



St Pauls Advice Centre

Data Protection Policy and Procedure

1.0 General

St Pauls Advice Centre records, processes and stores information about service users, staff, volunteers, contractors, suppliers and other individuals in order to carry out its day-to-day operations, meet its objectives and to comply with legal obligations.

We are committed to processing all personal information in accordance with the General Data Protection Regulation (GDPR), and any other relevant the data protection laws.

St Pauls Advice Centre has developed policies, procedures, controls and measures to ensure maximum and continued compliance with the data protection laws and principles, including staff training, procedure documents, audit measures and assessments. We operate a 'Privacy by Design' approach, assessing changes and their impact from the start and designing systems and processes to protect personal information.

St Pauls Advice Centre has identified that the organisation is both a Data Controller and a Data Processor.

2.0 Objectives

We are committed to ensuring that all personal data processed by St Pauls Advice Centre is done so in accordance with the data protection laws and its principles, along with any associated regulations and/or codes of conduct laid down by the Supervisory Authority and local law. We ensure the safe, secure, ethical and transparent processing of all personal data and have stringent measures to enable data subjects to exercise their rights.

St Pauls Advice Centre has developed the below objectives to meet our data protection obligations and to ensure continued compliance with the legal and regulatory requirements.

We ensure that: -

- We protect the rights of individuals with regards to the processing of personal information
- We develop, implement and maintain a data protection policy, procedure, audit plan and training program for compliance with the data protection laws
- Every business practice, function and process carried out by the organisation, is monitored for compliance with the data protection laws and its principles
- Personal data is only processed where we have verified and met the lawfulness of processing requirements
- We only process special category data in accordance with the GDPR requirements

- We record consent, where appropriate, at the time it is obtained and evidence such consent to the Supervisory Authority where requested
- All employees are competent and knowledgeable about their GDPR obligations and are provided with training in the data protection laws, principles, regulations and how they apply to their specific role and the organisation
- Individuals feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the data protection laws
- We maintain a continuous program of monitoring, review and improvement with regards to compliance with the data protection laws and to identify gaps and non-compliance before they become a risk, affecting mitigating actions where necessary
- We monitor the Supervisory Authority, European Data Protection Board (EDPB) and any GDPR news and updates, to stay abreast of changes, notifications and additional requirements
- We have robust and documented Complaints Policy and Data Breach controls for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection
- We have appointed a Data Officer who takes responsibility for the overall supervision, implementation and ongoing compliance with the data protection laws
- We have dedicated procedures in place to perform regular checks and assessments on how the personal data we process is obtained, used, stored and shared. We review this against our data protection policies, procedures and the relevant regulations to ensure continued compliance
- We provide clear reporting lines and supervision with regards to data protection
- We store and destroy all personal information, in accordance with our Data Retention and Erasure Policy which has been developed from the legal, regulatory and statutory requirements and suggested timeframes
- Any information provided to an individual in relation to personal data held or used about them, will be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language
- Employees are aware of their own rights under the data protection laws and are provided a Privacy Notice for Staff and Volunteers
- We have developed and documented appropriate technical and organisational measures and controls for personal data security and have a robust Information Security program in place

3.0 Definitions

Consent - Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

Data Controller - A natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

Data Processors - A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.

Data Protection - The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.

Data Subject - An individual who is the subject of personal data

Personal Data - Any information relating to an identified or identifiable natural living person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing - Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Special Categories of Data - "Sensitive Personal Data" are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. Data relating to criminal offences and convictions are addressed separately.

Supervisory authority - This is the national body responsible for data protection. The supervisory authority for our organisation is the Information Commissioners Office.

4.0 Roles and Responsibilities

The Executive Director is responsible for information governance including the responsibility of Data Protection (The Data Officer) and ensuring St Pauls Advice Centre is accountable and compliant with the General Data Protection Regulation (GDPR) and Data Protection Act 2018. The Data Officer will identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and upper management and to actively stay informed and up-to-date with all legislation and changes relating to data protection.

They will ensure that all processes, systems and staff are operating compliantly and within the requirements of the data protection laws and its principles and have overall responsibility for due diligence, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the data protection laws and our own internal objectives and obligations.

Staff who manage and process personal or special category information will be provided with data protection training and will be subject to continuous development support and mentoring to ensure that they are competent and knowledgeable for the role they undertake.

All members of the Management Committee and all staff whether direct employees, temporary/contract staff or volunteers of St Pauls Advice Centre or indirectly

employed through contractors and their sub-contractors are subject to comply with this policy and current Data Protection legislation.

5.0 Information Commissioner's Office (ICO) Registration

St Pauls Advice Centre is registered with the Information Commissioner's Office Register; registration number **ZA041611**. Our designated Data Protection Appointed Person (The Data Officer) is Rob France, who can be contacted at rob@stpaulsAdvice.org.

6.0 Training/Awareness

Data Protection will be part of core induction training. All new staff will receive awareness training on information governance, which will include confidentiality, data protection and information security.

Data Protection training including awareness and understanding of confidentiality, data protection, information security and freedom of information will be mandatory training for all staff on an ongoing basis and as and when legislation updates are relevant.

See our Induction and Training Policy for further information.

7.0 Data Audit

St Pauls Advice Centre have carried out a data protection information audit for each of its Services and HR/Finance Department to better enable us to record, categorise and protect the personal data that we hold and process.

The audit has identified, categorised and recorded all personal information obtained, processed and shared by St Pauls Advice Centre in our capacity as a data controller/processor and has been compiled on a central register which includes:

- What data we hold
- Who do we collect this data from/on
- Why we hold this data
- When do we collect this data
- When do we destroy this data
- Where do we hold or store the data
- How do we handle or process it
- Who has access to the data
- Do we share this data with anyone

8.0 Principles of Data Protection

The 6 GDPR principles of Data Protection require that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation')

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Accountability - GDPR requires that 'the controller shall be responsible for, and be able to demonstrate, compliance with the data protection laws principles' ('accountability') and requires that organisations show how they comply with the principles, detailing and summarising the measures and controls that they have in place to protect personal information and mitigate the risks of processing.

9.0 The Rights of Individuals

Under the GDPR and Data Protection legislation, Data Subjects have the following rights:

- The right to be informed – we inform you through our privacy statement and through other privacy-related communications, whether you interact with us in person, by telephone, by e-mail, online or using other channels.
- The right of access – you have the right to ask us for confirmation that your data is being processed and to access this data (a 'subject access request').
- The right to rectification – you have the right to have inaccurate or incomplete personal (factual) data corrected or completed.
- The right to erasure – you have the right in some circumstances to ask us to erase your personal data (the 'right to be forgotten'). Sometimes, this right may not apply, for example when the personal data needs to be retained for insurance purposes, or in relation to legal claims.
- The right to restrict processing – you have the right to ask us to limit how we collect and use your personal data, for example, to stop us deleting data that you might need in relation to a legal claim, or to restrict certain workers viewing your data where there may be a conflict of interest.
- The right to data portability – you have the right in some circumstances to be given your personal data in a structured, commonly used and machine readable form. This only applies to personal data you have given directly to us, where processing is carried out by automated means, and where the personal data is being processed based on your consent or in relation to a contract.

- The right to object – you have the right in some circumstances to object to processing of your personal data. This includes your right to object to: processing that we justify as being based on our legitimate interests; direct marketing; and processing of personal data for research and statistical purposes.
- Rights in relation to automated decision making and profiling – Missing Link has not identified any processing of personal data that currently involves solely automated decision-making or profiling.

See our Data Retention and Erasure Policy and Procedure and our Data Subject Access Request Procedure for further information.

10.0 Legal Basis for Processing (Lawfulness)

At the core of all personal information processing activities undertaken is the assurance and verification that we are complying with lawfulness of processing obligations. Prior to carrying out any personal data processing activity, we identify and establish the legal basis for doing so and verify these against the regulation requirements to ensure we are using the most appropriate legal basis.

The legal basis is documented on our data audit register and in our Privacy Notices and, where applicable, is provided to the data subject. The legal basis will vary depending on the category of data subject, for example, service users, employees, trustees, suppliers etc.

Data is only obtained, processed or stored when we have met the lawfulness of one or more of the processing requirements, where:

- The data subject has given consent to the processing of their personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which we are subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the organisation
- Processing is necessary for the purposes of the legitimate interests pursued by the organisation or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child).

11.0 Processing Special Category Data

Some of the personal data we process can be more sensitive in nature and therefore requires a higher level of protection. The GDPR refers to the processing of this data as 'special categories of personal data'. This means personal data about an individual's:

- race;
- ethnic origin;

- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data (where this is used for identification purposes);
- health data;
- sex life; or
- sexual orientation
- offending history.

Where we process any personal information classed as special category or information relating to criminal convictions, we do so in accordance with Data Protection legislation.

We will only ever process special category data where one or more of the following apply:

- The data subject has given explicit consent to the processing of the personal data. We will always ensure service users have the option to decline sharing sensitive data.
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim
- Processing relates to personal data which are manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest because we would not be able to provide our services without doing so
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
- Processing is necessary for reasons of public interest in the area of public health
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

We ensure appropriate policy documents are in place when the processing is carried out, specifying our: -

- Procedures for securing compliance with the data protection laws principles

- Policies as regards the retention and erasure of personal data
- Retention periods and reason (i.e. legal, statutory etc.)
- Procedures for reviewing and updating our policies in this area

12.0 Privacy Notices

St Pauls Advice Centre defines a Privacy Notice as a document that is provided to individuals at the time we collect their personal data (or at the earliest possibility where that data is obtained indirectly).

Our Privacy Notices provide individuals with all the necessary and legal information about how, why and when we process their data, along with their rights and obligations.

We have a link to our Privacy Notices on our website and provide a copy of physical and digital formats upon request. The notice is the customer facing policy that provides the legal information on how we handle, process and disclose personal information.

The notices are easily accessible, legible, jargon-free and are available in several formats, dependant on the method of data collection: -

- Via our website
- Linked to the footer of emails
- Verbally via telephone or face-to-face
- Service User Charter

13.0 Data Storage and Retention

St Pauls Advice Centre have defined procedures for adhering to the retention periods as set out by the relevant laws, contracts and our business requirements, as well as adhering to the GDPR requirement to only hold and process personal information for as long as is necessary. All personal data is disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and prioritises the protection of the personal data in all instances.

We will retain personal data for no longer than is necessary, taking into account the reasons that the personal data was obtained and our legal obligations.

Please refer to our Data Retention & Erasure Policy for further guidance and procedures.

14.0 Third Party Processors

St Pauls Advice Centre utilise external processors for certain processing activities (where applicable). We use data audits to identify, categorise and record all personal data that is processed outside of the company, so that the information, processing activity, processor and legal basis are all recorded, reviewed and easily accessible. Such external processing includes (but is not limited to): -

- IT Systems and Services
- Legal Services
- Human Resources
- Payroll
- Hosting or Email Servers

- Direct Marketing/Mailing Services

We have strict measures in place and review, assess and background check all processors prior to forming a business relationship. We obtain company documents, certifications, references and ensure that the processor is adequate, appropriate and effective for the task we are employing them for. This includes ensuring they comply with the GDPR and current data protection regulations.

The continued protection of data subjects' rights and the security of their personal information is always our top priority when choosing a processor and we understand the importance of adequate and reliable outsourcing for processing activities as well as our continued obligations under the data protection laws for data processed and handled by a third-party.

Where appropriate, we have a dedicated Processor Agreement template that details: -

- The processors data protection obligations
- Our expectations, rights and obligations
- The processing duration, aims and objectives
- The data subjects' rights and safeguarding measures
- The nature and purpose of the processing
- The type of personal data and categories of data subjects

15.0 Disclosure Exemptions

We take appropriate steps to ensure that no personal data is disclosed to unauthorised third parties. All employees are required to attend confidentiality training in order to learn how to exercise due caution when requested to disclose personal data to a third party.

Disclosure is permitted by the GDPR without the consent of the data subject under certain circumstances, namely:

- In the interests of safeguarding national security;
- In the interests of crime prevention and detection which includes the apprehension and prosecution of offenders;
- In the interests of assessing or collecting a tax duty;
- In the interests of discharging various regulatory functions, including health and safety;
- In the interests of preventing serious harm occurring to a third party; and
- In the interests of protecting the vital interests of the data subject i.e. only in a life and death situation.

The Data Officer is responsible for handling all requests for the provision of data for these reasons and authorisation by the Data Officer shall only be granted with support of appropriate documentation.

16.0 Privacy by Design

We operate a 'Privacy by Design' approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via our processes, systems and activities. We have developed controls and measures that help us enforce this ethos.

Data Protection by design ensures St Pauls Advice Centre consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle.

We are committed to:

- Putting in place appropriate technical and organisational measures designed to implement the data protection principles; and
- Integrating safeguards into our processing so that we meet the GDPR's requirements and protect the individual rights.

Data Minimisation: We only ever obtain, retain, process and share the data that is essential for carrying out our services and/or meeting our legal obligations and only retain data for as long as is necessary.

Our systems, employees, processes and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose. Data minimisation enables us to reduce data protection risks and breaches and supports our compliance with the data protection laws.

Pseudonymisation: We utilise pseudonymisation (e.g. key-coded/reference number used) where possible to record and store personal data in a way that ensures it can no longer be attributed to a specific data subject without the use of separate, additional information (personal identifiers). Encryption and partitioning is also used to protect the personal identifiers, being kept separate from the pseudonymised data sets.

When using pseudonymisation, we ensure that the attribute(s) being removed and replaced, are unique and prevent the data subject from being identified through the remaining markers and attributes. Pseudonymisation can mean that the data subject is still likely to be identified indirectly and as such, we use this technique in conjunction with other technical and operational measures of risk reduction and data protection.

Encryption: We utilise encryption as a further risk prevention measure for securing the personal data that we hold. Encryption with a secret key is used to make data indecipherable unless decryption of the dataset is carried out using the assigned key.

We utilise encryption via secret key for transferring personal data to any external party and provide the secret key in a separate format. Where special category information is being transferred and/or disclosed, the Data Officer is required to authorise the transfer and review the encryption method for compliance and accuracy.

Restriction: Our Privacy by Design approach means that we use restriction methods for all personal data activities. Restricting access is built into the foundation of our processes, systems and structure and ensures that only those with authorisation and/or a relevant purpose, have access to personal information.

17.0 Security and Data Breach Management

Alongside our 'Privacy by Design' approach to protecting data, we ensure the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred. Our Information Security and Risk Management Policy provides detailed measures and controls that we take to protect personal information and to ensure its security from consent to disposal.

We carry out data audits to ensure that all personal data held and processed by us is accounted for and recorded, alongside risk assessments as to the scope and impact a data breach could have on data subject(s). We have implemented adequate and appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Whilst every effort and measure is taken to reduce the risk of data breaches, we have dedicated controls and procedures in place for such situations, along with the notifications to be made to the Supervisory Authority and data subjects (where applicable).

Please refer to our Data Breach Policy & Procedures for further information.

18.0 Penalties

St Pauls Advice Centre understands its obligations and responsibilities under the data protection laws and recognises the severity of breaching any part of the law or Regulation. We respect the Supervisory Authority's authorisation under the legislation to impose and enforce fines and penalties on us where we fail to comply with the regulations, fail to mitigate the risks where possible and operate in a knowingly non-compliant manner.

Employees have been made aware of the severity of such penalties and their proportionate nature in accordance with the breach. We recognise that: -

- Breaches of the obligations of the controller, the processor, the certification body and the monitoring body, are subject to administrative fines up to €10,000,000 or 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- Breaches of the basic principles for processing, conditions for consent, the data subjects' rights, the transfers of personal data to a recipient in a third country or an international organisation, specific processing situations or non-compliance with an order by the Supervisory Authority, are subject to administrative fines up to €20,000,000 or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

19.0 Complaints

All complaints about the St Pauls Advice Centre processing of personal data may be lodged by a data subject directly with the Data Controller St Pauls Advice Centre.

Data Subjects with a complaint about the Processing of their Personal Data can contact the Information Commissioner's Office. An investigation of the complaint will be carried out in the extent that is appropriate based on the merits of the specific case. Information Commissioner's Office will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

See St Pauls Advice Centre's Complaint Policy and Procedure for full details.

20.0 Review

St Pauls Advice Centre will review this policy and associated procedures on an annual basis.

The Data Officer will update the Management Committee annually on progress, development and performance of Data Protection, Information Governance Management and implement Information Governance Management Action Plans.

21.0 Legal Framework

This policy is intended to meet our responsibilities within:

- Data Protection Act 2018
- General Data Protection Regulations (GDPR)
- Human Rights Act 1998
- Public Interest Disclosure Act 1998
- Protection of Freedoms Act 2012
- Counter-Terrorism and Security Act 2015: Prevent Duty
- Social Security Administration Act 1992,
- Children’s Act 1989, 2004
- Information Commissioners Office (ICO)

Cross Reference: Confidentiality Policy
Confidentiality Agreement
Whistleblowing Policy
Complaints Policy and Procedure
Safeguarding Policies
Information Security and Risk Management Policy
Service User Charter and DP Statement
Form of Authority: Permission to Share Form
Data Retention and Erasure Policy
Subject Access Requests Procedure
Data Breach Policy, Procedure and Incident Form
Privacy Notice for Clients
Privacy Notice for Staff and Volunteers
Privacy Notice for Job Applicants
Privacy Notice for Suppliers and Contractors

Document Control	
Date of Last Review:	November 2024
Date of Next Review:	November 2025
Review Cycle:	Annual
Changes from previous versions:	Reviewed – no changes made