St Martins
more than a home
for the homeless

Records Management

Area:	Organisational
Subject:	Records Management
Updated:	January 2024
Trustee Approval:	
Versions	Version 1.0
Associated policies	See below
Review Date:	January 2025

Glossary

The following terms and abbreviations are used in this policy:

Business Continuity Plan (BCP) – a plan which ensures that the main functions of the business are able to continue after a disaster;

Chief Executive Officer (CEO) – aka Managing Director, is the highest officer charged with the management of the organization.

Data Protection Impact Assessments (DPIAs) - a written assessment of the impact of the planned processing operations on the protection of personal data.

Data breach - the loss of control of personal data for which you are data controller.

Data Protection Health Check – is an annual self-assessment audit of our data protection provisions.

Data subject - any individual person who can be identified, directly or indirectly, via an identifier such as a name, ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity;

Information Asset Register (IAR) - a list that captures information about information assets, including their location, owner, value, business requirements, and technical dependencies.

Information Security Management System (ISMS) - a framework of policies and procedures for systematically managing an organization's sensitive data.

Information sharing (or data sharing) – can make life easier and more convenient. GDPR allows the sharing of personal information, to keep those we support safe and to provide them with better services.

Lawful basis - a legal reason for holding and using personal data. Data protection law requires organisations to specify and be explicit about the lawful basis they are using to process personal data. There are six lawful bases set out in Article 6 of the GDPR, and at least one of them must apply for the processing to be lawful.

Personal information (or personal data) - any information or opinion that could identify an individual. It can be factual or subjective, true or false, recorded or not. It can include obvious examples such as name, address, email, phone number and medical records, as well as less obvious examples such as online identifiers, preferences, and opinions.

Privacy Notice - informs individuals about how the organization collects, uses, and protects their personal data. It is a public document that explains our data processing practices and data protection principles.

Record of Processing Activities (ROPA) - a record of the steps taken to complete a task. Similar to an audit trail, but for the actions taken on a computer or in real life.

Introduction, scope and purpose

This is St Martins' (hereinafter referred to as 'us', 'we' or 'our') policy for the safekeeping of all records, from creation to disposal, and including the sharing of information externally. Together with other related policies and procedures it constitutes our Information Security Management System (ISMS) and ensures that all records are properly created, accessible and used, and finally disposed of in a secure and timely fashion. It guides team members regarding individual responsibility for accuracy and appropriate storage. This policy is the starting point for all things concerning records management and data protection as it covers:

- record keeping, from creation to disposal;
- all data which we process (keep), whether hard copy or digital;
- all team members, including contractors, locums and temporary staff;
- transparency;
- retention and disposal;
- information handling, including sharing;
- individual data rights (right to erasure, restrict, object etc);
- subject access requests.

Creation and use of records

When creating records we use standardised structures and layouts for their content as provided by our computer systems. All records are kept in accessible but protected locations as documented in our Information Asset Register (IAR). The security procedures concerning access to records are detailed in our policy 'Staff code on the use of computing facilities, electronic networks and communications'.

Throughout the lifespan of a record we:

- ensure documentation reflects the continuum of care and is viewable in chronological order;
- ensure records are maintained and updated, and shared with those who have a legal basis for seeing the information;
- provide team members with guidance and training on the creation and use of records and their legal responsibilities to share and safeguard personal confidential information.

Rights of data subjects

Under GDPR legislation all data subjects have the following rights:

- of access to their personal data (see Subject Access Requests, below).
- to erasure – (the right to be forgotten) of their data in certain circumstances.
- to restrict processing - to block or suppress processing of their personal data in certain circumstances.
- to object - to the processing of their personal data for certain purposes.
- to withdraw consent - to revoke agreement to process their personal data.
- be informed - about how, why, and for how long their data will be processed.

- to rectification of inaccurate or incomplete data.
- to data portability of their data to another controller.
- to not be subject to automated decision-making and profiling that have legal or significant effects on them.

Data subjects can make rights requests verbally or in writing to any point or person in the organisation. The ICO recommends that individuals follow-up any verbal requests in writing. No specific words are necessary but useful templates are available from the ICO website. For further advice please e-mail dataprotectionofficer@stmartinshousing.org.uk or caldicottguardian@stmartinshousing.org.uk.

Subject Access Requests

The right of access (above) is further explained and supported by our DSAR procedure.

Information handling

Secure handling of personal information ensures that it is protected and not disclosed inappropriately, either by accident or design, whilst in use or when being transferred, whether stored in hard copy or digitally. All processing of personal information must have a lawful basis. Our Record of Processing Activities (ROPA) identifies records all our processing of personal information and all the associated lawful bases. We ensure that all personal information received is handled securely including that arriving through verbal communications (including telephone, postal services and couriers), portable devices, fax, e-mail (see e-mail tips and guidance – in development – inc disabling autofill of e-mail addresses), and any other forms of information exchange (e.g. text messages, online portal upload etc).

Data classification

Data classification is the process of organizing data into categories based on the level of sensitivity and the impact to the organization if that data is disclosed, altered, or destroyed. Data classification in St Martins is currently in development and will be fully described here when ready for use.

Transparency

Our Privacy Notice explains to all our data subjects why we hold their data, how we process it and the lawful bases for doing so. The privacy policy is freely available on our website and is part of our commitment to transparency and accountability. It satisfies the individual's right to be informed under GDPR and is reviewed annually.

Our leaflet called 'Processing your information' is given to all those we support at the point that their information is first received and support begins. It explains the information we need and how we use it, including sharing with others, and individual data rights under GDPR.

All of our Data Protection Impact Assessments (DPIAs), detailing the types of personal data used by our business processes, are published on our website.

Information sharing

Our Privacy Notice explains why and with whom we share the personal information of our data subjects. We are also partners to a number of Information Sharing Agreements which are designed to apply specific standards and controls to the process. Our guidance note called 'Introducing ISAs' refers. All information sharing occurrences are recorded in our 'Sharing log'. When using a letter or an email to share information externally we apply double-checking measures especially when sensitive data is included. This ensures that the correct information is sent to the correct recipient and reduces the risk of some of the most commonly occurring data breaches.

Retention and disposal

Our records are retained for as long as necessary for the purposes they were originally collected, in accordance with our Retention Schedule. Records are securely destroyed in accordance with our Data Protection policy.

Data Protection Impact Assessment

All of our business processes which use personal information have a Data Protection Impact Assessment (DPIA) all of which are reviewed annually. A new DPIA is created whenever a new business process to handle personal data is considered.

Audit

All of our data protection provisions are audited by our annual Data Protection Health Check to demonstrate compliance with GDPR and to ensure record management of the highest standard.

Data incidents and breaches

A data incident or breach is defined as the loss of control of personal information for which St Martins is data controller.

St Martins is committed to protecting personal information and has in place a number of technical and organisational measures to help. These include, but are not limited to, secure passwords, encryption, building and office security, policies and procedures including this Record Management policy.

Examples of data incidents include the loss or theft of information or equipment, incorrect handling of protected information, information disclosed in error, unauthorised use or access to information or systems. An incident can be caused or facilitated by human error, lapse in diligence, lack of awareness or training, deliberate or accidental disregard for policy, poor physical security, scams or hacking. All incidents must be reported immediately to your line manager and from there to the Chief Executive and DPO. Your report should include key details of the incident, when and where it happened, which information and assets were compromised, number of people affected, and the immediate actions taken.

More serious breaches (where numbers are higher) may be serious enough to require reporting to the ICO. If so, they must be reported within 72 hours of the occurrence. This reporting step is usually handled by the DPO. If the DPO is unavailable the CEO will decide who best to deputise. The ICO website https://ico.org.uk/ offers guidance on what constitutes a serious breach and provides a portal for the reporting.

Roles and responsibilities

There are certain roles and responsibilities to ensure compliance with data protection law:

- Team members and managers - process and share personal data securely in compliance with GDPR using appropriate technical and organisational measures provided by St Martins.
- Data controller - defines how and why personal data is processed, and is accountable for compliance. St Martins is a data controller.
- Data processor - processes personal data on behalf of the controller, and must follow the controller's instructions and security requirements. St Martins is a data processor.
- Data protection officer (DPO) - advises and monitors the controller and the processor on their data protection obligations, acts as a contact point for supervisory authorities and advises team members and managers on data protection matters. St Martins' DPO is contactable at dataprotectionofficer@stmartinshousing.org.uk
- Caldicott Guardian - senior person who protects the confidentiality of personal information by considering the ethical and legal aspects of information sharing. They ensure that personal information is used responsibly to support the delivery of better care and advise team members and managers on data protection matters. St Martins' Caldicott Guardian is contactable at caldicottguardian@stmartinshousing.org.uk
- Information Commissioners Office - oversees and enforces GDPR and may issue fines and sanctions for non-compliance.

Associated Policies

Privacy notice

Confidentiality

CCTV (and CCTV procedure)

Data Protection

Information Governance

Retention Schedule

Business Continuity Plan

Communications

Code of conduct on use of computing facilities

DSAR procedure