St Pauls Advice Centre

Data Protection and Information Governance Policy

1. Purpose

Information is one of St Pauls Advice Centre's most valuable assets.

Every day people trust us with information about their finances, immigration status, housing, health, family relationships and other deeply personal aspects of their lives. Protecting that information is fundamental to maintaining that trust, delivering high-quality advice and fulfilling our legal, professional and ethical responsibilities.

Good information governance supports the quality, continuity and accountability of the advice services we provide. It enables us to provide safe, effective and accountable services, supports partnership working, protects individual rights and helps us demonstrate the quality of our work.

This policy explains the principles that govern how we collect, use, store, share, retain and dispose of personal information. It provides the framework for all other data protection procedures within the organisation.

2. Scope

This policy applies to everyone working on behalf of St Pauls Advice Centre, including:

- employees
- volunteers
- trustees
- contractors
- consultants

It applies to all information held by the organisation regardless of format, including:

- AdvicePro records
- electronic documents
- emails
- paper records
- photographs
- audio recordings
- video
- text messages
- information held by approved third-party providers.

3. Our Principles

Our approach to information governance is guided by five principles.

Trust

People should feel confident that the information they share with us will be treated respectfully, confidentially and securely.

Necessity

We only collect, use and share information that is genuinely needed to provide our services or meet our legal obligations.

Transparency

We explain clearly what information we collect, why we collect it, how it will be used and what rights people have.

Accountability

Everyone working on behalf of the organisation shares responsibility for protecting information and complying with this policy.

Learning

We continuously improve our information governance by learning from audits, complaints, breaches, supervision and changes in legislation or best practice.

4. Legislative Framework

We process personal information in accordance with:

- UK GDPR
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Human Rights Act 1998
- Common Law Duty of Confidentiality

We also comply with professional, contractual and regulatory requirements including Advice Quality Standard (AQS), Immigration Advice Authority (IAA), Financial Conduct Authority (FCA) requirements where applicable, and contractual obligations to funders and commissioners.

Where different standards apply, we will meet whichever requirement provides the greatest protection for individuals.

5. Data Protection Principles

Whenever we process personal information we will ensure it is:

- lawful, fair and transparent
- collected only for specified purposes
- limited to what is necessary
- accurate and kept up to date
- retained only for as long as required
- protected through appropriate organisational and technical security measures.

We will also be able to demonstrate compliance with these principles.

6. Information Governance Risks

We recognise that information governance risks include:

- accidental disclosure
- cyber attack
- phishing and fraud
- inappropriate sharing
- poor record keeping
- excessive retention
- loss or theft of equipment
- misuse of artificial intelligence
- home or remote working
- human error.

Information governance forms part of the organisation's wider risk management framework and significant risks will be reported to Trustees.

7. Roles and Responsibilities

Everyone working for St Pauls Advice Centre has a personal responsibility to protect information and to speak up if they believe information is being handled unsafely or inappropriately. We encourage a culture of openness, learning and continuous improvement rather than blame.

Trustees

Trustees provide strategic oversight and assurance that appropriate information governance arrangements are in place.

CEO / Data Officer

The CEO has overall accountability for information governance and acts as the organisation's Data Officer unless another individual is formally appointed.

The CEO will ensure:

- appropriate policies exist
- risks are managed
- breaches investigated
- staff trained
- compliance monitored
- trustees receive appropriate assurance.

Supervisors

Managers are responsible for ensuring that information is managed safely within their teams and that staff understand their responsibilities.

Each significant information system (for example AdvicePro, HR records and finance records) will have a designated manager responsible for its day-to-day governance.

Staff and Volunteers

Everyone working on behalf of the organisation must:

- protect confidential information
- follow this policy

- complete mandatory training
- report concerns immediately
- only access information required for their role.

8. Confidentiality in Advice Work

Confidentiality is central to the relationship between advisers and service users.

We will:

- explain why information is required
- only collect information relevant to the advice provided
- obtain authority before routine sharing
- respect the confidentiality of everyone involved in a case
- only disclose information without consent where there is a lawful or ethical justification.

Confidentiality is not absolute. Information may be disclosed without consent where safeguarding responsibilities, serious risk of harm, legal duties or court orders require disclosure.

9. Lawful Processing

Before processing personal information we will identify an appropriate lawful basis.

Most processing undertaken by St Pauls Advice Centre relies upon:

- legitimate interests
- legal obligation
- contract
- vital interests.

Where special category information is processed, we will identify an appropriate additional condition under UK data protection legislation.

We do not rely upon consent where another lawful basis is more appropriate.

10. Privacy by Design

Whenever we introduce:

- new technology
- new projects
- new partnerships
- new funding arrangements
- new methods of processing information

we will consider information governance from the outset.

11. Information Sharing

Information sharing must always be:

- lawful
- necessary
- proportionate
- recorded where appropriate.

Separate procedures apply to:

- safeguarding
- client file transfers
- subject access requests
- data breaches
- information sharing agreements.

12. Third-Party Providers

Where external organisations process information on our behalf, we will ensure they provide appropriate guarantees regarding confidentiality, security and compliance with UK data protection legislation.

Written agreements will be in place where required.

13. Artificial Intelligence

Artificial intelligence may support administrative and organisational tasks where appropriate.

Identifiable client information must not be entered into external AI systems unless they have been formally approved by the organisation and appropriate contractual and technical safeguards are in place.

The use of AI does not remove anyone's responsibility for confidentiality, professional judgement or the accuracy of information.

14. Individual Rights

We respect the rights of individuals under UK data protection law, including the rights to:

- be informed
- access information
- rectification
- erasure
- restriction
- objection
- data portability
- complain.

Requests will normally be managed under the Subject Access Request Procedure.

15. Records Management

The organisation will maintain appropriate:

- Records of Processing Activities
- retention schedules
- data sharing records
- breach registers
- complaint records
- subject access request registers.

Information will be retained and securely destroyed in accordance with the Data Retention and Erasure Policy.

16. Information Security

St Pauls Advice Centre is committed to maintaining robust technical and organisational security measures to protect the personal information we hold. As part of this commitment, we maintain Cyber Essentials certification and regularly review our cyber security arrangements to help protect against common cyber threats. Technical controls are supported by staff training, secure working practices and ongoing monitoring of information security risks.

We protect personal information through a combination of organisational, technical and physical security measures. These include:

People

- mandatory confidentiality agreements;
- induction and refresher training;
- role-based access to information.

Processes

- information governance policies and procedures;
- incident reporting and breach management;
- secure retention and disposal of records;
- regular review of access permissions.

Technology

- Cyber Essentials certified security controls;
- secure case management systems;
- multi-factor authentication;
- encryption where appropriate;
- malware protection;
- regular software updates and security patching;
- secure backups and recovery arrangements.

Additional safeguards apply when working remotely or using portable devices.

17. Data Breaches

All actual or suspected breaches of personal information must be reported immediately.

Every breach and significant near miss will be investigated to identify learning, improve practice and reduce future risk.

Data breaches will be managed under the Data Breach Policy.

18. Compliance

Compliance with this policy is a condition of working or volunteering for St Pauls Advice Centre.

Failure to comply may result in supervision, additional training, performance management, disciplinary action or termination of contractual arrangements, depending upon the circumstances.

19. Complaints

We welcome feedback about how we handle personal information and are committed to resolving concerns fairly, promptly and transparently.

Individuals who have concerns about the way their personal information has been handled are encouraged to raise them with the Data Officer in the first instance.

We will:

- acknowledge complaints promptly;
- investigate them impartially;
- provide a written response explaining our findings and any action taken;
- record complaints to support organisational learning and improvement.

Where a complaint identifies wider organisational risks or weaknesses, we will review our procedures, provide additional training or strengthen our controls as appropriate.

If an individual remains dissatisfied after our internal process has concluded, they have the right to complain to the Information Commissioner's Office (ICO).

20. Monitoring and Review

Information governance is subject to continuous monitoring and improvement.

We will review this policy at least annually, or sooner where required by:

- changes to legislation or ICO guidance;
- changes to organisational practice or technology;
- learning from audits, complaints or data breaches;
- new regulatory or contractual requirements.

As part of this review we will consider:

- compliance with legal requirements;
- findings from internal audits;
- complaints and subject access requests;
- breach reports and near misses;
- staff feedback and supervision;
- emerging information governance risks.

Minor amendments may be approved by the CEO where they do not materially alter the intent of the policy. Significant revisions will be approved by the Board of Trustees.

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:	July 2026
Date of Next Review:	July 2027
Review Cycle:	Annual
Changes from previous versions:	Comprehensive review and redraft. Updated for UK GDPR, Data Protection Act 2018 and Data (Use and Access) Act 2025. Rewritten in plain English, strengthened governance and accountability, introduced sections on information governance risks, confidentiality in advice work, privacy by design, AI, records management, complaints and monitoring, and aligned with the organisation's wider policy framework and current best practice.