Data Protection Policy and Procedure

The purpose of this policy is to enable Sundial Centre for Education on Harmful Practices (Sundial) to:

- comply with the law in respect of the data it holds about individuals;
- follow good practice;
- protect Sundial's staff, consultants, contractors, volunteers, members, service users and other individuals
- protect Sundial from the consequences of a breach of its responsibilities.

1. Legal Framework

Data Protection is important, not because it is about protecting data, but because it is about protecting people. People can be harmed if their data is misused, or if it gets into the wrong hands, through poor security or through careless disclosures. They can also be harmed if their data is inaccurate or insufficient and decisions are made about them, or about what services to provide to them on the basis of this data.

The General Data Protection Regulations 2018 regulates the collection, storage, use and disclosure of information about individuals by organisations. Any organisation that keeps information about individuals must comply with the act. The Act applies to *personal data* - information about identifiable living individuals that is:

- Held on computer or any other automated system
- Held in a *relevant filing system* (a paper system such as client records system, or a set of files on service users that is organised alphabetically by the name of the person or some other identifier such as case number)
- Intended to go onto computer or into a relevant filing system

2. Good practice principles

The Data Protection Act sets out six enforceable principles of good practice. These principles are that the data must be:

i) Processed lawfully
ii) Collected for a specific, explicit and legitimate purpose
iii) Adequate, relevant and limited to what is necessary

iv) Kept accurately and, where necessary, kept up to date
v) Kept for no longer than is necessary
vi) Processed in a manner that ensures appropriate security

3. Policy Statement

Sundial needs to collect and use personal data (see paragraph below) about our service users, employees, volunteers and other individuals, who are referred to in the Act as "data subjects" to carry out our business effectively and provide high quality services. We hold information about data subjects for service provision, administrative, personnel management, and membership management purposes.

Sensitive personal data

The Act defines "sensitive personal data" as personal data consisting of information as to racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; membership of a trade union; physical or mental health or condition; sexual life; the commission or alleged commission of any offence or any proceedings for any offence committed or alleged to have been committed, including the disposal of such proceedings or the sentence of any court in such proceedings.

The purpose for which we hold sensitive personal data about data subjects is for use solely for the aims of the charity. This includes but is not limited to: the provision of services to members and service users, assessing suitability and fitness for work, administering sick pay and sick leave, absence control, maternity leave and pay, parental leave, paternity leave and pay, adoption leave and pay, safe environment, complying with our obligations under the Disability Discrimination Act.

Statutory purposes

In addition to the purposes outlined above, we may collect, hold and process data including sensitive personal data if it is necessary to do so for compliance with any statutory duty with which we are required to comply or to prevent a criminal offence.

Marketing activities

Sundial will comply with the terms of the Act, and with other relevant legislations such as the Privacy and Electronic Communications (EC Directive) Regulations 2003, in relation to its marketing activities. Direct marketing refers not only to selling products and services to individuals, but also includes promotional activities. All individuals, without exception, have the right to prevent or stop their personal information being used for direct marketing. Sundial will state how personal information will be used and how individuals will be contacted.

4. Related Headway policies/procedures, resources:

- Data Audit 2018
- Service Level Agreement

5. Data Protection Procedure

The following procedure is designed to ensure that Sundial has mechanisms in place to ensure the principles of the General Data Protection Regulations 2018 are adhered to. This section provides guidance to all staff, consultants, contractors and volunteers including trustees, on their obligations in respect of accessing, holding or using personal information during the course of their employment or volunteering, such as service user information and information relating to other members of staff, consultants, contractors or volunteers. It applies to all employees and volunteers. Those managing others should take particular notice of content, however, since they may have additional responsibilities under the Act.

Sundial will ensure that:

- there is someone with specific responsibility for data protection within the organisation
- all personal information collected will be factual and objective
- all those who manage and handle personal information understand the requirements of the Act and their responsibilities under it
- all those who manage and handle personal information are appropriately trained and supervised to do so
- the methods of handling personal information are regularly audited, reviewed and evaluated

6. Responsibilities

This policy applies to all staff, consultants, contractors, volunteers, and Trustees or Board of Trustees or Management Committees. The procedure aims to set out the steps by which personal data is collected, the requirements to ensure records are completed appropriately and the requirements for the handling, storage and destruction of records.

The Trustees have overall responsibility for compliance with the Act, including registration and regular monitoring. The Trustees delegate compliance on a practical level insofar as service user information is concerned and compliance on all employee data as appropriate.

6.1 Senior Staff member/Trustees

Responsible for ensuring that all records are maintained and stored in accordance with the policy and procedure in place and adhered to. Also responsible for destruction of records in accordance with policy and procedure.

6.2 Staff, Consultants, Contractors, Volunteers and other individuals:

All other staff, consultants, contractors, volunteers and other individuals associated with Sundial are responsible for compliance with the policy and procedure.

7. Staff Responsibilities

7.1 Senior Person

- To ensure that all staff, consultants, contractors, volunteers and service users have access to and are aware of this policy.
- To ensure that safeguards are in place to protect the interests of the service user.

7.2 All staff /consultants/ contractors/volunteers / trustees

To be aware of and adhere to this policy and procedure.

The Act requires that all personal information is kept confidential and secure. You must therefore:

- observe all instructions or directions given to you in respect of confidentiality and security of information;
- comply with all confidentiality obligations contained within your employment/ volunteering contract;
- keep workstations locked when away from desks and keep any documentation containing personal information out of sight overnight, not left out on desks;
- inform the organisation of any changes to your personal details to enable us to comply with the Act and to aid the smooth running of the business;
- keep all lockable cabinets and drawers in which personal information is stored locked when not in use; and
- treat any documentation taken out of our offices in the same way as when in the office, ensuring security of information.

Information held must be accurate, relevant and not excessive. If you need to hold or collect personal information you must therefore:

- ensure that all documents containing personal information are up to date and held for no longer than is necessary; you should be aware that what constitutes “no longer than necessary” will vary and takes into consideration the type of information and the purpose to which it is to be put;

- ensure that all documentation or other materials no longer required containing personal information are disposed of via secure destruction bins / shredders; and
- ensure that the content of personal information held is objective; the information you hold may be disclosed to the individual concerned.

Staff/consultants/contractors/volunteers/trustees need to ensure that only the "authorised processing of information" takes place. In practice this means that:

- information held and used must be required in the course of your employment or volunteering ; you must not access, gather or hold information which you do not genuinely need in order to carry out your role;
- access to personal information should be refused to individuals both internally and externally (without the consent of the data subject), unless it is clear that these individuals are authorised to access or process such information.

Except in certain limited circumstances, it is a criminal offence to obtain or disclose personal data or the information contained in personal data or to procure the disclosure of the information contained in personal data to another person without the consent of the person responsible for our compliance with the Act.

This means that:

- you may be committing a criminal offence if you do not process data in an authorised manner, whether you do so deliberately or because you have not taken sufficient care;
- you must comply with the terms of this Policy and with any further instructions or directions given to you;
- if you have any doubts or queries concerning your access to, or use of, personal data in the course of your employment or volunteering, you should seek guidance from the Data Protection Officer.

7.3 Sundial staff / volunteer training

All staff and others responsible for the management of personal data must have had training in the provisions of the General Data Protection Regulations 2018. All staff, consultants, contractors and volunteers working with personal data need to be reminded that it is a disciplinary offence to disclose confidential information to unauthorised individuals

8. Audit Plan

The Chief Executive Officer / senior person (currently Kate Agha) will monitor adherence of the policy and report findings to the Trustees.

9. Third Parties

We do not normally have the need to provide information we retain on any of our staff, consultants, contractors, volunteers or service users to organisations or individuals outside Sundial other than to Social Services and other related statutory bodies during the course of client reviews and to any company which Sundial employs to undertake its administration processes. When we are asked to participate in client reviews, for referral purposes, or for any other reason we intend to pass information to another agency, we will always inform the client, volunteer or staff member of the information we intend to reveal and seek their agreement.

Data may also be disclosed to others at a data subject's own request, under the Freedom of Information Act.

10. Access and correction

The General Data Protection Regulations 2018 gives individuals a general right of access to the personal data which relates to them. For a copy of the information (to which the act applies) held about them an individual can write to:

Kate Agha, Chief Executive Officer, Unit 7685, PO Box 6945 London W1A 6US

The individual will be asked to verify their identity by sending Sundial a copy of their passport.

Sundial reserves the right to charge the maximum fee payable in terms of the General Data Protection Regulations for providing this information.

If the data held is inaccurate the individual is entitled to ask for it to be amended.

11. Retention of Data relating to service users, employment or volunteering

We observe and abide by the Employment Practices Data Protection Code which is not enforceable by law but which provides guidance on best practice for employers in obtaining and processing information about employees

The categories of information which we will hold and the minimum time for which we will normally hold it will be as follows:

Individuals	**What data?**	**How long will we retain the data?**

Staff, consultants, contractors, volunteers, trustees, young people and attendees at training sessions	Photographs	Life of charity
Staff, consultants, contractors, volunteers, trustees and young people	Films	Life of charity
People on newsletter list	Email addresses	Life of charity unless unsubscribe
Staff and volunteers	Name, address, email, telephone numbers	6 years after leaving Sundial
Trustees	Name, address, email, telephone numbers	6 years after leaving Sundial
Sponsors and donors	Name, address, email, telephone numbers	Life of charity
Staff and volunteers	CVs and employment information	1 year for unsuccessful candidates; 6 years after staff/volunteers leave Sundial
Kate Agha	Payroll	6 years after leaving Sundial
Staff and trustees	DBS	Life of charity (in case of criminal investigation)
Staff, volunteers, consultants and contractors	Bank details	6 years after leaving Sundial
FGM survivors	Survivors' stories	Life of charity
FGM survivors/families	Child protection notes	Life of charity (in case of criminal allegation; civil claim possible until children reach age 24)

The purpose for which we hold any information about data subjects after the end of employment (as indicated in the above table) is for use solely for any residual employment related matters including but not limited to the provision of job references, processing applications for re-employment, matters relating to retirement benefits and allowing us to fulfil contractual or statutory obligations.

12. Photographs and filming

We will request consent before taking any photographs or films of individuals and will let them know how any photographs and films will be used.

13. Electronic communications

We monitor electronic communications by employees, volunteers and service users including websites, to ensure that these systems are used in accordance with our internet policies.

14. Employee obligations

In the course of our business, we collect and process personal information, including that relating to service users, employees, contacts, and suppliers to which you may have access in the course of your employment. It is our policy to ensure compliance by our employees with the Regulations.

We reserve the right to implement the Disciplinary Policy and Procedure against anyone who fails to comply with the procedures set out in this policy and procedure.

15. References

Providing a reference involves the disclosure of personal data of the individual who is the subject of the reference. So that we can ensure we protect our employees' and volunteers data no references (whether to prospective employers or other institutions) should be given on behalf of the organisation without prior authorisation from the Chief Executive Officer / Board of Trustees.

This Policy does not prevent any employee giving a reference in a personal capacity but employees should make clear that such references are personal and not on behalf of the organisation and, if the reference is given on paper, that neither the organisation's name, address nor logo appear on the paper.

It is our policy to provide copies of references given by us to the individual who is the subject of the reference if they request a copy.

16. Marketing

We will inform individuals how and by whom their information will be used. This will include telling them that information may be shared with other organisations with similar aims and objectives. When we collect information from people and are in direct contact with them such as in a phone call or via our website we will provide an immediate opportunity for them to opt out of further contact and to let us know how they would like to be contacted.

We will not make unsolicited **phone calls** to any organisation or individual who has told us they do not want our calls, or to any number on the Telephone Preference Service list.

We will not send unsolicited marketing by **electronic mail** to individuals without first getting their permission.

In all our marketing we will identify who we are and provide contact details, postal address, email address and contact telephone number so that the recipient can contact us.

If an individual decides they no longer want to receive marketing, we will deal with their request promptly

17. Contacts for further advice on data protection

Information Commissioner's Office
Provides comprehensive information on the General Data Protection Regulations and the legal requirements for compliance via web site www.ico.gov.uk.

18. Data Security Breach Procedure

In the event of a data security breach being identified it should be reported as soon as possible (no more than 24 hours) to the Chief Executive Officer or most senior available staff member, as well as at least two trustees, including the Chair person.

18.1 Containment and recovery

- The Chief Executive Officer will make a decision as to who should take the lead on investigating the breach and ensure they have the appropriate resources.
- This person will establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise, e.g. isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door.
- This person will establish whether there is anything that can be done to recover any losses and limit the damage the breach may cause. As well as the physical recovery of equipment, this could involve the use of back up tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
- Where appropriate, the police should be informed.

18.2 Assessment of ongoing risk

The following should be established:

- What type of data is involved
- How sensitive is it
- If data has been lost or stolen, are there any protections in place such as encryption
- What has happened to the data
- Regardless of what has happened to the data, what could the data tell a third party about the individual
- How many individuals' personal data are affected by the breach
- Who are the individuals whose data has been breached
- What harm can come to those individuals
- What are the wider consequences
- If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

18.3 Notification of breach

- Are there any legal or contractual requirements? In certain circumstances, service providers have an obligation to notify the Data Protection Commissioner' in other areas sector specific rules may lead you towards issuing a notification.
- Can notification help you meet your security obligations with regard to the seventh data protection principle?
- Can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act on the information you provide to mitigate risks, for example by cancelling a credit card or changing a password?
- If a large number of people are affected, or there are very serious consequences, you should inform the Information Commissioning Office.
- Consider how notification may be made appropriate for particular groups of individuals, for example, if you are notifying children or vulnerable adults.
- Have you considered the dangers of 'over notifying'. Not every incident will warrant notification.
- Make sure you notify the appropriate regulatory body. A sector specific regulator may require you to notify them of any type of breach but the ICO should only be notified when the breach involves personal data
- There are a number of different ways to notify those affected so consider using the most appropriate one.
- Your notification should at the very least include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to respond to the risks posed by the breach
- When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what you are willing to do to help them

- Provide a way in which they can contact you for further information or to ask you questions about what has occurred – this could be a helpline number or a web page, for example.

18.4 Evaluation and response

It may be found that existing procedures could lead to another breach and you will need to identify where improvements can be made. The following points will assist you:

- Make sure you know what personal data is held and where and how it is stored.
- Establish where the biggest risks lie.
- Risks will arise when sharing with or disclosing to others. You should make sure not only that the method of transmission is secure but also that you only share or disclose the minimum amount of data necessary.
- Identify weak points in your existing security measures such as the use of portable storage devices or access to public networks
- Monitor staff/consultants/contractors/volunteers/trustees awareness of security issues and look to fill any gaps through training or tailored advice
- Consider whether you need to establish a group of technical and non-technical personnel who discuss 'what if' scenarios – this would highlight risks and weaknesses as well as giving staff/ consultants/contractors/volunteers/trustees at different levels the opportunity to suggest solutions
- It is recommended that at the very least you identify a group of people responsible for reacting to reported breaches of security

---

This policy was adopted by the Trustees on

…… (date)

On behalf of the Trustees:

…….. (signed)

This policy will be reviewed annually by the Trustees; next renewal date is:

……