Data Use and Access Policy

Organisation Name: [Insert Charity Name]
Version: 1.0
Approved by: [Board / SMT]
Date Approved: [DD/MM/YYYY]
Next Review Date: [DD/MM/YYYY]

---

1. Purpose

This Data Policy sets out how [Organisation Name] collects, uses, manages, shares, and protects data. Its purpose is to ensure that data is treated as a valuable organisational asset, used responsibly, lawfully, and effectively to support our mission and improve outcomes for the people and causes we serve.

This policy provides a clear framework for decision-making, accountability, and good practice across the organisation.

---

2. Scope

This policy applies to:

- All staff, trustees, contractors, consultants, and volunteers
- All data created, collected, processed, or stored by the organisation
- All systems, tools, platforms, and formats (including paper records, spreadsheets, databases, and cloud systems)

---

3. Principles

[Organisation Name] manages data in line with the following principles:

1. **Lawful and Fair Use** – Data is collected and processed in line with relevant legislation and regulatory guidance.
2. **Purpose-Driven** – Data is collected for clear, defined purposes that support organisational objectives.
3. **Proportionate** – We only collect data that we genuinely need.
4. **Accurate and Reliable** – Reasonable steps are taken to ensure data is accurate and kept up to date.
5. **Secure** – Data is protected against unauthorised access, loss, or misuse.

6. **Accessible and Useful** – Data is made available to those who need it to do their role effectively.
7. **Accountable** – Clear ownership and responsibility for data is defined.

---

4. Data Types Covered

This policy covers, but is not limited to:

- Personal data
- Special category data
- Supporter and beneficiary data
- Staff and volunteer data
- Financial and transactional data
- Monitoring, evaluation, and impact data
- Operational and performance data

---

5. Legal and Regulatory Framework

[Organisation Name] complies with all relevant data protection and information governance legislation, including:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR)

Related policies include:

- Privacy Notice
- Data Retention Policy
- Information Security Policy
- Acceptable Use Policy

---

6. Roles and Responsibilities

Board of Trustees

- Provide oversight and assurance that data is managed responsibly.

- Approve this policy and any material changes.

Senior Management Team

- Ensure this policy is implemented and resourced appropriately.
- Promote a positive data culture across the organisation.

Data Owner(s)

- Accountable for specific datasets or systems.
- Ensure data quality, appropriate access, and compliance.

All Staff and Volunteers

- Follow this policy and related procedures.
- Complete relevant training.
- Report data breaches or concerns promptly.

---

7. Data Collection

Data is collected:

- For clear, legitimate purposes
- Using fair and transparent methods
- With appropriate consent or lawful basis

We aim to collect data at the right level of detail and avoid unnecessary duplication.

---

8. Data Quality

[Organisation Name] is committed to maintaining good data quality. This includes:

- Clear definitions and standards
- Routine checks for accuracy and completeness
- Processes for correcting errors

Data quality issues should be reported to the relevant Data Owner.

---

9. Data Storage and Security

Data is stored securely using approved systems and tools. Controls include:

- Role-based access
- Strong passwords and multi-factor authentication where available
- Regular backups
- Secure disposal of data when no longer required

---

10. Data Sharing

Data is only shared:

- Where there is a lawful basis
- With appropriate safeguards in place
- In line with data sharing agreements where required

Third-party processors are assessed for compliance and security.

---

11. Data Retention and Disposal

Data is retained only for as long as necessary and in line with the organisation's Data Retention Policy. When data is no longer required, it is securely deleted or destroyed.

---

12. Data Breaches and Incidents

All suspected or actual data breaches must be reported immediately in line with the organisation's Data Breach Procedure. Appropriate action will be taken to assess, mitigate, and report incidents where required.

---

13. Training and Awareness

[Organisation Name] ensures that staff and volunteers receive appropriate training to understand their data responsibilities and maintain good data practices.

---

14. Review and Maintenance

This policy will be reviewed at least annually, or sooner if there are significant changes to legislation, systems, or organisational activities.

Approval

This Data Policy was approved by:

Name: _____
Role: _____
Date: _____