STRM – SEND the Right Message Registered Charity No. 1193572

Data Protection, GDPR & Information Governance Policy

Document Purpose

This policy sets out how STRM – SEND the Right Message approaches and manages personal data and information governance. It provides clarity, consistency and accountability in line with STRM's values, governance responsibilities and legal obligations.

STRM recognises that families, children and young people, staff, volunteers, trustees and partners trust the organisation with sensitive information. This policy ensures that personal data is managed lawfully, securely and transparently.

Document Statement

STRM is committed to operating in a safe, transparent, inclusive and legally compliant manner. This policy reflects our commitment to protecting children, young people, families, staff, volunteers and trustees while ensuring high standards of data protection and information governance across the organisation.

STRM complies with relevant UK legislation including:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR)
- Human Rights Act 1998 (Article 8 – Right to Privacy)
- Freedom of Information Act 2000 (where applicable)
- Children Act 1989 and 2004 (information sharing for safeguarding)
- Working Together to Safeguard Children statutory guidance
- Charity Commission guidance on trustee responsibilities and governance

STRM also follows guidance issued by the Information Commissioner's Office regarding good practice in data protection and information governance.

Document Application

This policy applies to:
Organisation-wide / Trustees / Staff / Volunteers / Contractors

Anyone processing personal data on behalf of STRM

It applies to all personal data processed by STRM, including information stored:

- electronically
- within cloud systems
- within CRM systems
- in emails
- on portable devices
- within paper records

Responsible for Implementation

Overall accountability: Board of Trustees
Operational responsibility: CEO / Business Manager

Author

Maggie Cleary, Chief Executive Officer

Effective Date 05-03-2026

Review Date 05-03-2028

This policy will be reviewed every 2 years, or sooner if there are significant changes in legislation, regulatory guidance or STRM operational practice.

Next scheduled review: March 2028

Associated Documents

This policy should be read alongside:

- Safeguarding Adults, Children & Young People Policy
- Code of Conduct
- Equality, Diversity & Inclusion Policy
- Health & Safety Policy
- Complaints Policy
- Privacy Notice – Families & Service Users
- Privacy Notice – Staff & Volunteers
- Candidate Privacy Notice
- Website Privacy & Cookie Notice
- Data Retention & Destruction Schedule
- Record of Processing Activities (ROPA)
- MOU Partner Data Sharing Agreements
- Data Protection Impact Assessment (DPIA) Template
- Data Breach Log
- Subject Access Request Log

Approval

Approved by the Board of Trustees

Chair of Trustees: _____
Name: _____Robert Carr_____
Date: _____05-03-2026_____

Contents

Appendices

Appendices (Internal Documents)

1. Introduction

STRM processes personal data as part of delivering support services to families and communities. This policy establishes a framework to ensure personal information is handled lawfully, securely and ethically.
The policy reflects requirements under the UK GDPR and Data Protection Act 2018 and aims to protect individuals while enabling STRM to carry out its charitable activities effectively.
This policy does not form part of any contract of employment unless explicitly stated.
STRM – SEND the Right Message Charity acts as the Data Controller for the personal data it collects and processes in connection with its services and organisational activities.

2. Scope

This policy applies to all individuals working on behalf of STRM.
It covers:
• collection of personal data
• storage and security of data
• sharing of information
• retention and disposal of records
• responding to data protection requests
• management of data breaches

3. STRM Commitment

STRM is committed to:
• acting in accordance with UK data protection legislation
• protecting the rights and privacy of individuals

• collecting only the information necessary for service delivery
• maintaining accurate and secure records
• ensuring transparency in how data is used
• providing staff and volunteers with appropriate training and guidance
STRM recognises that some information processed may include special category data, such as disability or health information, and appropriate safeguards are applied.

4. Roles and Responsibilities
Board of Trustees
The Board of Trustees is responsible for:
• ensuring STRM complies with legal obligations
• overseeing risk relating to data protection
• ensuring policies and procedures are in place

Chief Executive Officer (Data Protection Lead)
The CEO is responsible for:
• overseeing implementation of this policy
• responding to data protection concerns
• ensuring compliance with UK GDPR
• maintaining appropriate records and governance documentation

Managers / Coordinators
Responsible for:
• ensuring staff and volunteers understand the policy
• ensuring data is handled appropriately
• maintaining accurate documentation

Staff and Volunteers
Must:
• comply with this policy
• only access information necessary for their role
• protect confidentiality
• report any concerns immediately

5. Policy Provisions / Procedure

Data Collection
STRM will only collect personal data where necessary for legitimate organisational purposes.
Individuals will be informed about:
• why data is collected
• how it will be used
• how long it will be stored

STRM processes personal data where it is necessary for the legitimate interests of the organisation in delivering charitable services and support to families, provided that these interests do not override the rights and freedoms of individuals.

Data Storage
Personal data will be stored securely using appropriate technical and organisational measures.
STRM may use secure systems such as CRM platforms for case management and service delivery.
Access to systems is restricted to authorised personnel.
STRM primarily stores and processes personal data within the United Kingdom.
Where third-party service providers process data outside the UK, STRM ensures appropriate safeguards are in place in accordance with UK GDPR requirements.

Data Sharing
Information may be shared with trusted partners where necessary and lawful, including:
• referral partners
• safeguarding authorities
• statutory services
Where appropriate, data sharing agreements will be in place.

Data Retention
Personal data will only be retained for as long as necessary.
Retention periods are defined in the Data Retention & Destruction Schedule.

Data Security
STRM implements appropriate safeguards including:
• password protection
• restricted access to systems
• secure storage of documents
• safe disposal of confidential records

6. Breach of Policy
Failure to comply with this policy may result in:
• informal action
• formal disciplinary procedures
• termination of volunteer arrangements
• escalation to regulatory authorities where appropriate

7. Monitoring and Review
Compliance with this policy will be monitored by the CEO and Board of Trustees.
The policy will be reviewed in line with the review date stated above or sooner if required due to legislative change, operational need or identified risk.

APPENDICES

Appendix 1 – Data Protection Principles
Personal data must be:
1. Lawful, fair and transparent
2. Collected for specific purposes
3. Adequate and relevant
4. Accurate and kept up to date

5. Stored only as long as necessary
6. Processed securely
7. Processed with accountability

Appendix 2 – Lawful Bases for Processing
STRM may process personal data using:
• Consent
• Contract
• Legal obligation
• Legitimate interests
• Vital interests
• Public task (where relevant)

Data Protection Principles
These are the seven principles of UK GDPR Article 5.
Personal data must be:
• Lawful, fair and transparent
• Collected for specific purposes
• Adequate, relevant and limited to what is necessary
• Accurate and kept up to date
• Stored only as long as necessary
• Processed securely
• Processed with accountability

Appendix 3 – Individual Rights
Individuals have the right to:
• access their personal data
• request corrections
• request deletion in certain circumstances
• restrict processing
• object to processing
• request data portability

If an individual is unhappy with how STRM has handled their personal data, they have the right to raise a complaint with the **Information Commissioner's Office (ICO)**, the UK's independent authority for data protection.
Website: https://ico.org.uk

Appendix 4 – Data Breach Procedure
If a breach occurs:
1. Report immediately to STRM management
2. Assess risk to individuals
3. Record the breach in the breach log
4. Notify the Information Commissioner's Office if required within 72 hours of becoming aware of the breach where required under UK GDPR.
5. Inform affected individuals where appropriate

6. Review procedures to prevent recurrence

Appendix 5 – Subject Access Request Procedure
When a request is received:
1. Confirm identity
2. Record the request
3. Locate relevant data
4. Review for exemptions
5. Provide response within one month

Appendix 6 – Data Security Standards
STRM ensures:
• secure password protected systems
• restricted access to data
• secure cloud services where used
• safe storage of paper records
• secure disposal of information

STRM maintains appropriate technical and organisational measures in accordance with Article 32 of the UK General Data Protection Regulation.

Appendix 7 – Definitions
Personal Data:
Information relating to an identifiable individual.
Special Category Data:
Sensitive data including health or disability information.
Processing:
Any activity involving personal data including collection, storage or sharing.
Data Controller:
Organisation responsible for determining how personal data is used.

Appendix 8 – Record of Processing Activities (Data Mapping)
Under Article 30 of the UK General Data Protection Regulation (UK GDPR), organisations must maintain records of their data processing activities where they process personal data as part of their operations.
STRM maintains a Record of Processing Activities (ROPA) which documents how personal data is collected, used, stored and protected across the organisation.
The purpose of maintaining this record is to:
• demonstrate compliance with UK GDPR
• identify potential risks in how data is handled
• ensure transparency and accountability
• support data protection impact assessments where required
The ROPA is maintained internally and reviewed periodically by the CEO and Board of Trustees.

Security and Access
Access to processing records and systems is restricted to authorised staff or trustees where necessary for operational purposes.

Appropriate safeguards are applied to ensure data security and confidentiality.

Review
The Record of Processing Activities is reviewed periodically to ensure:
• accuracy
• compliance with current legislation
• alignment with STRM operational practice
Where new projects, services or systems are introduced, STRM will review whether a Data Protection Impact Assessment (DPIA) is required.

Typical Processing Activities at STRM
Examples of processing activities recorded within the ROPA may include:

Activity	Personal Data	Purpose	Lawful Basis	Storage	Retention
Family support referrals	Name, contact details, family information, SEND needs	Providing support services	Legitimate interests	Secure CRM system	As per retention schedule
Event registrations	Name, email, attendance records	Managing sessions and workshops	Consent / Legitimate interests	Booking systems	As per retention schedule
Volunteer management	Contact details, DBS checks, references	Managing volunteer roles	Legal obligation / Legitimate interests	Secure internal records	As per retention schedule
Staff employment records	Payroll, contact details, HR records	Employment administration	Contract / Legal obligation	Secure HR records	As per retention schedule