Data Protection Policy & Procedure

Document Information

Issue Date	**28/03/2024**
Review Date	**28/03/2025**
Document Number	**001017**
Process Owner(s)	**Chief Executive / Assistant Director, Practice Development**

CONTENTS

1.0 POLICY STATEMENT

The Data Protection Act 2018 set out strict rules for how SHP and other organisations use people's personal data. The act gives individuals the right to find out what data is held by organisations about them, why the data is held and to whom it is disclosed. Individuals have a right of access to their personal data, to correct it and if necessary, have the right to amend it or erase it.

SHP is committed to the collation, processing, and storage of personal data in a thoughtful and respectful way. The protection of personal data is embedded in our organisational practice, policies, and procedures.

Personal Data Collection

In compliance with the Data Protection Act 2018, SHP needs to collect and process personal data about clients, employees, suppliers, and contractors to be able to:

- Meet its charitable objectives and provide effective support in its services.
- Meet the performance requirements of its contracts.
- Account for the work we do to the commissioning organisations that fund us.
- Perform tasks (public task) carried out in the public interest or exercise a statutory authority vested in us.
- Perform tasks in connection with legal proceedings or obtaining legal advice.
- Comply with employment law obligations.
- Comply with our obligations under the Limitation Act 1980.
- Ensure we do not discriminate against people on the grounds of race, gender, age, disability, religion, or sexuality.

We are committed to protecting the privacy and integrity of all personal data and adhering to the six principles of the data protection regulations. When we request personal data, we make sure it is processed fairly and lawfully. We do this by making sure that we:

- Tell individuals the purposes for collecting and processing it.
- Tell individuals how they can access, amend, and erase it if necessary.
- Only collect what data is needed, ensuring it is adequate, relevant, and not excessive.
- Only use it in accordance with the limited purposes for which it was collected.
- Routinely and consistently check its accuracy and keep it up to date.
- Only retain it for as long as contractually and legally necessary.
- Dispose of it securely once the period of retention has ended.
- Have appropriate technical and organisational security measures in place to protect data against unauthorised or unlawful processing, accidental loss, damage, or destruction.
- Not transfer it outside the UK.
- Not rent or sell it to third parties.

SHP is registered with the Information Commissioners Office (ICO). Reg Number: **Z8447316**.

Privacy Notice

All clients in SHP services are given a Privacy Notice at assessment or upon receipt of service. This document sets out:

- What personal information we collect and the purposes for it.
- How long we keep personal information for and why.
- How we securely store and dispose of personal information.
- How a client can access personal information and amend or delete it if necessary.

Requesting Personal Data (Subject Access Request)

SHP is fully committed to facilitating access by the individual to their personal data, while bearing in mind the need to protect other individuals right to confidentiality. When a request is received, we will:

- Provide the individual with confirmation their personal data is held.
- Provide the individual with a description of their personal data, the source of the personal data (if possible), the reasons it is being processed and whether it will or has been given to any other organisations or people.
- Provide the individual with a copy of the personal data requested, once we are satisfied that we are releasing it to the right person.
- Respond within 28 days and not charge a fee.

Individuals may use our **Personal Data Request Form** to find out what information is held about them. The process is managed by the SHP **Subject Access Procedure**.

Data Retention

Information about SHP data retention periods is available through our **Data Processing Notice** (Appendix B) and is published on our website: **www.shp.org.uk**.

Data Protection Breaches

SHP will ensure compliance with the Data Protection Act 2018 for the management and reporting of data protection breaches. Our management process is set out in Section 6.10 of this policy and procedure.

All data breaches are recorded, reported, and managed as incidents on the SHP InForm system and monitored by the appropriate managers and SHP Data Protection Officers.

Data Protection Training

All SHP staff must complete the SHP mandatory **Data Protection Essentials** online training course on Owl during their induction, with refreshers every 2 years. Data Protection is also covered in our Casework Skills and InForm training and managers 1-2-1 inductions.

2.0 PURPOSE

The purpose of this policy and procedure is to:

- Demonstrate our commitment to protecting the rights and personal data of individuals.
- Ensure that personal data about individuals is not processed without their knowledge and wherever applicable, their consent.
- Ensure that SHP staff who process personal data understand their responsibilities.

3.0 SCOPE

Applicable to all SHP staff and others contracted to work on our behalf, across all SHP services and departments.

4.0 TERMS & DEFINITIONS

Personal Data is information relating to a living individual. This data includes digital or electronic data (including CCTV Images), and data in structured and accessible manual filing systems (paper-based systems).

Sensitive Personal Data is data relating to religious or other beliefs, sexual life, physical or mental health condition, race or ethnic origin, ethnicity, political opinions, trades union membership, criminal record.

Data Subject is a living individual about whom the data relates.

Subject Access Request (SAR) is the rights of the data subject (individual) to request a copy of their data under a formal process. SAR is one of the main rights under the Data Protection Act.

Data Controller is an organisation or body which uses personal data. SHP is a data controller and is required to notify the Information Commissioners Office (ICO) of the types of personal data that the organisation processes and the purposes for which it is being (or is to be) processed.

Data Processor is any organisation processing data of SHP's behalf.

Processing means the storage, transfer, viewing, access, analysis, and deletion of personal data.

Data Protection Impact Assessment (DPIA) is a risk assessment completed for new services and data systems to ensure protection of data is assessed and any identified risk mitigated.

Information Commissioners Office (ICO) is the UK's independent public authority set up to uphold information rights by promoting good practice, ruling on complaints, providing information to individuals and organisations, and taking appropriate action (including fining organisations) when the law is broken.

SHP INFORMATION SECURITY STANDARDS

Confidential	Sensitive personal information of clients, staff, and other stakeholders, including: ▪ Racial/ ethnic origin ▪ Political opinion ▪ Religious beliefs ▪ Trade union membership ▪ Physical/ mental health condition or status ▪ Sexual life; and ▪ Criminal record Personal information that identifies living individuals, including: ▪ Home or work address ▪ Age ▪ Telephone number ▪ Photograph ▪ Educational establishments attended ▪ Unpublished financial reports ▪ Risk registers/ unpublished strategic corporate plans ▪ Investment strategies ▪ Impending mergers and acquisitions ▪ Research information	▪ User passwords/ Door entry codes ▪ PINS (Personal Identification Numbers) ▪ Individual bank details ▪ Commissioning authority contracts ▪ Performance monitoring reports ▪ Draft reports ▪ Audit reports ▪ Incident and accident reports ▪ Unpublished research ▪ Benchmarking results ▪ Information covered by confidentiality and non-disclosure agreements ▪ Information collected as part of criminal/ HR investigations ▪ Management Information systems ▪ Individual's salary information ▪ Service addresses ▪ Board meeting papers (Inc. minutes and agenda) ▪ Executive management papers (Inc. minutes & agendas)
Internal	▪ Internal correspondence ▪ Management briefings ▪ SHP, policy, procedure, and manuals (excluding those authorised for website publication) ▪ Training materials and associated documentation	▪ Business continuity plans ▪ Working group papers and minutes ▪ Committee papers ▪ Internal telephone directory ▪ Office addresses
Public	▪ Annual accounts & statutory audits ▪ Fundraising and campaign information ▪ Website content	▪ Job advertisements ▪ News or media releases ▪ Head office address

5.0 ROLES & RESPONSIBILITIES

All SHP Staff (and others working on SHP's behalf) will:

- Complete mandatory training, concerning the protection of personal data.
- Observe this policy and procedure in the performance of their duties.
- Collect and process appropriate information, in accordance with the purposes for which it is to be used.
- Ensure data is accurately maintained on In-Form and other SHP information management systems.
- Adhere to SHP's 'Clear Desk and Desktop' practice at all times.
- On receipt of a request from an individual for their personal data, immediately notify their line manager.
- Understand that breaches of this policy may result in disciplinary action.

Managers / Department Heads will:

- Ensure staff have completed GDPR training during induction.
- Ensure compliance with SHP's retention periods.
- Ensure Privacy Notices are issues to clients at assessment or upon receipt of service.
- Monitor SHP's 'Clear Desk and Desktop' practice.
- Ensure all data breached are reported as an incident on SHP InForm.
- Liaise with the Data Protection Officer on all subject access requests and data protection breaches.

The Operational Data Team will:

- Manage SHP's InForm security, staff access and use.
- Support the Data Protection Officer with Subject Access Requests.
- Support the Data Protection Officer to manage and respond to data protection breaches.
- Manage the client data retention periods and ensure effective deletion of data in liaison with data processors.
- Conduct internal audits to ensure compliance with the Data Protection Policy and Procedure.
- Provide data protection information and guidance to staff.

The Assistant Director of IT & IT Team will:

- Manage SHP's Microsoft O365 security, staff access and use.
- Manage SHP's ActiveH security, staff access and use.
- Manage SHP's physical IT assets and security.
- Manage the data retention periods and ensure effective deletion of data in liaison with data processors.

- Conduct internal audits to ensure compliance with the SHP Information Security Policy.
- Conduct Data Protection Impact Assessments (DPIA's) where required.
- Support the Data Protection Officer with Subject Access Requests.
- Support the Data Protection Officer to manage and respond to data protection breaches.

The Data Protection Officers will:

- Maintain the Data Protection Policy and Procedure and supporting procedures and guidance.
- Maintain the Data Protection Breach Register.
- Conduct Data Protection Impact Assessments (DPIA's) where required.
- Act as the contact point for the SHP Board and the ICO.
- Manage and advise on subject access requests and data protection breaches.
- Liaise with managers and departments heads to conduct data protection impact assessments on new services and systems.
- Report data protection breaches to the Executive Management Team on a quarterly basis and to the board annually.
- Create and publish a GDPR Overview Report annually.

The Chief Executive & Board of Trustees will:

- Ensure sufficient resources are allocated and maintained to ensure effective data protection within the organisation.
- Review and approve the SHP Data Protection Policy and Procedure.
- Provide a direct point of contact for the Data Protection Officer to report to and liaise with in relation to data protection breaches.
- Review data protection breach reports from the Data Protection Officer and approve recommendations or corrective actions required.

SHP data protection support and guidance: DataProtection@shp.org.uk.

6.0 MANAGEMENT PROCESS

6.1 COLLECTION & PROCESSING OF CLIENT DATA

6.1.1: All client applicants to SHP services sign their referrals/applications to evidence consent for that personal information to be shared with us for our assessment.

6.1.2: All clients in SHP services are issued with a **Privacy Notice** to communicate what personal data SHP will collect and process. It informs them of their rights to access, amend and erase personal data. Staff are required to tick the 'Consent' box on the Client's Page on Inform to evidence this has been done before they can process personal information.

6.1.3: After the 'Consent' box is ticked the following information relating to client needs, support and risk management can be collected, processed, and stored securely:

- First and Second Name
- Date of Birth and Gender
- Address and Contact Details
- Ethnicity, Sexuality, Disability and Literacy
- Next of Kin and GP Details
- Economic Status
- NI, HB, NHS numbers and Social Services ID
- Initial needs and risk assessment information
- Ongoing support information and risk management information
- Ongoing contact and engagement information
- Ongoing welfare and occupancy management information
- Incidents, safeguarding and complaints information
- Final support outcomes and case closure information

6.1.4: The collation, processing and storage of any additional client personal data must be agreed with client consent and evidenced on the SHP **Additional Data Consent Form**, which must be signed by the client.

6.1.5: If SHP wishes to collect, process and store other types of personal information from a client that is not listed in 6.1.3 for the purposes of communication, fundraising or other promotional activity, then extra consent is required using the SHP **Media Consent Form**.

6.1.6: CCTV is in operation in many of our accommodation services for the safety and security of clients, staff, and visitors. CCTV signage will be on display in all services where CCTV is in operation. CCTV data is stored for a **maximum of 28 days** before automatic deletion.

6.1.7: All SHP accommodation services upload a photograph of a client to the SHP Inform page where their other personal information is processed and stored. This enables our services to keep clients, staff, and visitors safe and helps us provide person centred support. SHP staff ensure:

- The photograph is an appropriate representation of the client.
- The photograph is provided by or chosen by the client.
- The photograph is deleted from an SHP device if used once the image is uploaded.
- The photograph can be changed or deleted by the client if they wish.

6.1.8: SHP will not use the client's photograph for any purposes other than identification unless further consent has been obtained from the client.

6.2 SECURITY & STORAGE OF CLIENT DATA

Hard Copy Client Data

6.2.1: If a hard copy file is maintained for current clients receiving services, it will be stored in a secure filing cabinet(s) located in the staff office of the support service. Clients will be supported to keep their own hard-copy personal information safe where applicable.

6.2.2: Service Managers must ensure a common filing system is implemented and maintained within their service and all staff ensure they are familiar with the system, so they can store and access hard copy information as required.

6.2.3: **No hard copy client information should be left out of a file and unsecure in a staff office.**

6.2.4: A hard copy client file will not be removed from a designated staff office without the permission of a manager.

6.2.5: Individual documents of a client file that are required during a casework meeting or other client support may be removed from the file for this purpose. Care is to be taken to protect the information by ensuring it is stored securely by the responsible person and returned to the file as soon as possible after contact with the client or within 48 hours.

6.2.6: SHP operates a **'Clear Desk and Desktop'** practice in all staff offices and services to ensure no personal information of a sensitive or confidential nature is left unsecure at any time. This is maintained and monitored through:

- Providing staff with suitable storage for hard copy data.
- Dynamic inspections by Service Managers and Department Heads.
- Service and office audits by Data Protection Officers.

Soft Copy (Electronic) Client Data

6.2.7: SHP maintains the following electronic processing and storage systems: Microsoft O365, SharePoint and Teams; SHP website; CCTV in accommodation services. The following databases are used to process and store client information:

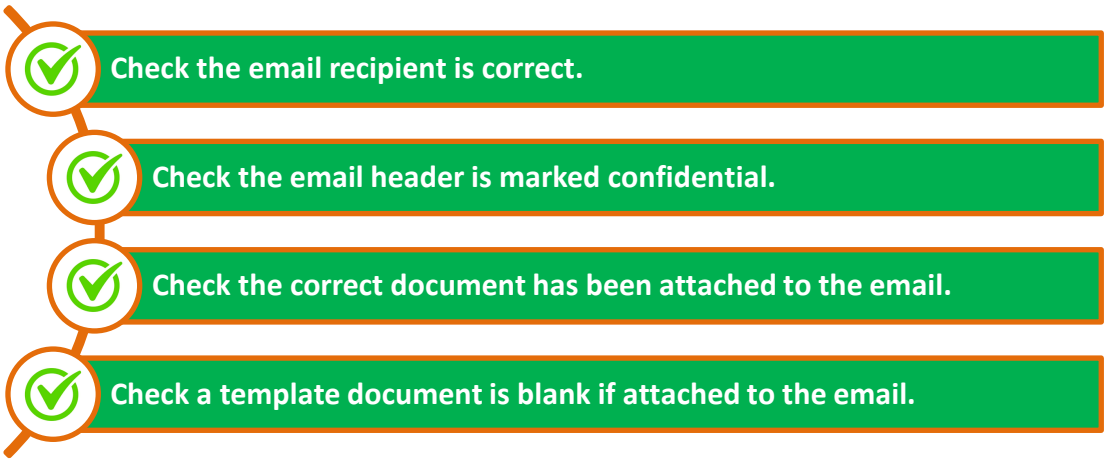
- **SHP InForm** (a cloud-based client record database – UK Data Storage Area UM9)
- **ActiveH** (a cloud-based rent accounting database)

6.2.8: The following security and data protection measures are in place:

- All computerised data processing systems are accessed by named logins, are password protected and require authentication codes.
- Individual passwords not shared and will be changed as prompted by the system administration protocols.
- Access to electronic records is subject to administrative permissions.

6.2.9: Electronic documents containing client information will be stored in the 'Notes and Attachments' section of the Client Page on SHP Inform if they are to be retained or in the allocated caseworker's One Drive. They are not to be stored on the services section of SharePoint or on desktops.

6.2.10: Electronic documents containing client information may be sent externally to individual named recipients by email, where possible using an encrypted system such as Egress Switch. Before staff press **SEND**, they should:



6.3 DISCLOSURE OF CLIENT DATA / INFORMATION SHARING

6.3.1: Clients of SHP services sign an **Information Sharing Consent Form** which is part of the Support Agreement. This evidences who we have agreed we can share personal information with on the client's behalf on a regular basis to carry out the required support and meet the client's needs. Clients can request to review this agreement at any time.

6.3.2: Only under exceptional circumstances will client information be processed or shared without their consent:

- Where a client does not have the mental capacity to give informed consent and a decision is made in their best interests and a record made of that decision.
- Where other vulnerable people may be at risk and information sharing is part of a Safeguarding Concern alert.
- Where an organisation requires the information to discharge its statutory rights.
- Where a criminal act has been committed.
- Where it is on public interest grounds.

6.3.3: **Client information, including the presence or otherwise of a person within SHP services must not be disclosed to general enquirers**. SHP will seek consent from a client before sharing their personal data with a third party, such as a regulatory body or audit inspector.

6.3.4: If a client does not wish information about them to be shared and they are mentally competent, then their wishes will be respected. This should be recorded in the summary section of their Support and Safety Plan. A manager should always be notified if it is identified that a significant need may not be met or that a risk may increase through an inability to share information.

6.3.5: To ensure best practice SHP provides its staff with the following resources:

- **Third Party Disclosure Guidance.**
- **Seven Golden Rules of Information Sharing.**

6.3.6: A client may sometimes call a staff office and wish to discuss a subject that involves disclosing information over the phone. In this case staff must ensure the person on the phone is the client to whom the information relates. If unsure staff must check the identity by requesting:

- The client's date of birth.
- When the client started receiving support from the service.
- The name of the client's caseworker or service manager.

6.3.7: When an SHP service engages in regular information sharing with a third party we will ensure both parties sign an Information Sharing / Service Level Agreement and share information fairly and lawfully.

6.3.8: If consent to share a one-off piece of information is verbal (e.g., a client agreeing a caseworker can provide information to the DWP over the phone on their behalf while they are present) then this should be recorded on the relevant action record.

6.4 RIGHT OF ACCESS TO PERSONAL DATA

6.4.1: All clients have the right to access personal data. This includes paper (hard copy) and electronic (soft copy) records.

6.4.2: A client may request to access personal data using a **Personal Data Request Form**. This process will be managed as set out in the SHP **Subject Access Procedure**.

6.4.3: Access to records can only be refused if the disclosure has not had the permission to be shared or otherwise would cause serious harm to the physical or mental health of the client or other individuals in the records. Staff and managers can access advice, guidance, and support from SHP Data Protection Officers to manage SAR's when required.

6.4.5: All Subject Access Requests will be processed **within 28 days**.

6.5 AMMENDMENTS TO & ERASURE OF CLIENT DATA

6.5.1: Clients have the right to comment on the information held on file and may request that information about them is corrected or deleted. A service manager must approve any amendments.

6.5.2: Clients have the right to ask SHP to restrict or object to the processing of certain personal information if they feel it is inaccurate or disagree with what we believe are our legitimate interest to process it. While SHP responds to any such requests the client's support may need to be put on hold until we review it and make decision. This decision will be based on whether we feel we can continue to provide effective support and risk management without processing that personal information.

6.5.3: Clients have the right to erasure or 'right to be forgotten'. This is not an absolute right and we will need to consider the circumstances of any such request. SHP's response will also be guided by the provisions of our retention periods.

6.5.4: Staff and managers can access advice, guidance, and support from SHP Data Protection Officers to manage amendments and erasure of client data when required.

6.6 ARCHIVING & DELETION OF CLIENT DATA

6.6.1: All information relating to clients who have left an SHP service will be archived and stored for a **minimum of 7 years** to comply with the Limitation Act 1980. Information relating to serious incidents, safeguarding concerns and complaints are kept for **15 years** where a duty of care issue has arisen.

6.6.2: **Confidential hard copy data in folders must be shredded when a client leaves a service.**

6.6.3: Services will have arrangements in place for disposal of confidential documents and have a hand shredder on site and a secure method or disposing of confidential waste.

6.6.4: Any 'hard copy' client data that is important and to be retained must be scanned by staff and uploaded as an electronic document for storage in the 'Notes and Attachments' section of the Client Page. This will include documents such as:

- Referral Information / Application Form.
- Support and Information Sharing Agreement.
- Occupancy Agreement (in accommodation services).
- Documents related to Incidents (Warning Letters), Safeguarding and Complaints.

6.6.5: **No client electronic data (soft copy) will be stored on SHP One Drives by services after a client has left the service and no longer receives support from SHP.**

6.6.6: Retention periods of electronic data on SHP InForm are automatically set and are deleted monthly using storage management software that records deletion information for audit purposes.

6.7 COLLECTION, PROCESSING, ARCHIVING & DELETION OF STAFF DATA

6.7.1: SHP collects personal data and special categories of data relating to its workforce in compliance with the GDPR principles. We do this for:

- Compliance with legal and industry standards (e.g., to prove eligibility for work in the UK and suitability to work with vulnerable people).
- Administration purposes (e.g., to operate payroll, pensions etc).
- Offer any necessary support requirements in their role (e.g., to support healthy attendance at work or make reasonable adjustments due to ill health, disability or for any other appropriate reason).
- Monitoring of equality and diversity within the organisation.

6.7.2: SHP data retention periods for staff information are in accordance with the following statutory requirements and are published in a Privacy Notice to job applicants and employees and in SHP's Data Processing Notice:

- **National Minimum Wage Regulations 2015**
- **Immigration, Asylum & Nationality Act 2006**
- **Income Tax (Pay as You Earn) Regulations 2003**
- **Working Time Regulations 1998**
- **Reporting of Injuries, Diseases & Dangerous Occurrences Regulations 2013**
- **Management of Health & Safety Regulations 1999**

6.7.3: CCTV is in place in accommodation services for the safety and security of clients, staff and visitors. **SHP does not process staff data stored on CCTV for periodic or pre-planned monitoring of staff attendance, performance, or conduct.** SHP will however process staff data stored on CCTV when investigating incidents in our services and when investigating and responding to reasonable concerns, issues or complaints raised by clients, staff, or other interested parties where there has been a breach of safety and security.

6.7.4: All new staff in accommodation services are informed of the CCTV policy as stated in 6.7.3 in their service induction.

6.7.5: All staff data processed by the HR & OD Department for the purposes detailed above are archived and stored securely and the retention periods are set out in SHP's Data Processing Notice.

6.7.6: Subject Access Requests for staff follow the same process as set out in Section 6.4 and are managed by the HR Team.

6.7.7: **SHP managers must ensure they collect and process staff personal data on the appropriate forms and records and store them in a secure location, a specific database, or their One Drive, and not in any accessible folders on the Service tab of SharePoint.**

6.7.8: The HR & OD Department will support SHP staff to manage their personal data securely.

6.8 CONTRACTORS, SUPPLIERS & PARTNERS

6.8.1: SHP collects and processes personal information from our contractors, suppliers and partners in accordance with our contracts or service level agreements (SLA's).

6.8.2: Information is collected and stored centrally by the Facilities Team and by relevant services and departments on Microsoft O365 / SharePoint.

6.9 DONORS & SUPPORTERS

6.9.1: SHP collects and processes personal information from our donors and supporters in accordance with the SHP Data Processing Notice. Donors and supporters are given information about data protection when they sign up via the SHP website and via the Just Giving or CAF websites that SHP uses.

6.9.2: SHP donors and supporters have a 'opt in' option if they wish to receive more information from the organisation and can 'opt out' at any time.

6.9.3: SHP operates a 2 year 'Refresh' process where the Fundraising and Communications Teams contact donors and supporters to ensure they are still consent to SHP holding their personal information and contacting them.

6.9.4: The SHP Fundraising Team use the **Donorfy** cloud-based platform to ensure all donor and supporter personal data is collected, processed, and stored in a safe and secure location.

6.10 WORKING WITH DATA PROCESSORS

6.10.1: Organisations or individuals processing data on SHP's behalf must have a contract in place that covers the protection of that data. We will not share personal data with a processor until a contract is in place.

6.10.2: The contract must identify the type of data being shared and how the processer will use the information and state the data processor should not use our data for any other purposes than the one we have set out in our contract.

6.10.3: SHP will ensure that its contracts are sufficient and legally binding. All managers are responsible for ensuring due diligence is exercised in the selection of a data processor as part of the procurement process.

6.10.4: Data processors working on behalf of SHP must notify the Data Protection Officer of any data protection breaches within 24 hours.

6.11 DATA PROTECTION BREACHES

6.11.1: SHP classifies data protection breaches as:

- Loss of theft of data.
- Loss or theft of IT equipment.
- Unauthorised access or use of data.
- Unauthorised sharing of information or inappropriate disclosure.
- Non-secure disposal of data.
- Hacking or corruption of security systems.
- Information obtained by deception.

6.11.2: On discovery of a data protection breach (or possible breach) SHP staff must notify the Data Protection Officer **within 24 hours** and complete an Incident Record on Inform. The following information must be provided:

- Nature of the breach, type of data and data subjects involved.
- Date and time of breach and when it was discovered.
- Any IT systems or IT system failures involved.
- Whether the data subjects are aware of the breach.
- Any actions already taken by staff.

6.11.3: The Data Protection Officer will follow ICO guidelines to ensure:

- **Identification and classification of the breach.**
- **Containment and recovery.**
- **Assessment of on-going risk.**
- **Notification of the breach.**
- **Evaluation and response.**

6.11.4: The Data Protection Officer will inform the Executive Management Team and Board of all major data protection breaches immediately and will report on minor breaches through a quarterly update to the EMT.

6.11.5: If the DPO assess that the breach will present a risk to an individual's rights and freedoms then it will be reported to then ICO **within 72 hours**. These risks will include:

- Loss of control over personal data or limitation of their rights.
- Discrimination.
- Identity theft, fraud, or financial loss.
- Unauthorised reversal of pseudonymisation or anonymisation.
- Damage to reputation.
- Loss of confidentiality of personal data.
- Any other significant economic or social disadvantage to the individual concerned.

6.11.6: The Data Protection Officer and EMT will ascertain whether there are any legal or contractual requirements to notify any third parties (e.g., funders, police, insurance.)

6.11.7: Where the risk of the data breach is high to the data subject(s) (e.g., risk of identity, financial fraud or if the data is sensitive and is lost or compromised) SHP will notify the data subject and will:

- State how and when the breach occurred and what data was involved.
- Explain what we have done to contain the breach.
- Advice the data subject what else they can do to protect themselves.
- Provide a named person who they can contact for further information or advice.
- Provide details of our complaints process.

6.11.8: All data protection breaches will be recorded on the SHP Data Breach Register on Inform by the Data Protection Officer.

6.11.9: Once the data protection breach is contained and all required reporting completed, the Data Protection Officer will review:

- The causes of the breach.
- The effectiveness of SHP's response.
- Organisational learning.
- Corrective actions required.

6.11.10: The findings of the Data Protection Officer's reviews will be reported to the Executive Management Team quarterly and to the Board of Trustees when flagged as serious by EMT.

6.12 DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

6.12.1: Data Protection Impact Assessments will be conducted by the Operational Data Team or relevant Department Head when designing and implementing new services or systems that collect, process, and store any personal data.

6.12.2: SHP Data Protection Impact Assessments are conducted using a pro-forma template and consist of an eight-step process:

- **Screening Questions**
- **Identifying Need for DPIA**
- **Description of Information Sharing & Processing**
- **Assessment of Necessity & Proportionality**
- **Information Security Process**
- **Identifying & Assessing Risks**
- **Identifying Measures to Reduce Risk**
- **Approval and Outcomes**

6.12.3: The SHP Data Protection Officers will support Dept Heads and monitor the DPIA process.

6.12.4: SHP Data Protection Impact Assessments will be available and accessible to external stakeholders, partners, and auditors as and when requested.

7.0 PERFORMANCE STANDARDS

Performance Standard One: SHP will respond to Subject Access Requests within 28 days.

Performance Standard Two: SHP will issue all clients with a Privacy Notice and a Support & Information Sharing Agreement.

Performance Standard Three: SHP staff will notify the Data Protection Officer of a data protection breach within 24 hours of the breach occurring.

Performance Standard Four: SHP will notify the ICO of all data protection breaches where an individual's rights and freedoms are at risk within 72 hours of the breach occurring.

Performance Standard Five: SHP will operate a 'Clear Desk and Desktop' practice in all services and offices to ensure the security of sensitive and confidential personal data.

Performance Standard Six: SHP will ensure all personal data is archived and deleted in accordance with this policy and procedure and the SHP Data Processing Notice.

8.0 MONITORING & REPORTING

SHP will maintain a Data Breach Register on InForm that will be reviewed by the Executive Management Team and Quality Sub-Committee on a quarterly basis.

The overall number and management of Data Breaches and Subject Access Requests each quarter is monitored on the Board of Trustees KPI Report.

Regular internal audits and inspections to ensure compliance with legislation will be conducted by the SHP Data Protection Officers and reported to the EMT and Board of Trustees annually. External data audits are managed by the SHP Data Protection Officers and reported through the same mechanism.

9.0 REFERENCES

- Data Protection Act 2018 (GDPR)
- Limitation Act 1980
- London Multi-Agency Safeguarding Framework DSA 2021
- National Minimum Wage Regulations 2015
- Immigration, Asylum & Nationality Act 2006
- Income Tax (Pay as You Earn) Regulations 2003
- Working Time Regulations 1998
- Reporting of Injuries, Diseases & Dangerous Occurrences Regulations (RIDDOR) 2013
- Management of Health & Safety Regulations 1999

10.0 ASSOCIATED DOCUMENTS

Policy Framework Documents

Data Processing Notice (Appendix B)
Information Security Policy
Subject Access Procedure
Document and Record Management Procedure
Data Protection Essentials Guidance
Third Party Disclosure Guidance
CCTV Policy Statement
Data Breach Register (SHP InForm)
Data Protection Impact Assessment (DPIA)

Client Documents & Templates

Support and Information Sharing Agreement (contains Privacy Notice). This document is generated through Inform Casework Records.
Additional Data Consent Form
Media Consent Form
Photo / Video Consent Form
Personal Data Request Form
Subject Access Letter (1)
Subject Access Letter (2)
Subject Access Letter (3)