex 1)

Added by the Data (Use and Access) Act 2025 (in force 5 February 2026). Covers only the short list of purposes in Annex 1, including safeguarding vulnerable individuals and preventing or detecting crime.

Do not confuse this with ordinary legitimate interests (basis 5). It applies only to the exact Annex 1 purposes. There is no balancing test, but you must still show the processing is necessary.

Special category data (health, disability, ethnicity, religion, sexual orientation, sex life, genetic or biometric data): A lawful basis alone is not sufficient. You also need a separate Article 9 condition, most of which sit in Schedule 1 DPA 2018. For charities, the most common conditions are: explicit consent; employment law obligations; substantial public interest (including safeguarding); or vital interests where consent cannot be given. Document both the lawful basis and the Article 9 condition separately.

Criminal convictions and offences data is not special category data. It is governed separately by Article 10 and the DPA 2018: you need both an Article 6 basis and a specific Article 10 / Schedule 1 condition, and for many conditions an appropriate policy document. Do not treat it as an Article 9 matter.

Source: UK GDPR Articles 6, 9 and 10 · Data Protection Act 2018 Schedule 1 · Data (Use and Access) Act 2025 (recognised legitimate interests, Annex 1) · ICO Lawful Basis Guidance (ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis)