St Martins
more than a home
for the homeless

Confidentiality Policy

Area:	**Personnel /12**
Subject:	**Confidentiality**
Updated:	**7 May 2024**
Trustee Approval:	
Review Date:	**7 May 2027**
Versions	
Associated policies	

St Martins
more than a home
for the homeless

Confidentiality Policy

Introduction

In the course of its day to day activities St Martins has access to a wide variety of personal information about individuals. This information is required to enable the organisation to carry out its role as support provider and employer.

The importance of respecting an individual's confidentiality is stressed in the Code of Conduct. When requesting personal information staff should always be clear why they need it and how it will be used and should ensure compliance with the Data Protection Act 2018.

The area of our work is subject to a variety of legal requirements and statutes of law, and must ensure that we are also complying with these requirements. St Martins aims to comply with both the letter and the spirit of the Data Protection Act 2018 and recognises that the right to freedom from unnecessary invasions into personal privacy is enshrined in the Human Rights Act 1998.

Personal information held by St Martins

The Data Protection Act 2018 makes clear that information stored about service users should be "adequate, relevant and not excessive" for the purpose required. With this in mind, all service user files should only contain necessary information.

St Martins will only keep information that is required for some specified purpose. The information will be relevant and not excessive for that purpose. Under the data protection legislation, there are six data protection principles that St Martins and all members of staff must comply with at all times in their personal data processing activities. In brief, the principles say that personal data must be:

Processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency).

Collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those 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 also 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).

Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed (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).

Managers will ensure that files are reviewed regularly as part of the supervisory process and offer guidance to staff about what it is appropriate to store.

Record Types

Access to this information is strictly controlled and stored confidentially. The Data Protection Act 2018 applies to both computerised data and manual filing systems, which may include but are not limited to:

- Case files, support plans and service user risk assessments
- Data bases of addresses and other personal information
- Contact sheets
- Records of meetings
- Information about service users from other agencies
- Benefits and rents information

Additionally, we may record the output of CCTV cameras situated near or within some of our accommodation projects and use it for the purposes of security and crime prevention.

All data and record types above are subject to the requirements of the Data Protection Act 2018. St Martins is accountable for the information it processes and staff ensure that they are confident in dealing with issues concerning client confidentiality and data protection.

Breach of Confidentiality

All employees have a duty to respect of confidentiality of all personal and business information held by St Martins. Breaches of confidentiality will be regarded by St Martins as a disciplinary offence and will be dealt with in accordance with the Disciplinary Procedures

National data opt-out

The National data opt-out applies when organisations share personal data for the purposes of research or planning. Individual data subjects can choose to stop this happening by opting-out. At this time, we do not share any data for planning or research purposes for which the national data opt-out would apply. We review all of the confidential patient information we process on an annual basis to see if this is used for research and planning purposes. If it is, then individuals can decide to stop their information being shared for this purpose. You can find out more information at https://www.nhs.uk/your-nhs-data-matters/.

Recording information on databases

When recording information on databases such as Salesforce, be aware that this information may be visible to a much larger group of people, increasing the risk of leaking or misuse. Data added is usually a permanent record in these systems.

Please remember:

- Don't add original documents from a third party unless instructed to do so
- Keep what is recorded strictly factual, avoid reporting gossip or rumour, presumption or personal opinion and carefully consider reporting information from third parties
- To ensure accuracy, when recording information the member of staff receiving the information must be the one to enter the details on notes / records
- What is recorded and how it is used needs to be fair to the service user
- What is recorded must be relevant to the support we offer the service user
- When recording notes bear in mind the service user may use their right to ask to read it.
- Keep all files that contain service users personal information safe from being accessed by anyone who does not have the right to see it
- Ensure all records are dated and signed

File Keeping and Security

Staff keep confidential service user information stored securely so that it cannot be accessed by unauthorised personnel. In the case of paper records, files are stored in lockable storage facilities to remain secure in the event of a break-in.

In the case of computerised files, this means that passwords and other access restrictions are in place.

Keep your computer screen turned away from public view and locked or switched off if you need to leave it unattended, particularly if viewing service users personal data.

Paper files should be arranged in such a way as to facilitate ease of access and understanding for any service user wishing to review their file.

Staff wishing to remove from the office any files containing personal information about service users must first get the permission of their line manager. The possibility that the security of the information may be compromised by it being taken off site should be considered and an assessment made as to how to maintain the security of the information.

Staff carrying service user information with them, away from its usual storage place, are responsible for what happens to the information and will be held accountable for any breaches of confidentiality that may occur as a result.

Computerised files should be backed up regularly to avoid accidental loss or destruction of data.

Ensure that all files or written information of a confidential nature are not left out where they can be read by unauthorised staff or others.

For accessing your working email or Salesforce account use only the password provided to you by St Martins. Do not use others employees passwords under any circumstances.

Service users' Right to Inspect their File

The Data Protection Act 2018 gives individuals a right to access information about themselves.

Service users and applicants are able to view and challenge any information held about them except where there is a genuine risk or harm or a third party would be identified who has not given their consent

Service users and applicants must put their request in writing

The tenant or applicant cannot be shown:

- Confidential information or information of a sensitive nature given to us (e.g. doctors or social workers)
- Information that involves other people unless you are able to black out the 3rd party data which removes all identifying features.

In such cases the information should be removed and a note attached to the front of the file indicating that they have been removed.

In all cases where a request to see information is made the project manager should go through the file and remove all sensitive material.

Where an individual formally requests a copy of all information held about him/her, this should be taken as a Data Subject Access Request (DSAR) under the Data Protection Act 2018. Advice on how to process DSARs can be sought from our Data Protection Officer at DataProtectionOfficer@stmartinshousing.org.uk.

Charges

St Martins will not make a charge for granting access to files or for reasonable requests for copies of documents.

Challenging Information

A service user may challenge any information held in their file or on a computer if they feel it to be incorrect and can provide evidence to support this.

If St Martins accepts that the information is incorrect they will correct or erase the information. If, however, St Martins does not accept that the information is incorrect it will attach a note recording the service user's view and the decision not to alter it.

Receiving third party information

Information about service users should be accepted from outside agencies and persons on the basis that it will be available to the service user should they seek access to their file.

Any information offered on condition that it is kept secret from the service user will be refused, unless it appertains to matters of health, safety and risk management. This should be discussed with line management who will ensure careful consideration is given as to whether or not the information needs to form part of the service user's file with the St Martins. The client should be informed when any significant information is received about them from a third party.

Third parties are responsible under the Data Protection Act 2018 for how they use/share the information they hold about a service user but once the information comes into our domain, we become equally responsible for how it is used.

Staff should record who by and where the information was obtained e.g. social worker, GP, resident

Disclosure of information to a third party

Information can be routinely shared with those agencies or individuals whom a client has included on their multi agency information sharing consent form.

In exceptional circumstances St Martins may be legally required to disclose information to third parties, such as when in the public interest or the safety of others. We will endeavour to inform the individual this has been done where appropriate or permissible to do so. St Martins will comply fully with the requirements of the law in all such circumstances".

Within St Martins, some services operate information sharing protocols with other agencies. Staff will make it clear to service users that, in many cases, accepting our services or accommodation will mean accepting that we are working in partnership with statutory authorities like the probation service or the local mental health team.

Verification

Staff will take steps to satisfy themselves that the person or agency requesting information about a client or staff member is genuine and has a right to the information before any information is disclosed.

However, where doubt exists, staff should consider the following:

- Asking callers to put requests in writing
- Calling back the person requesting the information to check their place of work, ideally by calling reception to get connected through.

If it is not possible for staff to satisfy themselves of the legitimacy of the request for information, a polite refusal should be extended to the caller and the matter referred immediately to the appropriate line manager within St Martins.

In the event of people calling in to offices or accommodation projects looking for information about service users or seeking confirmation that an individual is in residence, staff should decline to give any information and instead invite the caller to leave details of their request/message without revealing whether or not the individual lives there.

Public Health and Notifiable Diseases

While there is no legal obligation to do so, in circumstances when the health status of a client presents a risk to themselves, the public, to other service users or staff (eg: symptomatic TB) and the service user is unwilling to seek medical assistance, St Martins will inform the relevant medical authorities and seek advice on action to take and

management of risk. Any disclosure of a service user's medical condition/history must be authorised by a Service Manager.

Media Interest

Work with homeless people means that St Martins is sometimes in the public spotlight and required to comment on issues related to homelessness and housing. Such contact is generally positive and welcomed.

The St Martin's spokesperson with the media is normally the Chief Executive. All Staff are governed by the Code of Conduct which prohibits unauthorised contact with the media on any subject.

Additionally, service users should be protected from intrusive media contact where possible and advised of their rights to withdraw consent or co-operation from media projects even if this consent has been previously given.

Publicity

St Martins and its service users must respect the privacy of other individuals and projects when putting together publicity material. Service users must be consulted before information is disclosed and permission must be obtained before any photographs are used.

Reports and Statistics

The Data Protection Act 2018 states that, when all identifying details including reference no's have been removed from information about service users, the information is no longer regarded as confidential and can be used by St Martins for research, report writing and statistical purposes.

Housing Benefit Departments and Department of Social Security offices

The Social Security Administration Fraud Act 1997 places a duty on a landlord in receipt of Housing Benefit Direct to inform the Housing Benefits Office of any change in the service users circumstances where they know this is likely to affect a claim This could include whether or not the service user has moved or failed to move in, any change in rent and whether or not the service user has started or ceased to work. These disclosures are

outside the scope of the Data protection Act 2018 as the provisions of these Acts do not apply where the disclosures are required by another statue.

Where service users are making a claim for housing benefits, are in receipt of Housing Benefit or where St Martins receive Housing Benefits direct on behalf of a service user, the service user should be asked to complete the multi agency consent form, which gives the service users consent for St Martins staff to disclose such information as is requested by Housing Benefits office or where requests for other information are made in relation to any other claim.

Disposal of records

The Data Protection Act 2018 requires that we carefully dispose of service users' personal data when it is no longer required. St Martins does not keep personal data for any longer than is necessary".

Line managers will ensure that service user's files are regularly reviewed and information no longer required, is removed from the files and safely disposed of. In certain circumstances, it is necessary to keep service users information for longer than the prescribed period (eg: to pursue arrears, relating to a on-going legal matter).

All paperwork containing personal data or group business information disposed of by staff should be shredded and or placed into a confidential waste sack for removal. Breaches of confidentiality will be regarded by St Martins as a disciplinary offence and will be dealt with in accordance with the Disciplinary Procedures.

Working with the Police

St Martins wishes to maintain a constructive working relationship with the various Police Authorities operating in the localities where we offer services to clients. A good relationship is beneficial for the safety and security of service users, staff and the local community.

Given that service users often have a negative view of the Police, St Martins needs to ensure that St Martins established between staff and service users is not jeopardised by showing undue care when sharing information with the Police. Circumstances may include but are not limited to:

- Comply with the law and/or an appropriate Court Order
- Where there is a clear need to co-operate to manage risk - whether to service users, or the public or staff
- Where someone has a serious criminal history, whether or not we are aware of any current risk

- Where the Police have a clear and legitimate interest, for example, helping to section someone who is mentally ill
- Under the terms of formal information sharing protocol established under the auspices of the Crime and Disorder Act 2018. 22. Police Power to Access Information

Under the Police and Criminal Evidence Act (PACE), Police officers only have the right to take information about a service user if it relates to a crime they are investigating and they feel it is likely to be lost or destroyed.

Once someone has been arrested, the Police have powers to seize specified material that could be considered as evidence. This might include Untoward Incident Sheets which records staff observations on our premises. However, many of the records we keep in relation to clients would be classified as "excluded material" because they include personal information about clients given to us in confidence in the course of our professional work with the clients and obtaining these would require the Police to obtain a special Production Order at court.

The law in this area is complex and all staff should obtain authorisation from a manager before releasing documents to the Police.

Community policing

At a local level, many services have developed good working relationships with their local Community Safety, Beat Officers and Police Stations and this relies upon a level of informal information sharing about service users and the locality. Given that this information sharing is often general or anonyms (ie: describing problems within the project or with nuisance from outside), it is permissible and encouraged by St Martins. However, managers must ensure that the information sharing is properly controlled and seek advice before discussing anything that is likely to lead to Police action or breach client confidentiality.

CDA Protocols

The Crime and Disorder Act 2018 (CDA) requires the Police and local authorities to do all that they can to reduce crime and disorder within their area. In order to do this effectively, they are expected to develop local crime partnerships, seeking the co-operation of others within the community, who may have information which will assist them.

St Martins has signed up to various information-sharing protocols under the terms of Section 115 of the CDA. The existence of these protocols formalises the exchange of information between members and promotes confidence about the way information will be shared and handled. The fact that these protocols commit the organisation to information

sharing in specific circumstances does not, however, override our obligations under common law or the Data Protection Act.

The right of data subjects to access information held about them is particularly difficult to manage in the context of the CDA. Victims of crimes, witnesses and other informants need to be especially sure of confidentiality when they come forward with information and the success of crime detection/prevention initiatives would obviously be compromised if those suspected of offending were able to access the information. All requests for information must be very carefully considered and discussed with the Police and other partners to the protocol.

All requests for information, and information provided, under the auspices of a CDA information sharing protocol must be recorded so that an audit trail exists.

Information Sharing Agreements

Where there is information sharing with the police, local authorities or other agencies an Information Sharing Agreement (ISA) may often exist.

There are GDPR considerations in any such agreement. Please consult with the Chief Executive if an agreement is being drawn up, altered or renewed or if you think one may be necessary.

Missing Persons

There will be occasions when the St Martins is concerned enough about a service user going missing to formally make a missing persons' report to the Police. For this to be meaningful, it will be necessary to give the Police personal information about the client (eg: support needs, next of kin, usual sleeping out sites, etc.). Obviously in these circumstances, the vital interests of the client are at stake and the disclosure is therefore permissible under this policy and the law.

Additionally, St Martins may be in the position of knowing the whereabouts of a person who has already been notified as missing and whom the Police are searching for. In these circumstances, St Martins will notify the Police that we have seen the client but, if they wish to remain hidden, whether we would give further information about their exact whereabouts would depend on a management assessment of the individual circumstances and existing risk factors (such as age, vulnerability, etc.). Regardless, staff should urge and assist the client to make contact with those who may be concerned for them.

Sex Offenders Register

St Martins may work with clients whose past offences mean they have been required to join the Sex Offenders Register. The terms of being placed on the Register include a requirement for the individual to notify the Police of any change of address. Due to public safety concerns, where staff are aware of a client on the Register changing their address, this information will be notified to the Police regardless of any duty of client confidentiality.

Similarly if St Martins is aware that a service user has failed to take steps to comply with the Sex Offenders' Register despite being instructed to do so by the Courts, this information will be passed to the Police.

In the course of our work with service users in this category, it may also be necessary for staff to attend Multi Agency Protection Panels at which they are expected to share information about the client's progress and activities with a range of interested agencies (eg: Police, Probation, Social Services). Again, the public interest justifies this disclosure with or without the client's consent. In all cases, disclosure of information and attendance at meetings should be approved by line manager.

Access to information by Contractors

In general terms confidential information is not made available to external contractors, either about the individual clients or the nature of a project. However in the interest of contractor safety there is a legal obligation under the Health & Safety at Work Act. St Martins has legal liability for all its contractors or members of the public who may visit our offices/projects. One of the practical implications of this is that we must give our contractors any information that they need to keep themselves safe, such as warning markers or other relevant information.

CCTV

St Martins wishes to ensure that its service users, staff and visitors can enjoy a safe environment. In some circumstances, nuisance from within or outside accommodation or support projects has led to the decision to install CCTV cameras for the purposes of crime prevention and safety and security. In some instances, the output of these cameras is recorded. For more information please refer to the CCTV policy and procedure.

Training

All new staff must read the policies on data protection and on confidentiality as part of their induction process. Existing staff will be offered training to National Training Organisation standards covering basic information about confidentiality, data protection and access to records. Training in the correct method for entering information in service users' records should be given to all care staff. The nominated data user/data controller for St Martins should be trained appropriately in the Data Protection Act 1988. All staff who need to use the computer system should be thoroughly trained in its use.

Where applicable, all new staff will receive training on the basic principles and the operation of Salesforce and any other databases and software programmes used by St Martins as necessary

Data Protection

Advice on data protection matters including CCTV can be sought from our Data Protection Officer and Caldicott Guardian via e-mail at DataProtectionOfficer@stmartinshousing.org.uk and CaldicottGuardian@stmartinshousing.org.uk.

I acknowledge receipt of this Confidentiality policy and I confirm that I have read and understood it. I understand that I am responsible for complying with the terms of this policy.

Signed: . . . . . .

Print name: . . . . . .

Dated: . . . . . .

Versions

Version	Changes	Date Changes made	Who signed off
1.1	New format		
1.2	Updated following Data Protection review	April 2021	
2.0	Updated National data opt-out section and Data Protection Officer & Caldicott Guardian details	May 2022	
3.0	Updated in view of new Records Management policy, and amended 'Data' to 'Information' Sharing Agreements.	May 2024	Director Operations (Internal)

Associated Policies

Records Management

Data Protection

Privacy Notices

CCTV