holistic approaches to health & wellbeing

Data Protection Policy

This policy applies to all employees, self-employed staff, clients, children & young people, parents/carers and volunteers of The Sadie Centre.

Introduction

The purpose of this policy is to enable The Sadie Centre to:

- Comply with the law in respect of the data it holds about individuals
- Follow good practice
- Protect employees, self-employed staff, clients, children & young people, parents/carers, volunteers and other individuals
- Protect The Sadie Centre from the consequences of a breach of its responsibilities

The Data Protection Act (DPA 2018)

The Data Protection Act gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.
The Act works in two ways. Firstly, it states that anyone who processes personal information must comply with eight principles, which make sure that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with the rights of Data Subjects
- Secure
- Not transferred to other countries without adequate protection

The second area covered by the Act provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records.

Policy Statement

The Sadie Centre will:

- Comply with both the law and good practice
- Respect individuals' rights
- Be open and honest with individuals whose data is held

- Provide support as and when required for employees and volunteers who handle personal data, so that they can act confidently and consistently.

The Sadie Centre recognises that its priority under the Data Protection Act is to avoid causing harm to individuals. Information about employees, volunteers and clients will be used fairly, securely and not disclosed to any person unlawfully.
Secondly, the Act aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, The Sadie Centre will seek to give individuals as much choice as is possible and reasonable oversight of data is held and how it is used.

The Sadie Centre is the Data Controller and if required, is registered under the Data Protection Act 2018. All processing of personal data will be undertaken in accordance with the data protection principles.

Definitions

The Data Subject is the individual whose personal data is being processed. Examples include:

- Employees – current and past
- Self Employed – current and past
- Volunteers
- Job applicants
- Service users
- Suppliers

Processing means the use made of personal data including:

- Obtaining and retrieving
- Holding and storing
- Making available within or outside the organisation
- Printing, sorting, matching, comparing, and destroying

The Data Controller is the legal 'person', or organisation, that decides why and how personal data is to be processed. The data controller is responsible for complying with the Data Protection Act.

The Privacy Officer (Centre Director) is the name given to the person in organisations who is the central point of contact for all data compliance issues.

Responsibilities

The Board of Trustees/Management team recognises its overall responsibility for ensuring that The Sadie Centre complies with its legal obligations.

The Privacy Officer (Centre Director) is currently Roberta Meldrum/Jenny Flynn who has the following responsibilities:

- Briefing the board/committee on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other employees/volunteers on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Handling subject access requests
- Approving unusual or controversial disclosures of personal data
- Electronic security
- Approving data protection-related statements on publicity materials and letters

Each employee and volunteer at The Sadie Centre who handles personal data will comply with the organisation's operational procedures for handling personal data (including induction and training) to ensure that good Data Protection practice is established and followed.

All employees and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

Significant breaches of this policy will be handled under The Sadie Centre disciplinary procedures.

Security

This section of the policy only addresses security issues relating to personal data. It does not cover security of the building, business continuity or any other aspect of security.

Any recorded information on clients, volunteers and employees will be:

- Kept in locked cabinets.
- Protected by the use of passwords if kept on computer.
- Destroyed confidentially if it is no longer needed.

Access to information on the main organisation database/server is controlled by a password and only those needing access are given the password. Employees and volunteers should be careful about information that is displayed on their computer screen and make efforts to ensure that no unauthorised person can view the data when it is on display.
Notes regarding personal data of clients should be shredded or destroyed.

Data Recording and Storage

The Sadie Centre has databases/spreadsheets holding basic information about clients, employees and volunteers. This is backed-up by Courtland Services Partnership Limited (our IT Services provider).

The Sadie Centre will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

- The database system is reviewed and re-designed, where necessary, to encourage and facilitate the entry of accurate data.
- Data on any individual will be held in as few places as necessary, and all employees and volunteers will be discouraged from establishing unnecessary additional data sets.
- When 'on the move' paperwork to be locked in the boot of the car.
- Secure lockable filing cabinet to be used when storing paperwork away from the Centre.
- Effective procedures are in place so that all relevant systems are updated when information about any individual changes.
- Employees and volunteers who keep more detailed information about individuals will be given additional guidance on accuracy in record keeping.
- Data will be corrected if shown to be inaccurate.

The Sadie Centre stores archived paper/electronic records of clients, employees and volunteers securely in lockable rooms.

Data Retention

The Centre abides by the Records Management Code of Practice 2021.

The Data Schedule of Retention is below:

Record Type	**Retention Period**
Financial Records	7 Years
Client Adult Clinic Records	8 Years
Children's Clinic Records	Until the child is 25 years of age
Digital Client Records	Continual retention.
Adult Safeguarding Records	8 Years
Children's Safeguarding Records	Until the child is 25 years of age
Incidents – serious incidents requiring investigation	20 Years

Thereafter records are discarded with safe disposal.

Information Security Policy

The Centre handles sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organisation.

The Centre commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end the Centre Directors are committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.

Employees handling Sensitive cardholder data should ensure:

- Handle Centre and cardholder information in a manner that fits with their sensitivity;
- Limit personal use of The Centre information and telecommunication systems and ensure it doesn't interfere with your job performance;
- The Centre reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;
- Do not use e-mail, internet and other Centre resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Do not disclose personnel information unless authorised;
- Protect sensitive cardholder information;
- Keep passwords and accounts secure;
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval;
- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended;
- Information security incidents must be reported, without delay, to the individual responsible for incident response locally – Please find out who this is.

We each have a responsibility for ensuring our Centre's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager.

Access to the sensitive cardholder data

All Access to sensitive cardholder should be controlled and authorised. Any Job functions that require access to cardholder data should be clearly defined.

- Any display of the card holder should be restricted at a minimum of the first 6 and the last 4 digits of the cardholder data.
- Access rights to privileged user ID's should be restricted to least privileges necessary to perform job responsibilities
- Privileges should be assigned to individuals based on job classification and function (Role based access control)
- Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to employees that have a legitimate need to view such information.
- No other employees should have access to this confidential data unless they have a genuine business need.

- If cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained as detailed in Appendix B.
- The Sadie Centre will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the for the cardholder data that the Service Provider possess.
- The Sadie Centre will ensure that a there is an established process including proper due diligence is in place before engaging with a Service provider.
- The Sadie Centre will have a process in place to monitor the PCI DSS compliance status of the Service provider.

Protect Data in Transit

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.

- Card holder data (PAN, track data etc.) must never be sent over the internet via email, instant chat or any other end user technologies.
- If there is a business justification to send cardholder data via email or via the internet or any other modes then it should be done after authorisation and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, IPSEC, GSM, GPRS, Wireless technologies etc.,).
- The transportation of media containing sensitive cardholder data to another location must be authorised by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

Access to Data

All clients have the right to request access to all information stored about them. Any subject access requests will be handled by the Privacy Officer (Centre Director) within the required time limit (within 30 working days of receiving the request).

Subject access requests must be in writing. All employees and volunteers are required to pass on anything which might be a subject access request to the Privacy Officer (Centre Director) without delay.

Where the individual making a subject access request is not personally known to the Privacy Officer (Centre Director), their identity will be verified before handing over any information.

The required information will be provided in easy to use formats e.g. PDF, XLS & CSV.

The Sadie Centre will provide details of information to clients who request it, unless the information may cause harm to another person.

Employees have the right to access their file to ensure that information is being used fairly. If information held is inaccurate, the individual must notify the Privacy Officer (Centre Director) so that this can be recorded on file.

Transparency

The Sadie Centre is committed to ensuring that in principle, Data Subjects are aware that their data is being processed and:

- For what purpose it is being processed
- What types of disclosure are likely
- How to exercise their rights in relation to the data

Consent

Consent will normally not be sought for most processing of information about clients and employees, although employees' details will only be disclosed for purposes unrelated to their work with The Sadie Centre (e.g. financial references) with their consent.

Information about clients will only be made public with their consent, or in the case of Safeguarding or a medical emergency (this includes photographs).

'Sensitive' data about children/young people will be held only with the knowledge and consent of the individual's parent/guardian/carer.

Consent should be given in writing, although for some services it is not always practicable to do so. In these cases, verbal consent will always be sought to the storing and processing of data. In all cases it will be documented on the database that consent has been given.

The Sadie Centre acknowledges that, once given, consent can be withdrawn, but not retrospectively. There may be occasions where The Sadie Centre has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn.

Direct Marketing

The Sadie Centre will treat the following unsolicited direct communication with individuals as marketing:

- Seeking donations and other financial support
- Promoting via our Constant Contact newsletters
- Promoting sponsored events and other fundraising exercises

Whenever data is first collected which might be used for any marketing purpose, this purpose will be made clear, and the Data Subject will be given a clear opt-out. If it is not possible to give a range of options, any opt-out which is exercised will apply to all Constant Contact marketing. Constant Contact does not have a policy of sharing lists, obtaining external lists or carrying out joint or reciprocal mailings.

Whenever e-mail addresses are collected, any future use for marketing will be identified, and the provision of the address made optional.

Employee/volunteer training and acceptance of responsibilities

All employees/volunteers who have access to any kind of personal data will be given copies of all relevant policies and procedures during their induction process, and the operational procedures for handling personal data. All employees will be expected to adhere to all these policies and procedures.

- Data Protection will be included in the induction training for all
- Pro-Action is available when necessary for employees/volunteers to explore Data Protection issues. The Centre is a registered organisation with the Information Commissioner's Office which can also offer guidance as and when required.

Client Data Protection

All personal data shall be obtained, maintained, stored, used and shared only in strict accordance with the Data Protection Act 2018.

Information relating to individuals supported by The Sadie Centre through the work of the organisation will be dealt with in the following manner:

- Tutors are expected to destroy attendance records within 12 months of the course taking place
- All other information will be kept securely for no longer than needed
- Information that is of vital importance to the future protection of an individual or a child/young person will be securely archived and stored as long as express agreement is obtained from the data subject (or as felt appropriate)

All personal data must be protected by appropriate security measures to safeguard against unauthorised or unlawful processing of personal data (e.g. locked filing cabinet). All employees/volunteers and representatives of The Sadie Centre must:

- Only access and use data that is relevant to and necessary to the performance of their job function
- Make yourself familiar with The Sadie Centre data protection policy and procedures

Confidentiality

During the course of your employment/volunteering with The Sadie Centre you may have access to and be entrusted with information in respect of children/young people, plus the business and financing of the centre and its affairs, all of which is, or may be confidential.

You shall not (except in the proper course of your duties) during or after the period of your employment/volunteering divulge to any person, or otherwise make use of (and shall use your best endeavours to prevent the publication or disclosure of) any confidential information concerning any children/young people or the business and finances of the centre, or any such confidential information concerning any of its clients.

System and Password Policy

All users, including contractors and vendors with access to The Sadie Centre systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

- A system configuration standard must be developed along industry acceptable hardening standards (SANS, NIST, ISO).
- System configurations should be updated as new issues are identified (as defined in PCI DSS requirement 6.1).
- System configurations must include common security parameter settings.
- The systems configuration standard should be applied to any news systems configured.
- All vendor default accounts and passwords for the systems have to be changed at the time of provisioning the system/device into The Sadie Centre network and all unnecessary services and user/system accounts have to be disabled.
- All unnecessary default accounts must be removed or disabled before installing a system on the network.
- Security parameter settings must me set appropriately on System components.
- All unnecessary functionality (scripts, drivers, features, subsystems, file systems, web servers etc.,) must be removed.
- All unnecessary services, protocols, daemons etc., should be disabled if not in use by the system.
- Any insecure protocols, daemons, services in use must be documented and justified.
- All users with access to card holder data must have a unique ID.
- All users must use a password to access The Sadie Centre network or any other electronic resources.
- All user ID's for terminated users must be deactivated or removed immediately.
- The User ID will be locked out if there are more than 5 unsuccessful attempts. This locked account can only be enabled by the system administrator. Locked out user accounts will be disabled for a minimum period of 30 minutes or until the administrator enables the account.
- All system and user level passwords must be changed on at least a quarterly basis.
- A minimum password history of four must be implemented.
- A unique password must be setup for new users and the users prompted to change the password on first login.
- Group, shared or generic user account or password or other authentication methods must not be used to administer any system components.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively.
- All non-console administrative access will use appropriate technologies like ssh, vpn etc. or strong encryption is invoked before the administrator password is requested.
- System services and parameters will be configured to prevent the use of insecure technologies like telnet and other insecure remote login commands.
- Administrator access to web-based management interfaces is encrypted using strong cryptography.
- The responsibility of selecting a password that is hard to guess generally falls to users. A strong password must:

    a) Be as long as possible (never shorter than 6 characters).

b) Include mixed-case letters, if possible.
c) Include digits and punctuation marks, if possible.
d) Not be based on any personal information.
e) Not be based on any dictionary word, in any language.

- If an operating system without security features is used (such as DOS, Windows or MacOS), then an intruder only needs temporary physical access to the console to insert a keyboard monitor program. If the workstation is not physically secured, then an intruder can reboot even a secure operating system, restart the workstation from his own media, and insert the offending program.
- To protect against network analysis attacks, both the workstation and server should be cryptographically secured. Examples of strong protocols are the encrypted Netware login and Kerberos.

Anti-virus policy

- All machines must be configured to run the latest anti-virus software as approved by The Centre. The preferred application to use is Webroot Anti-Virus software, which must be configured to retrieve the latest updates to the antiviral program automatically on a daily basis. The antivirus should have periodic scanning enabled for all the systems.
- The antivirus software in use should be cable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits)
- All removable media (for example floppy and others) should be scanned for viruses before being used.
- All the logs generated from the antivirus solutions have to be retained as per legal/regulatory/contractual requirements or at a minimum of PCI DSS requirement 10.7 of 3 months online and 1 year offline.
- Master Installations of the Antivirus software should be setup for automatic updates and periodic scans.
- End users must not be able to modify and any settings or alter the antivirus software.
- E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain virus.

Remote Access policy

- It is the responsibility of the Organisation employees, contractors, vendors and agents with remote access privileges to the Organisation's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the Organisation.
- Secure remote access must be strictly controlled. Control will be enforced by two factor authentication via one-time password authentication or public/private keys with strong pass-phrases.
- Vendor accounts with access to the organisation network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required.

- Remote access connection will be setup to be disconnected automatically after 30 minutes of inactivity.
- All hosts that are connected to the Organisation internal networks via remote access technologies will be monitored on a regular basis.
- All remote access accounts used by vendors or 3rd parties will be reconciled at regular interviews and the accounts will be revoked if there is no further business justification.
- Vendor accounts with access to the Organisation network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required.

Third party access to card holder data

- All third-party companies providing critical services to the organisation must provide an agreed Service Level Agreement.
- All third-party companies providing hosting facilities must comply with the organisation's Physical Security and Access Control Policy.
- All third-party companies which have access to Card Holder information must:

  1. Adhere to the PCI DSS security requirements.
  2. Acknowledge their responsibility for securing the Card Holder data.
  3. Acknowledge that the Card Holder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law.
  4. Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure.
  5. Provide full cooperation and access to conduct a thorough security review after a security intrusion to a Payment Card industry representative, or a Payment Card industry approved third party.

Wireless Policy

- Installation or use of any wireless device or wireless network intended to be used to connect to any of the organisation networks or environments is prohibited.
- A quarterly test should be run to discover any wireless access points connected to the organisation network.
- Usage of appropriate testing using tools like net stumbler, kismet etc. must be performed on a quarterly basis to ensure that:
- Any devices which support wireless communication remain disabled or decommissioned.
- If any violation of the Wireless Policy is discovered as a result of the normal audit processes, the security/privacy officer or any one with similar job description has the authorisation to stop, cease, shut down, and remove the offending device immediately.

If the need arises to use wireless technology, it should be approved by the organisation and the following wireless standards have to be adhered to:

1. Default SNMP community strings and passwords, passphrases, Encryption keys/security related vendor defaults (if applicable) should be changed immediately after the installation of the device and if anyone with knowledge of these leaves the organisation.
2. The firmware on the wireless devices has to be updated accordingly as per vendors release schedule
3. The firmware on the wireless devices must support strong encryption for authentication and transmission over wireless networks.
4. Any other security related wireless vendor defaults should be changed if applicable.
5. Wireless networks must implement industry best practices (IEEE 802.11i) and strong encryption for authentication and transmission of cardholder data.
6. An Inventory of authorised access points along with a business justification must be maintained.

Appendix A – Agreement to Comply Form – Agreement to Comply with Information Security Policies

_____

Employee Name (printed)

_____

Employee Signature

_____

Job Title

I agree to take all reasonable precautions to assure that organisation internal information, or information that has been entrusted to the Organisation by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with the Organisation, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal manager who is the designated information owner.

I have access to a copy of the Data Protection/Information Security Policies, I have read and understand these policies, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the policies and other requirements found in the organisation's security policy. I understand that

non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of information security policies to the designated security/privacy officer.

_____

Date

Appendix B

Asset/Device Name	Description	Owner	Approved User Location

List of Service Providers

Name of Service Provider	Contact Details	Services Provided	PCI DSS Compliant	PCI DSS Validation Date