St Martins
more than a home
for the homeless

Closed Circuit Television (CCTV)

Area:	Organisational
Subject:	Closed Circuit Television
Updated:	January 2023
Trustee Approval:	
Review Date:	January 2026
Versions	

St Martins
more than a home
for the homeless

Closed Circuit Television (CCTV)

Introduction

St Martins' closed circuit television (CCTV) system is registered with the Information Commissioner's Office under the terms of the Data Protection Act 2018. This policy outlines St Martins' use of CCTV and how it complies with the Act.

Purpose

St Martins uses CCTV to provide a safe and secure environment for people who use services, staff and visitors, to prevent the loss or damage to property and assets, and for the prevention, investigation and reduction of crime, which may include the provision of evidential data to the Police and other agencies (see Disclosure, below). The CCTV system is owned by St Martins. Deployment is determined by service managers, approved by the Senior Management Team and signed-off by directors. It's operation is managed by service managers as described in St Martins' CCTV procedure.

Installation

The CCTV system installed comprises one video recorder and up to nine fixed cameras at each selected St Martins premises. Additionally, door control/access systems comprise door cameras which may not record images. Where the CCTV installation is connected to the network, viewing access and control is achieved via a networked PC or a smart phone.

Justification for use

The use of CCTV to monitor entrances and other common areas is approved and signed-off. The system is intended to capture images of anti-social behaviour and of individuals entering or damaging property or removing goods without authorisation. Door control/access systems are to aid staff in recognising visitors and permitting their admittance. CCTV is not used in private areas within St Martins facilities. Monitoring of common and public areas will be conducted in a manner consistent with all other St Martins policies, including Privacy, Confidentiality, Information Governance, Data Protection, Code of conduct on use of computing facilities and other relevant policies.

St Martins
more than a home
for the homeless

Closed Circuit Television (CCTV)

Responsibilities

- St Martins Chief Executive Officer, or their nominated deputy, has the following responsibilities:
    - Oversee and co-ordinate the use of CCTV monitoring by St Martins.

- St Martins directors, or their nominated deputies, have the following responsibilities:
    - Sign-off of each CCTV installation;
    - Authorisation of disclosure requests.

- St Martins Senior Management Team has the following responsibilities:
    - Approval of each CCTV installation;

- St Martins services managers, or their nominated deputies, have the following responsibilities:
    - Ensure that all use of St Martins CCTV system is conducted in accordance with this policy and is consistent with the highest standards and protections;
    - Review camera locations and positions;
    - Recommend compliance with or rejection of disclosure requests.
    - Disclose recorded CCTV data in compliance with this policy and the CCTV procedure, and where authorised by the appropriate director;
    - Consider feedback and complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment;
    - Ensure that all areas being monitored are compliant with any privacy expectations of individuals within or outside St Martins and be confident that no infringement is likely to occur;
    - Report on the CCTV system as required by the Senior Management Team;
    - Ensure that CCTV data is stored in a secure place accessible by authorised personnel only;
    - Ensure that CCTV data is stored for a period not exceeding three calendar months and is then erased, unless requested by another organisation (see Disclosure, below) or required as part of a criminal investigation or court proceedings.
    - Ensure that a System Administrator is appointed for each CCTV installation.

- Authorised St Martins staff with access to the CCTV system have the following responsibilities:

- Fulfil disclosure requests passed from service managers, after approval by the appropriate director, in compliance with the relevant guidance and within 28 days of their submission;
- Annotate completed disclosure requests and arrange for their secure storage in Head Office.

- CCTV System Administrators have the following responsibilities:
  - install firmware upgrades;
  - configuration changes;
  - add/remove users (upon authorisation from the appropriate service manager).

Compliance

- Service managers and authorised staff with access to CCTV data are aware of their responsibilities under this policy, the restrictions which apply and the CCTV disclosure procedure to be followed when accessing and disclosing recorded images. Through this policy and procedure, St Martins complies with the Data Protection Act 2018 and the Information Commissioners Office (ICO) CCTV Code of Practice which ensures that CCTV is used responsibly and thereby establishes trust and confidence in its use.

- The CCTV system is used in a professional, ethical and lawful manner. Any use of CCTV for purposes other than those stated above (Purpose) is prohibited by this policy. For example CCTV is not used for monitoring normal staff activity or performance.

Data Protection Impact Assessments

- Where new CCTV systems or cameras are to be installed, St Martins will carry out a full Data Protection Impact Assessment (DPIA) identifying risks related to the installation and ensuring full compliance with data protection legislation. This may require consultation with people who use services, staff and local residents. St Martins will carry out a full DPIA on any upgrade or replacement of the system being considered.

Location of Cameras

- Cameras will be sited so they only capture images relevant to the purposes for which they are installed and care will be taken to ensure that reasonable privacy expectations are not violated. St Martins ensures that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection

Closed Circuit Television (CCTV)

Act 2018. Every effort is made to position cameras so that their coverage is restricted to St Martins premises. Cameras placed to monitor external areas are restricted in their view or positioned in such a way as to prevent or minimise recording of private property.

- Use of CCTV to monitor areas where individuals have a reasonable expectation of privacy is not justified. St Martins has selected the camera locations which are least intrusive to protect the privacy of individuals. CCTV is not used in private areas within residential facilities.

- CCTV monitoring of public areas may include the following:

    - **Premises and property:** premises perimeter, entrances and exits, lobbies and corridors, special storage areas, office locations, receiving areas for goods/services;
    - **Access Control Systems:** restricted access areas at entrances to premises and other areas;
    - **Security Alarms:** intrusion alarm panels, exit door controls, external alarms.

Covert Surveillance

- St Martins does not engage in covert surveillance.

Notification

- This policy is available to people who use St Martins services and visitors to St Martins premises, from St Martins' website. This policy is available to staff from St Martins' intranet. Notification signage, indicating that CCTV is in operation, is displayed at the entrance to those St Martins properties with CCTV installed. Signs include the contact details and the purpose for using CCTV.

Storage and Retention

- The images captured by the CCTV system are stored for a period not exceeding three calendar months and then erased, except where they are associated with a security incident and are retained specifically for investigation of that incident. In such cases, recordings are retained for three years from the date of recording. All CCTV recordings in all media are then erased and disposed of securely.

Closed Circuit Television (CCTV)

Secure Access

- CCTV recorded data is stored in a secure environment accessible only by authorised staff. A written access log is kept. Access control and maintenance of the CCTV system is the responsibility of the premises manager.

Disclosure

- Disclosure of CCTV data is managed by use of St Martins' Closed Circuit Television (CCTV) procedure, except where an Information Sharing Agreement (ISA) between St Martins and the requesting organisation takes precedence. CCTV data is released where an appropriate disclosure request is made in writing, including sufficient information to enable the data to be identified including date, time and location. Requests must be approved by the appropriate service manager and authorised by the appropriate director before the data is released. St Martins will respond to requests within 28 days, but reserves the right to refuse disclosure where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation. Spent disclosure requests are stored for three years at Head Office before secure destruction.

- Disclosure requests will be considered from:

    - Data subjects, or their legal representatives, pursuant to a Subject Access Request (individuals have the right to request access to CCTV data relating to themselves under the Data Protection Act 2018) or subject to a court order;
    - Police, local authority, fire brigade, HSE inspectors and HSE RIDDOR inspectors;
    - St Martins' insurance company where required in pursuance of a claim for damage at the insured property.

- Disclosed data is provided to the requestor in an appropriate format. Where data contains images relating to third parties, St Martins will take appropriate steps to mask and protect the identities of those individuals.

Complaints

- Complaints concerning the operation of CCTV will be considered when submitted via St Martins' Complaints Policy.

Staff Awareness

- Authorised staff, service managers, directors and CEO are aware of their responsibilities under this policy and understand that all CCTV data must be handled in its accord. Staff misuse of CCTV information will lead to disciplinary proceedings.

Closed Circuit Television (CCTV)

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.

Versions

Version	Changes	Date Changes made	Who signed off
0.1	First draft for pre SMT review	Jan 2021	
0.2	Amended draft including SMT comments, for review at SMT on 4 Feb 2021.	25 Jan 2021	
0.3	Amended draft including Pirry Keohane comments on 5 Feb 2021.	5 Feb 2021	
0.4	Amended draft inc comments from service managers meeting of 18/2/21	18 Feb 2021	
1.0	As agreed by service managers on 4/3/21.	4 March 2021	Service managers
1.1	Includes service manager's recommendation to disclose, signpost to the Closed Circuit Television (CCTV) procedure, and influence of Information Sharing Agreements.	27 April 2021	
2.0	Changes as v1.1 above.	5 May 2021	Service managers
3.0	Includes non-recording systems plus contact details for Data Protection Officer and Caldicott Guardian.	January 2023	Data Protection Officer

Closed Circuit Television (CCTV)

Associated Policies:

Privacy notice

Information Governance

Confidentiality

Data protection

Code of conduct on use of computing facilities

Complaints