SaferPlaces
Domestic Abuse Support Services

Information Governance Policy

Introduction

We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the DPO (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

CONTENTS

Definitions

Business purposes

The purposes for which personal data may be used by us:

Personnel, administrative, financial, regulatory, payroll and business development purposes.

Business purposes include the following:

- Compliance with our legal, regulatory and corporate governance obligations and good practice
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- Ensuring business policies are adhered to (such as policies covering email and internet use)
- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information
- Investigating complaints
- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
- Monitoring staff conduct, disciplinary matters
- Marketing our business
- Providing support services

Personal data	Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts. *Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV, Personal details of clients including details of experiences of domestic abuse.*
Sensitive personal data	*Personal data about an individual's racial or ethnic origin, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.*

Scope

This policy applies to all staff. You must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

The Data protection policy is overseen and maintained by the DPO Allison Gardner. It is the responsibility of the DPO to oversee the day to day implementation of the policy and supporting processes, the Policy is updated and maintained to the standard outlined in the ISO 9001 management system.

Our procedures

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening or it is processed under another suitable legal basis.

The DPO's responsibilities:

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by Saferplaces
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing
- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- The DPO will coordinate with the communications officer to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

Responsibilities of the ICT Manager

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly

The processing of all data must be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

Our Terms of Business contains a Privacy Notice to clients on data protection.

The notice:

- Sets out the purposes for which we hold personal data on clients and employees
- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers
- Provides that clients have a right of access to the personal data that we hold about them

Sensitive personal data

In most cases where we process sensitive personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure Health and Safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive and operate procedures to support this aim. We will also ensure that data is processed solely for the purpose it was collected unless the individual concerned has explicitly agreed to further processing for an alternative purpose.

Individuals may ask that we correct inaccurate personal data relating to them. If you identify that personal information held about you is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO, Allison Gardner.

Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the DPO so that they can update your records.

Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords.
- Data stored on memory sticks must be locked away securely when they are not being used. Memory sticks containing personal data must be adequately encrypted as referenced in the ICT policy manual.
- The DPO must ratify any cloud platform used to store data
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines below.

Data Category	Retention Period (in years)	Priority	Physical Records Necessary?
Company and Governance	Indefinite	1	Yes
Financial Information	7	1	No
Human Resources	6	2	No
Medical Records	None (after exit)	1	No
Accidents & Incidents	Indefinite	1	Yes
General Health & Safety	3	2	No
Client Files	2	2	No
General	1	3	No

Administration

Detailed definition of data categories

Company & Governance / Contracts & Leases – Indefinite Retention – Physical copies must be retained – Priority 1

In this context company and governance data include memorandum and articles of association, minutes from meetings of the board of directors and any data that details significant change in company practice or operation.

This is a legal requirement and therefore justified

Financial Information –– Physical copies must be retained – Priority 1

In this context financial information refers to information regarding monies received to Safer Places from any other body or individual and monies paid by Safer Places to any other body or individual, records of all assets and liabilities and any regulatory documentation pertaining to Safer Places financial practices for any period of time.

This is a legal requirement and therefore justified

Human Resources / Staff Files – 6 Year Retention Period – Priority 2

In this context Human Resources and Staff files consists of any documentation pertaining to staff members in any and all capacities including all personal information such as addresses, contact information or details of employment.

This is a legal requirement and therefore justified

Medical information – Immediate removal at end of association – Priority 1

In this context medical information includes any details on the health of any individual who has been in association with Safer Places; these may include medical records, medical history or details of medication. This includes staff and other non-client affiliates.

We are required to store this information on current members of staff and clients in case of an emergency. Records will be removed when staff leave or clients leave.

Accidents & Incidents / Occupational Health – Indefinite Retention – Physical copies must be retained - Priority 1

In this context Accidents or Incidents or Data held on occupational health include any data where any form of mental or physical injury has or could potentially have occurred in the work place these may include incident reports and accident logs.

This is a legal requirement and therefore justified

General Health & Safety – 3 Year Retention – Priority 2

In this context data on Health & Safety include any data recorded about Health and Safety in general that do not relate to a specific incident or accident, these may include health Safety checks or room inspections.

Safer Places feels 3 years is adequate retention of such information that may need to be associated to incidents/accidents or other important events. Given the minimal personal information stored on the form we do not deem this excessive.

Client Files / Client Records/Children's Files – 2 Year Retention Period – Priority 2

In this context client files include any data that is held about a client that pertains to a client's time spent within any and all Services offered by Safer Places, this will include any and all details of support received as well as information on the perpetrator of their abuse and any relevant details of activities whilst at Safer Places. This applies to information held on children.

Safer Places feels there is justification for holding this information for 2 years due to the high level of repeat victimisation within the domestic abuse sector, many of our clients repeatedly access many of our services over a period of many years, as such we improve our service and ability to support these clients by retaining such information, easing their access to our services. It also enables us to identify repeat offenders of domestic abuse.

General Administration – 1 Year Retention – Priority 3

In this context general administration includes any files held that include personal information about anyone that do not fall under any other category in this document and do not make up part of a person's file e.g. coffee morning attendance.

Safer Places feels that one year is sufficient to ensure it can call upon such information as statistics or to aid investigations to improve service delivery but ensures that details are not held for an excessive amount of time.

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the UK without first consulting the DPO.

Subject access requests

If you receive a subject access request, you should refer that request immediately to the DPO. We may ask you to help us comply with those requests.

Please contact the DPO if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

Processing data in accordance with the individual's rights

You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.

Training

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training is provided through in-house and through an online training platform on a regular basis.

It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.
- Completion of training is compulsory.

Data Sharing

It is the policy of Safer Places that any requests for information from non-statutory organisations must only be actioned where there is a genuine reason and an identified legal basis specified under GDPR guidelines[1].

Primarily sharing of information is done following the written agreement of the person to whom it pertains. Saferplaces may share data under another lawful

basis, where this is the case it will be processed under an information sharing agreement which will outline;

- What data will be shared
- Which organisations it will be shared with
- How it will be shared
- How the data subject's rights under GDPR will be upheld.

Some agencies have a statutory right to information and Safer Places must respond to requests from them.

All information given to statutory organisations can only be released with the authority of the DPO or member of SMT.

Safer Places will ensure the person to whom the information refers will be informed of the request.

All staff, trustees and clients have a right to view their personal file. Safer Places will provide data within 30 days in line with requirements under GDPR

[1]https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

Protecting Data in Transmission

Two important factors must be considered before sharing client data

Data should only be shared if at least one of the qualifying conditions have been met

- The individual has given consent
- Data is processed under an authorised information sharing agreement.
- Under conditions as specified within the Safeguarding policy and procedure

If you are uncertain whether or not you can share information, consult with your line manager and follow the processes as outlined in the Safeguarding Policy

It's important to note that emails are **not secure** and cannot be used to transmit client data without applying proper controls and protection, there are 2 stages to securing client data in transit as outlined below:

Secure Email

From information governance training you should have been made aware of how important it is to secure client personal data before it is sent externally via email. Safer Places uses the **CJSM (Criminal Justice System Secure Mail) network to send data securely**. If your line manager requested that you have access to this system, you will have received the details via your initial setup email, alternatively you can request access by emailing **helpdesk@saferplaces.co.uk.**

Encrypting Documents

Whilst sending documents via the CJSM, it is still critical the document is encrypted.

You can encrypt Microsoft office documents by following the below guidance - Safer Places uses the Office 2010 or later suite of office applications which support 128bit AES encryption through the in-build password protection mechanism

1. How to encrypt an office document - https://support.office.com/en-gb/article/Add-or-remove-protection-in-your-document-workbook-or-presentation-05084cc3-300d-4c1a-8416-38d3e37d6826
2. Password Protecting PDF.pdf

It's important that the password to unlock the file is communicated by **Phone** and not in the same or a subsequent email.

GDPR provisions

Where not specified previously in this policy, the following provisions will be in effect on or before 25 May 2018.

Privacy Notice - transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. The following are details on how we collect data and what we will do with it:

What information is being collected?	
Who is collecting it?	Safer Places
How is it collected?	Directly from clients with consent and input directly on to Safer Places systems,
Why is it being collected?	To provide support services pertaining to Safer Places core goal of supporting victims of domestic abuse. Safer Places also collects personal details on staff to ensure statutory compliance.
How will it be used?	Client Data is used exclusively to provide client lead support services. Where Safer Places may wish to use the data for an alternative purpose client consent will always be obtained.
Who will it be shared with?	No personal data may be passed to any person or organisation outside

	Safer Places without express consent. However, there are two exceptions to this; ▲ Where there is a risk to yourself or others ▲ Where there is a statutory legal requirement for Safer Places to provide the information
Identity and contact details of any data controllers	Allison Gardner PO BOX 2489 Harlow Essex
Details of transfers to third country and safeguards	-
Retention period	2 years for client data other data is stored in line with statutory requirements

Conditions for processing

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Justification for personal data

We will process personal data in compliance with all six data protection principles.

We will document the additional justification for the processing of sensitive data, and will ensure any biometric and genetic data is considered sensitive.

Consent

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free. Some technical limitations exist that means some data cannot be directly given in a machine readable format.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if a legitimate exemption applicable under GDPR guidelines applies. Where services are active it should be noted that requests to erase data may result in suspension of services provided.

Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all ICT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

International data transfers

No data may be transferred outside of the EEA without first discussing it with the DPO. **Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.**

Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary

- Maintain a register of compliance failures

- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures

Please refer to our Data Breach Policy for our reporting procedure.

Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

Compliance and Audit Table	
Owner of this policy	AG
Version Number	1.0
Date last reviewed	01/05/2018
Next routine review date	01/05/2019
Justification (Legal or Company)	Legal