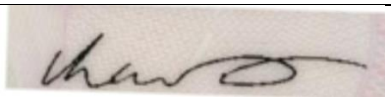
Document Title:	Data Protection Policy
Document Purpose:	This policy sets out the key principles all staff, including employees, volunteers and anybody involved in Send The Right Message's (STRM) work are required to follow when using and storing information about staff, supporters and the families and individuals we work with
Document Statement:	It is a fundamental principle of STRM's work with children, young people, families and adults that we use and store all personal information safely and lawfully. This is central to our successful operation as a charity and maintaining the confidence of those with whom we work, who work for, and with us. We must all, therefore, respect the privacy of all personal information and be aware of our data protection obligations.
Document Application:	Organisation-wide- all staff, volunteers and Trustees
Responsible for Implementation:	**Data Protection Officer- CEO**
Author:	**Tricia Cowdrey**
Effective date:	**1st January 2024**
Review/Expiry date:	**31st December 2028, or if a change in legislation**

Associated Documents
Data Protection Act
Code of Conduct for staff and volunteers
Complaints, comments and complements policy
Whistleblowing policy
Safer Recruitment Policy
Staff and Volunteer Handbooks

Signed 

Chair of Trustees: Vicki Lamb

Contents

1. Data Protection Principles
2. Privacy Notices
3. Accuracy, Adequacy, Relevance and Proportionality
4. Storage and Archiving
5. Security and Confidentiality
6. Processing in Accordance With the Rights of the Data Subject
7. Legal Justifications
8. Special Category Personal Data
9. Legitimate Interests
10. Data Retention

Appendices-

APPENDIX 1 Privacy Notice -long Version

APPENDIX 2 Employee Privacy Notice

APPENDIX 3 Filming and Photography Policy

APPENDIX 4 Confidentiality Statement

APPENDIX 5 Data Retention and Destruction Schedule

1. DATA PROTECTION PRINCIPLES

1.1 STRM must only process data in accordance with its legal obligations and duties, as set out in the fundamental principles below. As a member of staff or volunteer, you must only process data in accordance with its legal obligations and duties, as set out in the fundamental principles below. As a member of staff or volunteer, you must only process personal data in accordance with these principles:

1.2 Fair, lawful and transparent processing for an authorised purpose

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. It must also only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

In practice, this means that you must not process personal data unless one of the legal justifications for processing is met:

Consent – Valid consent has been obtained from the data subject.

Performance of a contract - Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract;

Processing is necessary for compliance with a legal obligation to which STRM is subject (e.g. where STRM needs to comply with HMRC or money laundering obligations);

Processing is necessary to protect the vital interests of a data subject or another person – this condition can only apply in life and death situations e.g. safeguarding;

Processing is in the legitimate interests of STRM, except where such interests are overridden by the interests, rights or freedoms of the data subject.

When Special Categories of data, (otherwise known as sensitive personal data) are collected, explicit consent to processing must be obtained, unless certain limited circumstances apply.

Further information in relation to each of these legal justifications for processing both personal and special category data is set out under “Legal Justifications”, below.

2. PRIVACY NOTICES

STRM has privacy notices (See Appendix 1 and 2) which apply to employees, volunteers, contractors and service users. The appropriate privacy notice must be provided to data subjects at the point at which personal information is collected. For an employee, that is when they apply for a job or are offered a job, or for a supporter, when they make a donation or express interest in an event.

For services, where STRM is a data controller of data a STRM services data privacy notice will apply. The DPO will provide guidance as to the correct notice to use. Where STRM is the data processor of data for a service, the data controller’s privacy notice will need to be used. The DPO can provide guidance in relation to this

If you have any questions in relation to the above, contact the Data Protection Officer, or the CEO at admin@strmsupport.co.uk

The appropriate notice will need to be provided to the data subjects at the point at which personal information is collected. For services, this is most likely to be when a family is referred to or signs up to a service.

The Privacy Notices set out the purposes for which data will be used by STRM and are intended to ensure that our data processing is fair and transparent and that data subjects know how we collect and use their data and have the opportunity to exercise their rights in relation to their data (see below).

The Data Protection Officer is responsible for keeping the Privacy Notices up to date.

If you process personal data collected by STRM as a data controller, then you must consider the fairness of how the data is used and must not use data collected for one purpose for another purpose without the explicit authorisation of the data subject of the Data Protection Officer.

If you process data as part of a service where STRM are the data processors, you must only process data in line with the instructions of the controllers.

Whenever personal information is collected for purposes not covered by the existing STRM Privacy Notices, appropriate privacy notices will be developed by the DPO

3. ACCURACY, ADEQUACY, RELEVANCE AND PROPORTIONALITY

All personal data that STRM holds must be adequate, relevant and limited to what is necessary in relation to the purposes for which it was processed.

Personal data must also be accurate and, where necessary, kept up to date. Reasonable steps must be taken to ensure that personal data which is inaccurate is erased or rectified without delay; In practice, this means that: You must make sure that any personal or sensitive personal data that you process is accurate, adequate for the purposes you need it for (and not more than you need), relevant, and proportionate for the purpose for which it was obtained.

Individuals are entitled to ask STRM to correct personal data relating to them which they consider to be inaccurate

You must ensure that personal data held by STRM relating to you is accurate and updated as required. If your personal details or circumstances change, you must inform your line management and the HR Department so that STRM's records can be updated.

4. STORAGE AND ARCHIVING

Personal data must be kept in a form which allows identification of data subjects for no longer than is necessary for the purposes for which personal data is being processed.

In practice this means that:

Data must only be held in accordance with the STRM Data Retention Policy and its accompanying schedules. All records, including electronic and paper records containing personal data must be destroyed safely after the specified retention period, in accordance with the Data Retention Policy.

5. SECURITY AND CONFIDENTIALITY

Data must be processed in a way that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

In practice, this means that:

STRM must protect personal data from unlawful or unauthorised processing and against accidental loss, destruction or damage through a number of means;

All STRM staff and volunteers must ensure data is kept secure in accordance with this policy, which sets out your responsibilities in relation to the security of and handling of data.

Where external organisations provide STRM services or engage a third party to support an STRM project, security arrangements must be set out in contracts with those organisations, and measures must be followed and implemented to safeguard the security of personal data the third-party organisation will be handling.

All known potential data protection breaches (such as the loss of personal data or evidence that an unauthorised person has accessed it) must be reported immediately to a line manager and the Data Protection Officer in accordance with the Data Breach Procedure

6. PROCESSING IN ACCORDANCE WITH THE RIGHTS OF THE DATA SUBJECT

STRM must fully enable those who it holds data about (Data Subjects) to exercise their specific rights in relation to the data we hold on them. If you receive any request in relation to a data subject's data, please see the Information Rights Procedure for how to deal with the request. The data subject rights that you are most likely to encounter are set out below

6,1 Subject Access Requests (SARs)

Any person about whom STRM holds personal data is entitled to make a Subject Access Request (a 'SAR') to STRM to find out what information we hold about them. Such request could be in letter or email format and simply ask for STRM to provide them with a copy of information held about the requester.

If you receive a request that you think could be a Subject Access Request from a Service User, member of staff, volunteer or any other individual or organisation, send the request to admin@strmsupport.co.uk as soon as possible as STRM will only have 30 days to respond to the request. The Data Protection Officer will then help you to respond to the request.

6.2 Right to Prevent Direct Marketing

Individuals all have the right to ask that STRM doesn't contact them with marketing letters, emails, text messages or phone calls. If such a request is received by any STRM member of staff, the DPO must informed as soon as is practicable and in any case within three days of the request.

STRM practice is to rely on a combination of consent for its electronic communications and legitimate interests in relation to its postal marketing communications. Anyone responsible for marketing must ensure that the necessary consent has been obtained or that a legitimate interests assessment is conducted before undertaking marketing communications.

An option for recipients of any STRM mail to opt out of STRM communications and instructions for how to do so must be included in all marketing and fundraising communications If in doubt, contact the Data Protection Officer

6.3 Right to Correct Inaccuracies

You may receive a request from a data subject to correct inaccuracies in the data you hold about them. If this request is simple, such as updating their address or contact details, such requests can be dealt with in the normal course of business. However, if the request concerns the accuracy of other records or there is any dispute as to whether or not the data recorded is,, in fact,, inaccurate, refer to the Information Rights Procedure.

6.3 Right to Erasure

An individual may request that STRM erase personal data held about them. In such cases, STRM will use its discretion to determine whether it is able to do so, in accordance with the Information Rights Procedure.

Any concerns in relation to the rights of a data subject must be referred to the Data Protection Officer

7. LEGAL JUSTIFICATIONS

7.1 Consent – Key Principles

Consent will provide the legal basis for the processing of personal data in a range of circumstances for STRM such as electronic fundraising and marketing and in limited circumstances, for some services. The categories of processing where this may apply are set out below.

Consent is one lawful basis for processing personal data, and consent (or Explicit Consent) can legitimise the processing of special category personal data (otherwise known as sensitive personal data).

When should consent be used? Consent is appropriate if you can offer people real choice and control over how you use their personal data and want to build their trust and engagement. If we cannot offer a genuine choice, consent is not appropriate.

Whenever you wish to rely upon consent as the legal basis for processing personal data, the following key principles apply:

- In order to provide valid consent, the data subject must be over 13 years of age and have capacity to consent. If they are under 13 years of age or are over 13, but do not have capacity, the consent of a parent or guardian must be obtained for the processing.
- If a data subject is between 13 and 16 years of age, obtaining the consent of both the young person and a parent / guardian is encouraged.
- All consents must comply with the requirements set out in this policy.

What is “Valid consent”? In order to be valid, the consent obtained for processing someone’s personal data must follow the following rules:

- Consent must be freely given; this means giving people genuine ongoing choice and control over how you use their personal data.
- Consent must specifically cover the controller’s name, the purposes of the processing and the types of processing activity.
- Consent requests must be prominent, separated from other terms and conditions, concise, easy to understand, and user friendly.
- Consent must be specific and broken down into the different data processing activities for which you are seeking consent.
- Consent should be obvious and require a positive action to opt in. The use of pre-ticked opt in boxes is not permitted.
- Consent can be obtained verbally or in writing, but must be clear, in each instance. If consent is obtained verbally, a clear record should be kept of what was discussed, when it was discussed and that consent was obtained. If consent is obtained in writing, a copy of the consent form must be retained.
- Explicit consent, such as for the processing of special categories of personal data must be expressly confirmed in words, rather than by any other positive action.
- There is no set time limit for consent. How long it lasts will depend on the context. Consent should be reviewed and refreshed as is appropriate for the purpose the consent is held. If in doubt, contact the Data Protection Officer.
- Make sure consents remain valid – if the type of personal data you are collecting or what you are doing with it changes, check whether the consent you hold covers that type of processing. If not, the consent will need to be updated to cover the new type of processing.
- Everyone has the right to withdraw consent they have given. People must therefore be told that they have a right to withdraw, (alongside information about how to withdraw consent) at any time.

8. SPECIAL CATEGORY PERSONAL DATA

Special Category Personal Data should not be processed unless either, specific, explicit consent has been obtained from the data subject to that special category personal data being processed, or one of the exceptions for processing special category data without consent under the Data Protection Act 2018 and the GDPR applies.

Obtaining specific, explicit consent means ensuring that the data subject understands exactly what special category personal data you are processing and why and that you have obtained their explicit, direct consent for that processing. As with all other consent, as set out above, explicit consent can be verbal or in writing, but a clear record must be kept of the consent obtained.

The principles set out above in relation to what constitutes valid consent and all of the consent principles apply equally to explicit consent.

9. LEGITIMATE INTERESTS

legitimate interests can only be relied upon as a legal basis for processing personal data if it is in the legitimate interests of STRM to process the personal data concerned, except where these interests are overridden by the interests or the fundamental rights and freedoms of the individual concerned.

This is particularly important where the data subject is a child as extra care should be taken.

Whether legitimate interests can be relied upon as a basis for processing must always be assessed in accordance with the Legitimate Interests Assessment Procedure.

An example of where legitimate interests might apply is the processing of bank details to facilitate the payment of salaries. It is in both STRM's and the employee's legitimate interests that staff are paid. The need for personal data to be processed for that is unlikely to be outweighed by any concerns that employees might have around STRM processing their bank details in that manner. The fact that STRM keeps that employee personal data safe and secure and only uses that personal data for that purpose supports the conclusion that the fundamental rights of employees are not overridden as a result of that processing.

If you are already processing personal data without consent and you feel that legitimate interests applies – get in touch with the Data Protection Officer as soon as possible.

If it is determined that the legitimate interests category is not met for processing personal data, another legal basis will need to be considered. If there is no legal basis for the processing, it must not go ahead. If in doubt, contact the Data Protection Officer.

Consent and Legitimate Interests are likely to be the two main legal bases upon which STRM processes data. However, this policy will be updated from time to time in accordance with the law and practice.

STRM is committed to protecting the data of those it works with and for and ensuring compliance with its legal and regulatory obligations. If you have any questions in relation to this policy or any aspect of data protection please contact the Data Protection Officer

10. DATA RETENTION

10.1 Legal Principles- This applies to all data that STRM holds in all departments, such as Services, HR, Finance and Fundraising and applies to personal data, special categories of data and non-personal data, such as finance records and contracts.. Data that is not personal data or special category data must be treated in accordance with this policy and the Data Retention Schedules to comply with legal and regulatory requirements (e.g. of HMRC), best practice, and to ensure the efficient management of documents and electronic files.

10.2 Personal data and special category data- The General Data Protection Regulation (GDPR) and UK data protection legislation requires that STRM complies with the following principles in relation to retention of personal data and special category data:

1. Data Minimisation: The personal data that we store on individuals and how long we store it for, is minimised;

2. Storage Limitation: Data must not be kept longer than is necessary for the purpose for which is it is being processed, and that period should be kept to a strict minimum;

3. Lawfulness, Fairness and Transparency: STRM must be transparent and inform individuals how long their personal data will be retained for, at the point that the personal data is obtained. If that's not possible, we should outline the criteria used to determine that period.

Where STRM is the data controller, we must determine the period for which personal data is retained and ensure that anyone processing personal data on our behalf complies with our data retention requirements. Where STRM is the data processor, we must comply with the data retention instructions of the data controller. The principles set out above mean that different types of personal data should be retained for different periods, as set out in the Data Retention Schedules. The relevant retention period will depend upon:

- What the data / information is used for;
- Legal or regulatory requirements;
- Agreed industry practices (where relevant);
- The ease or difficulty of making sure the data remains accurate and up to date;
- The current and future value of the information;
- The costs, risks and liabilities associated with retaining the data;

4. Use of the Data Retention Schedules should be made whether you are using electronic files (e.g. on a database such as data stored on a shared drives or in emails), or paper files, always refer to the relevant Data Retention Schedule, set out at Appendix 5, which will set out the applicable retention period you must comply with. If you have any questions, contact the Data Protection Officer.

Paper records Paper records must not duplicate electronic case files unless there is a contractual or regulatory requirement to do so. Where possible, and where there is no legal requirement to retain an original document, paper documents must be

scanned onto the electronic case file. The original paper copy must then either be returned to the originator, or destroyed if not required.

A paper record must not be used to store creative material originated by a service user unless this is part of a therapeutic intervention and cannot be scanned onto the electronic case file. Wherever possible, personal documents should always be returned to the service user or their carer at the point of closure of the file after being scanned onto the electronic case file or photocopied.

Contractual / Partnership requirements If STRM is regarded as a data processor and the partner or commissioner is the data controller, STRM will be required to follow the retention policy of the data controller.

In such cases, the retention period may be referred to in the contract with the partner/commissioner, or you may need to ask them to tell you what their data retention policy requires.

Special cases - When retention of records in excess of the time set out in the Data Retention Schedules may be necessary, there may be occasions when information needs to be retained and preserved beyond the limits set out in the Schedules, including:

- Where there are legal proceedings, or a regulatory or similar investigation that are known to be likely, threatened or actual;
- Where a crime is suspected or detected; or where
- Contractual provisions in documentation require the approval of someone outside of STRM prior to destruction.

If you are in any doubt as to whether any of the above apply, contact the Data Protection Officer.

5 Closed Case Files- STRM must keep a record of closed case files and securely store the closed case file list. When STRM is a data controller and is not required to comply with the data retention policies of a third party, the next step, following completion of the Closed Case File Record is that the service shall retain all paper case files for 2 years, following which they will be archived.

6. Destruction of archived files will take place on an annual basis, in line with the Retention Periods Schedule.

7. Returning Files Where a Commissioner or third party, as data controller, requires files to be returned to them- the transfer of files (electronic or paper) must be undertaken securely to ensure no loss of data or damage to the integrity of the data. If you have any questions in relation to how you can securely transfer either paper or electronic files, please contact the Facilities or Digital Systems Teams before undertaking the transfer. For further guidance on individual documentation, please contact the Data Protection Officer .

Appendix 1: Privacy Notice

PRIVACY NOTICE- LONG VERSION

1. INTRODUCTION

We understand that the privacy of all of our volunteers, supporters and service users is essential to them and that they care about how their personal data is used.
This Privacy Notice refers to all individuals as "you" for convenience. We respect and value your privacy and will only collect, hold, use, or share your personal data in ways described here and in a way that is consistent with our obligations and your legal rights.

Information about us SEND the Right Message Charity is a registered charity no: 1193572 and is a charitable incorporated organisation regulated by the Charity Commission.

Data Protection Officer: Mrs Maggie Cleary, Chief Executive Officer

Email address: info@strmsupport.co.uk

2. What does this Notice cover?

This Privacy Notice explains the types of personal data we collect, how it is collected, how it is held, how we use it, and how it is processed. It also explains your rights under data protection legislation relating to your personal data. Further information about your rights can be obtained from the Information Commissioner's Office or your local Citizens Advice.

3. What is "personal data"?

Personal data is any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier. Personal data is, in simpler terms, any information about you that enables you to be identified. Personal data covers obvious information such as your name and contact details but also less obvious information such as identification numbers, electronic location data, and other online identifiers. The personal data we collect and use is in paragraph 5 below.

4. What are my rights?

Under data protection legislation, you have the following rights, which we will always work to uphold.
You have the right to:
a) be informed about how we process your personal data;
b) access and be given a copy of the personal data we hold about you. (See paragraph 10 below about this);
c) require us to correct any personal data that we hold about you if any of it is inaccurate or incomplete;
d) be forgotten: in certain circumstances, you have a right to have your personal data erased from our records;

e) restrict (i.e., prevent) the processing of your personal data;
f) object to the way we process your personal data (e.g., for direct marketing); g) withdraw consent: if we are relying on your consent as the legal basis for using your personal data, you are free to withdraw that consent at any time;
h) data portability: the right in certain circumstances to have us transfer your personal data to another organisation and
i) not be subject to a decision based solely on automated processing (including profiling), which legally affects you. We do not use your personal data in this way. As to how to contact us for more information about our use of your personal data or exercising your rights as outlined above, see paragraph 11 below.
Your personal data must be kept accurate and up-to-date. If any personal data we hold about you changes, please keep us informed if we have that data. Suppose you wish to complain about our use of your personal data. In that case, you have the right to complain to the Information Commissioner's Office, but don't hesitate to contact us first (see paragraph 11 below) so that we might try to resolve your concerns ourselves.

5. What personal data do you collect and how?

We may collect and hold some or all of the personal data below either by interaction with you or via our website

- Identity Information, including name, title, date of birth and gender. Contact information, including address, email address, and telephone number.
- Payment information, including card details, bank account numbers and whether you are a taxpayer.
- Health information, including details of any formal diagnoses

6. How do you use my personal data?

Under UK data protection legislation, we must always have a lawful basis for using personal data. The following table describes how we may use your personal data and our lawful bases for doing so.

What data do we use?
- Managing our relationship with you, e.g., as a volunteer or employee.
- Personal details
- Contact details
- Payment details
- Required for the performance of our contract with you.
- To be able to make payments
- Supplying our services to you.
- Personal details
- Contact details
- Payment details

Required for the provision of services

- Managing payments for our services.

- Personal details
- Payment details
- Required for the provision of services and for administering our charity

Communicating with you, including where you enquire about us and our work, activities, volunteering, and events.

- Personal details
- Contact details

We must read and store your messages to respond as you would expect. We are supplying you with information about our work by email where you must that. (You may opt out at any time by emailing us at info@strmsupport.co.uk

- Personal details
- Contact details

You have given your active permission to receive our newsletter updates.
Receiving a donation from you and claiming Gift Aid on your donations

- Personal details
- Contact details
- Payment details

This is necessary for us to fulfil your intention of donating money: you expect a confirmation message.
Managing our events

- Personal details
- Contact details
- Payment details

This is needed to inform you about the events and fulfil your intention to pay for services.
Health information

- Personal details
- Health details

This is needed to ensure that our service providers, staff, and volunteers can meet your medical and emotional needs.

- For marketing purposes, which may include contacting you by email, WhatsApp, telephone and/or Facebook messenger and/or text message with newsletters, fundraising appeals, campaigns, or other information or information about our products or services.
- You will not be sent any unlawful marketing or spam.
- We will always work to fully protect your rights and comply with our obligations under the UK data protection legislation and the Privacy and Electronic Communications (EC Directive) Regulations 2003, and you will always opt out.
- We will only use your personal data for the purpose(s) for which it was initially collected unless we reasonably believe that another purpose is compatible with that or those original purpose(s) and need to use your personal data for

that purpose. If we use your personal data this way and you wish us to explain how the new purpose is compatible with the original, please get in touch with us using the details in paragraph 11 below.

- If we need to use your personal data for a purpose unrelated to, or incompatible with, the purpose(s) for which it was initially collected, we will inform you and explain the legal basis which allows us to do so.
- In some circumstances, where permitted or required by law, we may process your personal data without your knowledge or consent. This will only be done within the bounds of the data protection legislation and your legal rights.

7. How long will you keep my personal data?

We will not keep your personal data for any longer than is necessary, considering the reason(s) for which it was first collected. Please refer to our data retention and destruction policy

8. How and where do you store or transfer my personal data?

We will only store or transfer your personal data within the UK. This means that it will be fully protected under the data protection legislation. The security of your personal data is essential to us, and to protect your data, we take several necessary measures, including the following:

- limiting access to your personal data to those employees, volunteers, agents, contractors, and other third parties with a legitimate need to know and ensuring that they are subject to duties of confidentiality;
- procedures for dealing with data breaches (the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, your personal data), including notifying you and/or the Information Commissioner's Office where we are legally required to do so;

9. Do you share my personal data?

We will not share any of your personal data with any third parties for any purposes, subject to the following exception in some limited circumstances: we may be legally required to share specific personal data, which might include yours, if we are involved in legal proceedings or complying with legal obligations, a court order, or the instructions of a government authority. We may sometimes contract with the following third parties to supply services.

If any of your personal data is shared with a third party, as described above, we will take steps to ensure that your personal data is handled safely, securely, and in accordance with your rights, our obligations, and the third party's obligations under the law, as described above in paragraph 8.

10. How do I contact you?

To contact us about anything to do with your personal data and data protection, please use the following details (for the attention of Mrs Maggie Cleary, Data Protection Officer: Email address: info@strmsupport.co.uk

12. Changes to this Privacy Notice

We may change this Privacy Notice from time to time. This policy will be reviewed annually or when there is a change in circumstances, in work practices or the introduction of new legislation.

APPENDIX 2

EMPLOYEE PRIVACY NOTICE

We process personal data relating to those we employ to work as, or are otherwise engaged to work as, part of our workforce. We do this for employment purposes, to assist in the running of the business and/or to enable individuals to be paid.

The personal data we process may include, but may not be limited to, the following:

- data relating to your identity (including name, data of birth, gender, photographs, passport, National Insurance Number, immigration status, marital status, dependents),
- contact details (business and home address, telephone numbers, email addresses, emergency contact details),
- employment details (position, office location, terms of employment, performance and disciplinary records, sickness and holidays),
- background information (CV, previous experience, qualifications and certifications, criminal records check (for vetting purposes, where permissible and in accordance with applicable law),
- financial information (bank details, tax information, salary, benefits, expenses),
- IT information – information related to your access to our systems (login details, IP addresses, log files, access/times/durations of use, location).

The collection of this information will benefit us by:

- improving the management of workforce data across the business,
- enabling development of a comprehensive picture of the workforce and how it is deployed,
- informing the development of recruitment and retention policies,
- allowing better financial modelling and planning,
- ensuring compliance with our policies and procedures and our legal obligations,
- enabling monitoring of selected protected characteristics.

We will not share information about you with third parties without your consent unless the law allows or requires us to do so.

Under the data protection legislation you have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress,
- prevent processing for the purpose of direct marketing,
- object to decisions being taken by automated means,
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed,
- claim compensation for damages caused by a breach of the data protection legislation.

If you would like to find out more about our data retention policy and how we use your personal data, or if you want to see a copy of the information about you that we hold, please contact info@strmsupport.co.uk

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

APPENDIX 3: FILIMING AND PHOTOGRAPHY POLICY

1. AIMS

To use films and images to help build a strong and positive community for our group and to represent them in the most effective manner.

2. POLICY

We are very much volunteers, and this means that there are not large banks of staff available to deal with heavy duty administration. We believe that the below measures taken by us are proportionate, reasonable, and legally compliant.

We regularly use photographs of our members and their families for promotional or sponsorship reasons. These are usually provided by them to us for that purpose and consent is implicit.

All images will be stored electronically for no longer than 12 months. Those images posted on Social media will remain there unless we are specifically asked to physically remove them.

3. CONSENT AND CONFIDENTIALITY

In other situations, wherever reasonably possible, we will ask for express consent to be provided via our email address info@strmsupport.co.uk

In our group events, written consent from all involved would not be practical and we would therefore notify members/families of our intent to use photographs/films via clearly displayed signage.

We ask that any party who wishes to notify us that this is not agreeable to them would carefully alert us that images should not be taken. If this is not done, we consider it wholly reasonable to be able to create a record of a public event and assume consent in good faith.

We take care not to identify individuals unless necessary and relevant, unless this is planned. We need to be made aware of safeguarding reasons for not doing so (see email address above). Families often forward photographs and films to us for display. It is reasonable that these are used and that, in general, photographs and films made are very much part of the building of a community and a useful communication tool for interested parties to learn what we do and what we can offer. It is also incredibly important to us that we represent the full spectrum of disability and society in our media. It is our hope that this is understood by all groups within our society and that they feel they are equal stakeholders in this group which effectively belongs to all.

We have sometimes encountered issues with families where, for example, Domestic Violence has split families and parents do not wish for their children to be identifiable online where there are risks of safeguarding.

We would ask, in these situations, that this is made known to our staff clearly via email (as in the paragraph below) when necessary. We also take care that images used by us are appropriate (particularly when these feature vulnerable children).

GDPR rules also offer protection to those who wish to be left out of the above and we would expect anyone who opts not to have images featuring them/their families to make this clear to us info@strmsupport.co.uk to make your wish to be kept out of photographs/films known). If anyone finds photographs which feature them/their families on our website or open page which they do not wish to see published, please also follow the above procedure immediately to see that these are removed.

APPENDIX 4 CONFIDENTIALITY STATEMENT AND INFORMATION SHARING PROTOCOL

1. General principles

1.1 SEND THE RIGHT MESSAGE (STRM) recognises that colleagues (employees, volunteers, trustees, secondees and students) gain information about individuals and organisations during their work or activities. In most cases such information will not be stated as confidential and colleagues must exercise common sense discretion in identifying whether this information should be communicated to others.

Information given in confidence must not be disclosed without consent unless there is a justifiable reason e.g., a requirement of law or there is an overriding public interest to do so.

1.2 Confidential information includes anything that contains the means to identify a person, e.g., name, address, post code, date of birth, National Insurance Number, passport and bank details. It includes information about sexual life, beliefs, omission or alleged commission of offences and other sensitive personal information as defined by the Data Protection Act. It also includes information about organisations such as confidential business plans, financial information, contracts, trade secrets and procurement information.

1.3 Colleagues should seek advice from the CEO about confidentiality and sharing information as necessary.

1.4 Colleagues will avoid exchanging personal information or comments about individuals with whom they have a professional relationship.

1.5 Talking about the private life of a colleague is to be always avoided, unless the colleague in question has instigated the conversation.

1.6 Colleagues will avoid discussing confidential information about organisations or individuals in social settings.

1.7 Colleagues will not disclose to anyone any information considered sensitive, personal, financial or private without the knowledge or consent of the individual.

1.8 Where there is a statutory duty on STRM to disclose information, the person or people involved will usually be informed that disclosure has or will be made unless this would put at risk the safety of any individual or jeopardise a potential criminal investigation. Details about disclosure of information and who has been informed will always be kept on record and stored securely with restricted access.

1.9 Confidential information will be stored securely. It will not be left on desks but locked away. On the computer it will be stored in password protected folders.

2. Why information is held

2.1 Most information held by STRM relates to individuals, voluntary and community organisations, self-help groups, volunteers, students, employees, trustees, or services which support or fund them.

2.2 Information is kept to enable STRM colleagues to understand the history and activities of individuals or organisations in order to deliver the most appropriate services.

2.3 STRM has a role in putting people in touch with voluntary and community organisations and keeps contact details which are passed on to any enquirer, except where the group or organisation expressly requests that the details remain confidential.

2.4 Information about students is given to the training organisation and the college, but to no one else.

2.5 Information about protected equality characteristics of users is kept for the purposes of monitoring our equal opportunities policy and also for reporting back to funders.

3. Access to information

3.1 Information is confidential to STRM as an organisation and may be passed to colleagues, line managers or trustees on a need-to- know basis to ensure the best quality service for users.

3.2 Where information is sensitive, i.e., it involves disputes or legal issues, it will be confidential to the employee dealing with the case and their line manager. Such information should be clearly labelled 'Confidential' and should state the names of the colleagues entitled to access the information and the name of any individual or group who may request access to the information.

3.3 Colleagues will not withhold information from their line manager unless it is purely personal.

3.4 Users may have sight of STRM records held in their name or that of their organisation. The request must be in writing to the CEO giving 14 days' notice and be signed by the individual. Sensitive information as outlined in para 3.2 will only be made available to the person or organisation named on the file.

3.5 Employees may have sight of their personnel records by giving 14 days' notice in writing to the CEO.

3.6 When photocopying or working on confidential documents, colleagues should ensure people passing do not see them. This also applies to information on computer screens.

4. Storing information

4.1 General non-confidential information about organisations is kept in unlocked filing cabinets and in computer files with open access to all at STRM office.

4.2 Personnel information on employees, volunteers, students, and other individuals working within STRM Committee will be kept in lockable filing cabinets by STRM

4.3 Files or filing cabinet drawers bearing confidential information should be labelled 'confidential'.

4.4 In an emergency, the CEO may authorise access to files by other people.

5. Duty to disclose information

5.1 There is a legal duty to disclose some information including:

5.1.1 Child and vulnerable adult abuse will be reported to the relevant statutory services

5.1.2 Drug trafficking, money laundering or acts of terrorism will be disclosed to the police.

5.2 In addition, colleagues believing an illegal act has taken place, or that a user is at risk of harming themselves or others, must report this to the CEO who will report it to the appropriate authorities.

5.3 Users should be informed of this disclosure unless this would put at risk the safety of any individual or jeopardise a potential criminal investigation. Details

about disclosure of information and who has been informed will always be kept on record and stored securely with restricted access.

6. Disclosures

6.1 STRM complies fully with the DBS Code of practice (E File) regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information.

6.2 Disclosure information is always kept separately from an applicant's personnel file in secure storage with access limited to those who are entitled to see it as part of their duties. It is a criminal offence to pass this information to anyone who is not entitled to receive it.

6.3 Documents will be kept for 2 years and thendestroyed by secure means. Photocopies will not be kept. However, STRM will keep a record of the date of issue of a Disclosure, the name of the subject, the type of Disclosure requested, the position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the recruitment decision taken.

7. Data Protection Act

7.1 Information about individuals, whether on computer or on paper, falls within the scope of the Data Protection Act and must comply with the data protection principles. These are that personal data must be:

· Obtained and processed fairly and lawfully.

· Held only for specified lawful purposes.

· Adequate, relevant, and not excessive.

· Accurate and where necessary kept up to date.

· Not kept longer than necessary, for the purpose(s) it is used

· Processed in accordance with the rights of the data subject under the Act.

· Appropriate technical and organisational measures are to be taken to guard against loss or destruction of, or damage to, personal data

· Not transferred to countries outside the European Economic Area without an adequate level of protection in place.

8. Breach of confidentiality

8.1 Misuse of personal data and security incidents must be reported to line managers so that steps can be taken to rectify the problem and ensure that the same problem does not occur again. This includes unauthorised access to person-identifiable information where a member of staff, or third party, does not have a need to know. It also includes incidents of information lying around in a public area, theft, and loss of information.

APPENDIX 5 DATA RETENTION AND DESTRUCTION SCHEDULE Retention of records in Send The Right Message Employment Staff and volunteer records should be retained for six years after the end of employment but need only to contain sufficient information to provide a reference (e.g. training and disciplinary records). Copies of any reference should be retained for six years after the reference request. Director's files should be kept for six years.	
Application form	Duration of employment, destroy when employment ends
References received	Duration of employment, destroy when employment ends
Sickness and maternity records	Six years from the end of employment
Annual leave records	Six years from the end of employment
Unpaid leave/special leave records	Six years from the end of employment
Records relating to an injury or accident at work	12 years
References given/information to enable a reference to be provided	Six years from the end of employment
Recruitment and selection material (unsuccessful candidates)	Six months after recruitment is finalised
Disciplinary records	Six years after employment has ended
Statutory maternity pay records, calculations and certificates	Retain while employed and for seven years after employment has ended
Redundancy details, calculation of payments and refunds	Seven years from the date of redundancy

Note: if an allegation has been made about the member of staff, volunteer or trustee, the staff record should be retained until they reach the normal retirement age or for ten years, if that is longer. E.g. around Safeguarding.	
DBS checks	
Record disclosure reference numbers. and date of the check and return to the volunteer or staff member.	
Safeguarding concern recording forms	
All safeguarding concern forms and related information should be kept for ten years. If the record relates to children and young people, it must be kept until they are 21 years old before destruction.	
Financial records	
Income tax and NI returns, income tax records and correspondence with HMRC	Six years (public-funded companies)
Payroll records (also overtime, bonuses, expenses)	Not less than six years after the end of the financial year to which they relate
Corporate	
Employers liability certificate	40 years
Insurance policies	Permanently
Certificate of incorporation	Permanently
Minutes of Board of Trustees	Permanently
Memorandum of association	Original to be kept permanently
Articles of association	Original to be held permanently
Variations to the governing documents	Original to be stored permanently

Statutory registers	Permanently
Membership records	20 years from the commencement of membership register
Rental or hire purchase agreements	Six years after expiry
Others	
Deeds of title	Permanently
Leases	12 years after the lease has expired
Accident Books	Three years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21).
Health and safety policy documents	Retain until superseded
Assessment of risks under health and safety legislation	Retain until superseded