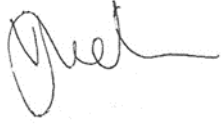




# CCTV POLICY

|  |  |                               |
|--|--|-------------------------------|
| <b>POLICY NO &amp; CATEGORY</b>                          | <b>IG 10</b>   | <b>Information Governance</b> |
| <b>VERSION NO &amp; DATE</b>                             | <b>5</b>   | <b>June 2023</b>              |
| <b>RATIFYING COMMITTEE</b>                               | <b>Clinical Governance Committee</b>   |                               |
| <b>DATE RATIFIED</b>                                     | <b>June 2023</b>   |                               |
| <b>NEXT REVIEW DATE</b>                                  | <b>June 2026</b>   |                               |
| <b>EXECUTIVE DIRECTOR</b>                                | <b>Executive Director of Operations</b>  |                               |
| <b>POLICY LEAD</b>                                       | <b>Trust Local Security Management Specialist.</b>                                   |                               |
| <b>POLICY AUTHOR</b>                                     | <b>As Above</b>  |                               |
| <b>Exec Sign off Signature (electronic)</b>              |  |                               |
| <b>Disclosable under Freedom of Information Act 2000</b> | <b>Yes</b>   |                               |

## Policy context

- To provide guidance in support of Trust wide security systems that create a safe working environment for patients, service users and staff.

## Policy requirement (see Section 2)

- To document and set out how to regulate the management and operations of systems in compliance with the Data Protection Acts (DPA) 2018 and General Data Protection Regulations (GDPR) in relation to the use of Closed-Circuit Television Systems (CCTV).

# CONTENTS

|   | Page(s)   |
|---|-----------|
| <b>1. Introduction</b>  | <b>3</b>  |
| 1.1 Rationale   | 3         |
| 1.2 Scope   | 3         |
| 1.3 Principles  | 4         |
| <b>2. Policy</b>  | <b>4</b>  |
| <b>3. Corporate Procedure</b>   | <b>6</b>  |
| 3.1 Pre-Installation Requirements   | 6         |
| 3.2 Quality of Images   | 6         |
| 3.3 Processing and retention of Images  | 7         |
| 3.4 Requests for Access   | 8         |
| 3.5 Covert Surveillance   | 11        |
| 3.6 Training  | 11        |
| <b>4. Responsibilities</b>  | <b>11</b> |
| <b>5. Development and Consultation Process</b>                                    | <b>16</b> |
| <b>6. Audit and Assurance</b>   | <b>16</b> |
| <b>7. Reference Documents</b>   | <b>17</b> |
| <b>8. Bibliography</b>  | <b>18</b> |
| <b>8. Glossary</b>  | <b>18</b> |
| <b>9. Appendices</b>  | <b>18</b> |
| Appendix 1 Equality Impact Assessment   | 19        |
| Appendix 2 Local Operating Procedure for Body Worn CCTV                           | 23        |
| Appendix 3 Information Leaflet  | 26        |
| Appendix 4 Data Protection Act Definitions  | 27        |
| Appendix 5 Assessment Framework for Mental Health Act<br>Commissioners and Others | 29        |

# INTRODUCTION

## 1.1 RATIONALE

- 1.1.1 The rationale and purpose of this policy is primarily as part of Trust wide security systems to create a safe and secure environment for our service users, visitors and staff.
- 1.1.2 It also sets out to regulate the management and operations of systems to comply with the Data Protection Acts (DPA) 2018 and General Data Protection Regulations (GDPR) in relation to the use of Closed-Circuit Television Systems (CCTV) and camera surveillance within Birmingham and Solihull Mental Health NHS Foundation Trust (BSMHFT). Under the DPA 2018 legally enforceable standards apply to the collection of data (images).
- 1.1.3 In addition to the DPA 2018 and GDPR, the Information Commissioners Office (ICO), has also produced guidance as to the use of CCTV called, **In the picture: A data protection code of practice for surveillance cameras and personal information**. If any CCTV shows a recognisable person, it is classed as personal identifiable data and therefore covered under DPA 2018 and GDPR. The ICO Guidance has the dual purpose of assisting organisations /operators using CCTV systems to understand their legal obligations at the same time reassuring the public that appropriate safeguards are in place.

## 1.2 SCOPE

- 1.2.1 This policy applies to all staff (substantive, agency, contractor, temporary, those in partnership / under contract, volunteers, students, or apprentices) within BSMHFT and others working on behalf of the Trust, in respect of the use of CCTV Camera Surveillance. It describes what CCTV systems may be used for, how they are to be specified, installed, maintained, and operated and who is to be responsible for them. It sets out the rights of access by 'subject persons' to recorded data and images. The policy also details limitations on the use of covert CCTV surveillance, which is covered by the Regulation of Investigatory Powers Act (RIPA) 2000.
- 1.2.2 This policy applies to all use of CCTV within BSMHFT including where facilities are owned, managed, or operated under contract or Private Finance Initiatives (PFI) arrangements. Where buildings are leased or occupied under shared use arrangements assurances must be obtained and form part of the relevant contractual agreement from landlords that CCTV systems installed within these premises comply with legislation/guidance and requirements of this policy. BSMHFT services provided within HMP Birmingham must follow prison policy in relation to CCTV and therefore are NOT covered under this policy document.

## **1.3 PRINCIPLES**

1.3.1 Trust CCTV systems are registered with the ICO as being intended to help provide a safe and secure environment for staff, service users, their carers, and visitors, and specifically be for the following purposes:

- To maintain security of individuals and property in a vulnerable area.
- To protect and maintain the wellbeing of service users, staff, and visitors and to keep our service users clinically safe and secure.
- To provide guidance when valid requests are made for access to recorded CCTV images and data.
- To prevent and detect crime and to facilitate the apprehension and prosecution of offenders and apprehension of suspected offenders.
- Internal Trust investigations

1.3.2 All routine use of CCTV will be overt, that is cameras will be sited in plain view and the use of CCTV publicised using signage etc.

## **2. POLICY**

2.1 Prior to considering compliance with the principles of the DPA 2018 and GDPR, a user of CCTV or similar surveillance equipment, will need to determine:

**The type of personal data being processed i.e., is there any personal data as defined by the Act.**

In accordance with the Trust Confidentiality Policy and the Data Protection Principles, contained in the DPA 2018, personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes and not in any manner incompatible with those purposes.
- Adequate, relevant, and not excessive.
- Accurate.
- Not kept for longer than is necessary.
- Secure.

2.2 Prior to installation the purpose(s) of any CCTV installation must be established and documented, and be consistent with the circumstances listed in Article 8 of the European Convention on Human Rights e.g.:

- Public safety
- The prevention of disorder and crime

2.3 The use of CCTV in clinical areas must be justified and for specific purposes but any use must be given careful consideration in terms of the extent to which it is necessary for safety and security, balanced against the level of interference with the privacy of individuals. There is also specific guidance provided by the Department of Health with the Health Building Note 03-01 and the Environmental Design Guide.

- 2.4 To enhance the safety of Service Users and staff within Seclusion Rooms and associated facilities, CCTV equipment will be routinely installed.
- 2.5 The installation of CCTV equipment within a clinical area/seclusion suite will not replace the usual observations employed by staff. Its provision is to allow observation specifically for areas of reduced natural lines of sight and to address the consequences of service users' actions/attempts to prevent staff undertaking observations.
- 2.6 Where CCTV is installed within clinical areas and/or seclusion suites then appropriate warning signs must be clearly displayed at the entrance to the area and within the specific location. Service Users will also be informed verbally on admission to the facility by clinical staff, at service user forums or as soon as practicable following admission, that CCTV systems are used within the clinical area. This is known as a Fair Processing Notice and must be issued.
- 2.7 Where CCTV cameras are installed within clinical areas, access to the associated CCTV monitors is restricted to on duty Trust staff allocated to work in that specific area. CCTV systems within clinical areas are installed to allow observations for the purposes of safety & security for both the staff and patients.
- 2.8 Where staff are found to be misusing CCTV or abusing their position to inappropriately access footage, they will be subjected to disciplinary proceedings under the Trust's disciplinary procedure and could face criminal proceedings.
- 2.9 With reference to para 2.8, the relevant manager must consider potential safeguarding risks to vulnerable individuals. Trust Safeguarding colleagues should be contacted to assess these risks. [Managing Safeguarding Allegations Concerning People in a Position of Trust \(Policy HR37\)](#) refers.
- 2.10 Where CCTV is installed within nonclinical areas e.g., receptions, individuals are to be informed using appropriate signage notifying that CCTV is in use. Where anyone is identified as being visually impaired or identifies themselves as such, Trust staff should verbally inform them that CCTV is in use within the building and the purposes for this.
- 2.11 Managers who have CCTV systems within their units must ensure that systems are being used in accordance with the law, that all staff have read and understood this policy and that only authorised and appropriately trained, competent staff use the CCTV systems installed. All such training will be documented within staff's individual training records (see para 3.6).
- 2.12 Where CCTV systems develop faults these will be reported promptly and repaired as soon as is practicable. Faults relating to network/software issues are to be reported to ICT Service Desk and equipment faults/failures should be reported to the relevant SSL Estates and Facilities Department helpdesk.

- 2.13 Police officers routinely use Body Worn Cameras (BWC) when attending incidents including those within mental health settings. This is now also legislated within the Mental Health Units (Use of Force) Act 2018. This means that:
- a) Police will utilise BWC when called to mental health settings because of violence or to assist staff in response to an emergency that may involve officers and the use of physical restraint, recordings can be used in evidence.
  - b) The decision whether to use BWC is a judgement for the Police officer(s) to make and it should be the exception NOT to deploy BWC in such circumstances which they will have to explain/justify.
  - c) Recordings of BWC are strictly controlled by Police and assurances that patient confidentiality will be maintained have been given. An Information Sharing Protocol between West Midlands Police and the Trust is covered by a separate document policy.
- 2.14 Where Body Worn Cameras are used by Security Officers who are contracted to work within the Trust (currently only within the Birmingham New Hospitals PFI estate), their use will be restricted to public areas of buildings, such as reception areas, foyers, and waiting rooms. They will also be utilised in all publicly accessible external areas of Trust buildings.
- 2.15 For the purposes of this policy, BWC's used by Trust staff or contracted staff working on behalf of the Trust, are classified as an extension of the Trust CCTV systems and all associated recorded data is to be managed as detailed within this policy. A BWC Operating Procedure can be found at Appendix 2 of this policy.

### **3. CORPORATE PROCEDURE**

#### **3.1 Pre-Installation Requirements**

- 3.1.1. The use of CCTV can have a positive impact in managing security related risks. However, poorly specified systems can raise expectations that cannot be achieved. When considering the installation or the extending of existing CCTV systems, the LSMS, Operational/Service Managers and SSL Estates colleagues will meet to determine the extent and purpose of the proposed installation and to agree the specification of the equipment to be installed.

#### **3.2. Quality of Images**

- 3.21. It is a key facet for the use of CCTV that the quality of images produced by the equipment is adequate for the purpose that the scheme was established for. The Trust CCTV schemes are established for the prevention and detection of crime, the apprehension and prosecution of offenders and record other occurrences for example H&S incidents and monitor access and egress of people.

It is essential therefore that images recorded and available to view are of high quality to be of use to investigators and evidential purposes, the technical standards to achieve this are set out in British Standard EN 62676.

Data/Images must be processed in a manner consistent with the legal rules of evidence in terms of continuity.

### 3.2.2 The following standards are to be applied to Trust CCTV equipment:

- Upon installation an initial check should be undertaken to ensure that the equipment performs properly by the installer and monitored by SSL.
- To ensure consistent quality of images, a digital recording format should be specified, and CCTV must be capable of clearly identifying all persons entering sites/buildings and their actions/behaviour when within its field of view.
- System functions such as location and a date/time reference must be accurate. Audits will be completed by the LSMS annually to ensure the accuracy of this information. The system must be capable of automatically or remotely being changed to the correct to either GMT or BST as necessary.
- Cameras should be situated so that they capture images relevant to the purpose for which the scheme was established.
- CCTV cameras within seclusion suites are to be sited to ensure that all areas within the facility can be fully observed if observation panels are deliberately obscured.
- If cameras or equipment become defective there is a clear procedure for ensuring the equipment is repaired under existing maintenance contracts by reporting the fault to the appropriate SSL Estates helpdesk.
- Signs must be displayed so that persons are aware that they are entering an area which is covered by surveillance equipment. This is a requirement of the Data Protection Act which requires organisations to be fair and lawful about any processing of personal data. These signs must be clearly visible and legible and contain the following information:
  - **The identity of the organisation responsible for the scheme (The Data Controller) i.e., Birmingham and Solihull Mental Health NHS Foundation Trust.**
  - **The purpose of the scheme:**
    - ❖ Crime prevention and detection.
    - ❖ Apprehension and Prosecution of offenders.
    - ❖ Safety and Security of Service Users and Staff
    - ❖ Trust Investigations
  - **Anything else deemed necessary e.g., Details of whom to contact regarding the scheme and a telephone number.**

### 3.3. Processing and retention of Images

- 3.3.1. Monitors displaying images from areas in which individuals would have an expectation of privacy should not be viewed by anyone other than Trust employees who are on duty and authorised to be within the relevant area. It should be noted that a greater expectation of privacy is likely in clinical areas

than may apply in external or “public” areas of facilities such as car parks, entrances, or internal corridors.

- 3.3.2. It is acceptable for images from the exterior of a building to be viewed by security or reception staff, whilst it is not acceptable or appropriate for anyone other than on duty clinical staff to view images from clinical inpatient areas.
- 3.3.3. This must be considered when determining where to locate the CCTV monitors and images should not be accessible to unauthorised staff or visitors, e.g., not in reception areas where monitors and images can be seen.
- 3.3.4. CCTV monitors within clinical areas/seclusion suites must not be routinely switched on or used by staff to observe service users, unless there has been a deliberate attempt by a service user to impede staff observing them. Any decision to switch on a CCTV monitor in a clinical area/seclusion suite to observe service users will be made by the senior staff member on duty and fully documented within the relevant RiO progress notes. See [Seclusion and Segregation policy](#) for more detailed information.
- 3.3.5 BSMHFT will retain CCTV images for a period of 30 days following which footage will be deleted. Routinely, footage should not be retained for longer than is necessary, as stated by DPA 2018 and GDPR.
- 3.3.6 Where an incident has occurred, and CCTV footage that is of evidential value is available, then this footage will be downloaded and saved for the purposes of investigation. Once such a request has been received, the data must be retained. This is a requirement of the Department of Health Code of Practice on record retention.
- 3.3.7 Once the retention period has expired all recorded images are automatically re-recorded over. Images retained for evidential purposes are to be stored in a secure location to which access is controlled.

## **3.4 Requests to Access Footage**

- 3.4.1. All requests for CCTV footage will be dealt with by the Information Requests Team who will locate, review, and secure the images requested. Requests should be sent to: [bsmhft.informationrequests@nhs.net](mailto:bsmhft.informationrequests@nhs.net) If required, leads at Trust sites must assist the Information Requests Team with gaining copies of footage within 7 working days.
- 3.4.2 The Information Requests Team will not accept requests for CCTV footage from individuals (including staff) following damage or vandalism to property or physical harm. In these circumstances the Information Requests Team must receive a formal request from either the Police or an individual's insurance company (which in the case of an insurance company the request must include a copy of the individual's consent to release the footage). In addition, it is important to note that the Information Requests Team will not locate, review, or secure any footage until an appropriate and valid request has been received from either the Police or insurance company. If the formal request is



received after the 30-day retention schedule the footage will no longer be available.

3.4.3. In accordance with data protection legislation, the Trust has 30 calendar days from receipt of a valid and complete request for CCTV footage to locate, review, redact (if required) and release the footage.

3.4.4 The Information Requests Team will need to determine whether the images of third parties are held under a duty of confidence. In general terms images recorded from outside the hospital buildings and in public areas such as reception areas etc. are unlikely to be held under a duty of confidence. Images recorded within waiting rooms and clinical areas are likely to be considered as being held under a duty of confidence.

3.4.5 The Information Requests Team will retain a record of all CCTV requests for audit purposes that will include the following information:

- The identity of the individual making the request.
- The date of the request
- The reasons for agreeing or refusing to supply the images requested
- The name and signature of the manager making the decision
- The date the request was completed.

3.4.6 Before releasing any footage, the Information Requests Team will burn the footage onto disc applying encryption. The password will be sent separately to the disc. For discs that are being collected in person the Information Requests Team will request that a confirmation of collection letter is signed by the recipient.

3.4.7 Any requests received for the disclosure of CCTV footage under the Freedom of Information Act 2000 will be directed to the Freedom of Information Office, where such requests will be considered within the strict guidelines of the Act.

### **3.4.8 Individuals**

3.4.8.1 Images of individuals captured by CCTV cameras constitutes as their personal data. Under the DPA 2018 and GDPR, individuals have the right to obtain copies of their personal data and a description of such data, the purposes for which it is being processed and the recipients (or classes of recipients) to whom it may be disclosed.

3.4.8.2 For an individual to request CCTV footage of themselves the Trust's subject access request (SAR) process must be followed, in accordance with the Trust's policy and procedure. Before the footage is released it will be located and reviewed by the Information Requests Team. In instances where no recorded images are retained (instantaneous viewing only) individuals will be informed that the system produces no recordable images.

3.4.8.3 Until a request for CCTV footage has been determined as being valid and complete, the Information Requests Team will not locate, review or secure any footage. If a valid and complete request is not submitted in a timely

manner this may result in the footage being destroyed before being secured due to the 30-day retention period.

### **3.4.9 Internal Requests for Investigation Purposes**

- 3.4.9.1 Internal requests for CCTV footage for the purpose of internal investigations must only be made in writing to the Information Requests Team from either the Associate Directors, Heads of Service, or lead investigator with specific reasons as to why the footage is required.
- 3.4.9.2 Until the request for CCTV footage has been determined as being valid and complete, the Information Requests Team will not locate, review, or secure any footage. If a valid and complete request is not submitted in a timely manner this may result in the footage being destroyed before being secured due to the 30-day retention period.

### **3.4.10 Police Requests**

- 3.4.10.1 When the Police request access to CCTV footage a complete and valid WA170 form must be submitted to the Information Requests Team. A WA170 form allows a data controller to decide if the request is proportionate and the footage can be released. The Information Requests Team will locate, review, and secure the footage.
- 3.4.10.2 Where there is an urgent operational need for CCTV footage to be accessed by the Police, this must be provided following approval from an appropriate senior manager or on call manager. An example would be a vulnerable missing person report, other possible clinical risks involving high risk individuals initiated by the Trust, or investigation of serious crimes. A documented record/Eclipse Incident report must be made by the senior nurse/manager on duty detailing why CCTV footage was accessed and by whom. If due to the urgent nature it is not possible for the Police to provide a completed WA170 form, this must be submitted to the Information Requests Team retrospectively and no later than the following working day of the incident.
- 3.4.10.3 Until the request for CCTV footage has been determined as being valid and complete, the Information Requests Team will not locate, review, or secure any footage. If a valid and complete request is not submitted in a timely manner this may result in the footage being destroyed before being secured due to the 30-day retention period.

### **3.4.11 Insurance Companies / Solicitors**

- 3.4.11.1 Insurance Companies representing individuals wishing to access images from the Trust CCTV system need to make a formal written request to the Information Requests Team, providing proof of the individuals consent who they are representing.
- 3.4.12. Until the request for CCTV footage has been determined as being valid and complete, the Information Requests Team will not locate, review, or secure

any footage. If a valid and complete request is not submitted in a timely manner this may result in the footage being destroyed before being secured due to the 30-day retention period.

### 3.5 Covert Surveillance

- 3.5.1 Within BSMHFT premises the use of CCTV must be generally overt. CCTV schemes established under this policy mean people must be made aware that a CCTV scheme is in operation, and it may only be used for clearly defined and specified purposes.
- 3.5.2 The targeted, deliberate, and covert monitoring or observation of specific persons, including their movements or activities could amount to directed or intrusive surveillance for the purposes of the Regulation of Investigatory Powers Act 2000. (RIPA) This Act provides that such covert surveillance can only be authorised with regard to the “proportionality and collateral intrusion test” and carried out by specified authorities (e.g., Police).
- 3.5.3 In some circumstances, a specified authority that is lawfully able to authorise covert surveillance under the Act (e.g., the police) may request the Trust’s assistance in carrying out such surveillance for the purposes of a specific investigation.
- 3.5.4 Such activity will only be permitted with approval of the Executive Director of Operations, following advice from the LSMS, and being satisfied it is lawful and appropriate to carry out such activity.
- 3.5.5 Any request from the Police to use premises from which the Trust operates to conduct covert surveillance not linked to the Trust’s activities must be discussed with the LSMS.

### 3.6 Training

- 3.6.1 Specific operational training will be provided to authorised users by the suppliers of the relevant CCTV equipment.

## 4. RESPONSIBILITIES

| Post(s)                         | Responsibilities  | Ref |
|---------------------------------|---|-----|
| Chief Executive                 | The DPA 2018 and GDPR requires that an individual be nominated as Data Controller. The Data Controller is “a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed”. The Chief Executive has the overall statutory responsibility for Data Protection within the Trust. |     |
| Service, Clinical and Corporate | Service Directors are responsible for ensuring compliance with the policy within their directorate and are to disseminate it within their areas of  |     |

|                                       |   |  |
|---------------------------------------|---|--|
| Directors                             | responsibility, with any amplifying instructions/guidance relevant to their directorates. Service Directors may devolve the day-to-day running of the scheme to a designated person (System Manager), normally the manager of the facility or location, on larger or shared sites agreement will be reached as to who manages the system on a day-to-day basis. This individual is the CCTV System manager. |  |
| Deputy Director of ICT and Programmes | All CCTV SARS from individuals, third parties and the Police will be managed by the Information Requests Team who report to the Deputy Director of ICT and Programmes who will arrange for all such requests to be reviewed and the applicable images located. All such requests or enquires received must be directed to the Information Requests Team.  |  |
| Information Requests Team             | The Information Requests Team are responsible for ensuring requests for CCTV footage are valid and lawful. Once this has been determined, the team are responsible for securing and viewing the footage. In addition, the team are responsible for ensuring the footage is saved appropriately and encrypted before being shared.   |  |
| Head of Records and Clinical Coding   | The Head of Records and Clinical Coding is responsible for providing advice to the Local Security Management Specialist (LSMS) and Systems Managers who are designated as the responsible persons, on the disclosure of material in response on SARs.   |  |

|   |  |  |
|---|--|--|
| Policy Lead,<br>Local security<br>management<br>Specialist (LSMS) | <p>The LSMS is responsible for advising Managers across the Trust on the use of CCTV systems. They will advise and assist Local Managers with any proposed additions or changes to current CCTV system(s).</p> <p>The LSMS conducts an annual programme of security audits of Trust premises, which incorporates a review of CCTV systems to ensure that they are operated in accordance with the relevant legislation and Codes of Practice.</p> <p>Where staff are provided under contract, who may be called upon to operate CCTV systems the LSMS is to ensure that adequate assurances are in place that contractors staff are suitably trained and where applicable licensed in accordance with the Private Security Industry Act (2000), to carry out their assigned tasks.</p> <p>They are responsible for providing guidance regarding operational requirements for CCTV systems and advising on the use of any covert or directed CCTV surveillance.</p> <p>The LSMS is responsible for providing advice on the provision of access and material to law enforcement agencies including the police, as well as advising on the provision of system upgrades/software or additional equipment, in collaboration with Estates, ICT and Data Protection Officer.</p> |  |
| Information Asset<br>Owner  | <p>The nominated IAO for CCTV matters will complete and maintain the required asset documentation including the Data Privacy impact Assessment as required. (DPIA)</p> <p>This involves issues of privacy and confidentiality when the organisation carries out any task that involves processing or sharing personal data/information or commercially sensitive data/information. This is to address any privacy concerns, to assess privacy risks to individuals in the collection, use, storage, disclosure and disposal of data/information or any other processing that is likely to result in a substantial risk to individuals' interests.</p>  |  |
| Summerhill<br>Services Limited<br>(SSL)                           | <p>SSL provide the Estates &amp; Facilities services to the Trust. They are responsible for advising, assisting, and arranging in the procurement and maintenance of CCTV equipment.</p> <p>They will ensure that fault reports received are actioned and repairs made by ICT in respect of network faults or arrange for contractors/service provider(s) at the earliest opportunity to repair other</p>  |  |

|                                       |  |  |
|---------------------------------------|--|--|
|                                       | <p>breakdowns/failures.</p> <p>They will monitor systems so that when faults/breakdowns occur action is taken to return them to normal operation with the minimum of delay.</p>  |  |
| Information Communications Team (ICT) | <p>ICT are responsible for ensuring that at all times there are staff/resources/arrangements are in place to maintain Trust networked systems, so they are performing fully and effectively.</p> <p>ICT provide support for network connectivity to enable the use of CCTV equipment and the associated software.</p>  |  |
| Site CCTV System Managers             | <p>Trust CCTV systems are operated either for the benefit of one department/area or for several areas/groups. CCTV systems provided under PFI contractual arrangements will be administered by the provider on behalf of the Trust, whilst systems that are restricted to a specific area will be administered by a nominated individual within that area. Those responsible for overseeing CCTV measures at the Trust must not abuse their position. They must not video CCTV recordings on mobile devices to share with others or discard recordings for personal benefit.</p> <p>Where staff are found to be abusing their position, they will be subject to disciplinary proceedings under the Trust's disciplinary procedure and could face criminal proceedings. Trust Safeguarding colleagues should also be contacted to assess any risks to vulnerable individuals and the implementation of PiPOT procedures where appropriate.</p> <p>System managers are to:</p> <p>Engage with the LSMS to ensure that the CCTV system in use is operated in accordance with Data Protection Legislation and the Information Commissioners Code of Practice.</p> <p>Produce local operating instructions for the CCTV System(s) they are responsible for.</p> <p>Ensure that only authorised individuals have access to CCTV system and data captured and stored by it.</p> <p>Ensure that staff operating the CCTV system have received appropriate training to enable them to fulfil the requirements of their role as detailed below.</p> <p>Ensure that the system is operating and maintained correctly. This includes ensuring that daily/weekly checks are carried out, and that correct time/date stamp is displayed. All such checks should be fully</p> |  |

|                         |   |  |
|-------------------------|---|--|
|                         | <p>documented to demonstrate that such checks have been completed and if necessary, what actions have been taken.</p> <p>Ensure that the Information Governance Team is informed of all CCTV SARS and that the Trust discharges its legal obligations in this regard. The Information Governance Team will complete the CCTV SAR.</p> <p>Ensure that any Faults/Issues with the operation of the system are reported to the relevant Estates team.</p> <p>Attend relevant training events as required to ensure the CCTV system they are responsible for is operated in accordance with Data Protection Legislation and the Information Commissioners Code of Practice.</p>   |  |
| Team Managers           | <p>Data Protection Legislation and the Information Commissioner's CCTV Codes of Practice include a requirement that all staff are to be aware of the rights of an individual in relation to Data Protection. Line Managers at all levels within the Trust are to ensure that this policy is communicated to all those staff that they have management responsibilities for and who are required to operate CCTV systems during their role.</p>  |  |
| All Staff & Contractors | <p>All Staff have a personal responsibility for security. This includes maintaining the confidentiality of security issues within the Trust, including the operating procedures and capabilities of CCTV systems.</p> <p>Staff are to inform the Information Governance Team and the LSMS, through their manager, of any official contact they might have with the Police or other external agency with a security responsibility, where such contact is related to or might impact on the Trust use of CCTV systems. This includes requests from the Police for disclosure of CCTV images. All requests must be sent to the Information Governance Team to action.</p> <p>Security operatives supplied under contract to the Trust must possess a public space surveillance (CCTV) licence. Under the provisions of the Private Security Industry Act 2001, it is a criminal offence for staff to be contracted as public space CCTV operators in England, Wales, and Scotland without an SIA licence. Contractors operating CCTV systems on behalf of the Trust, will be expected to do so in accordance with Trust policy. Any misuse of the Trust CCTV systems will not be tolerated.</p> |  |

## 5. DEVELOPMENT AND CONSULTATION PROCESS

| Consultation summary                                  |  |  |
|---|--|--|
| Date policy issued for consultation                   |  | January 2023                                   |
| Number of versions produced for consultation          |  | 1  |
| Committees / meetings where policy formally discussed |  | Date(s)  |
| Trust Health & Safety Committee                       |  | January 2023                                   |
| Information Governance Steering Group                 |  | January 2023                                   |
| Trust wide Consultation                               |  | January 2023                                   |
| PDMG  |  | March 2023                                     |
| Where received  | Summary of feedback  | Actions / Response                             |
| Counter Fraud Service                                 | Comments provided in relation to disciplinary and criminal proceedings where abuse of position identified for system managers and contractors when accessing/operating CCTV systems on behalf of Trust.<br>Monitoring element to highlight policy review period and changes in response to legislation changes or in response to identified breach of process. | Policy amended to reflect comments made.       |
| SSL Estates   | Clarification around retention periods in para 3.3.5   | Paragraph amended.                             |
| PDMG  | Amendment to para 2.9<br>Amend Equality Assessment Human Rights section re abuse of position and disciplinary actions.<br>Reference to Safeguarding as above.  | Document amended to reflect feedback received. |

## 6. AUDIT AND ASSURANCE

Implementation of this policy will be monitored through regular audits across the Trust; interviewing staff and service users and regularly reviewing confidentiality incidents.

Incidents will be logged and reported to the relevant Information Governance Assurance meeting, and where applicable taken to the Information Governance Steering Group (IGSG).

| Element to be monitored                                     | Lead                                | Tool   | Frequency | Reporting Committee |
|---|-------------------------------------|--------|-----------|---------------------|
| Compliance with 30-day deadline for completion of CCTV SARs | Head of Records and Clinical Coding | Report | 6 monthly | IGSG                |



|  |             |   |  |               |
|--|-------------|---|--|---------------|
| SSL will ensure that fault reports received are actioned and repairs necessary repairs completed.                  | SSL Manager | All fault calls to be directed to ICT helpdesk then forwarded to SSL manager dedicated to CCTV. They will then forward to unit SSL manager to action repairs. CCTV assets register to be updated with any changes to the system | When faults are reported                                 | IGC           |
| ICT to ensure that connectivity between CCTV equipment and its associated software operates correctly.             | Head of ICT | ICT Technicians checking network system   | When faults reported                                     |               |
| System effectiveness, compliance with purpose of the policy.   | LSMS        | Reports from ICT/IG Team/SSL  | Annually, or during system upgrades                      | H&S Committee |
| The policy will be reviewed every 3 years, or when legislation changes or after a breach of the policy guidelines. | LSMS        | Incident Reports. Updates from IGSG   | As required or in accordance with policy review schedule | H&S Committee |

## 7. REFERENCE DOCUMENTS

- Trust Confidentiality Policy (IG01)
- Trust Managing Safeguarding Allegations Concerning People in a Position of Trust (HR37)
- CCTV Code of Practice. Information Commissioner Office 2000
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998.
- Data Protection Act 2018.
- Freedom of Information Act 2000
- EU General Data Protection Regulation (2016)

- Mental Health Units (Use of Force) Act 2018
- In the Picture: A data protection code of practice for surveillance cameras and personal information (2017) – Information Commissioner’s Office
- Private Security Industry Act 2001.
- The Use of CCTV in NHS and Independent Mental Health Units: A Framework for Assessment. Mental Health Act Commission (2005)
- Department of Health Building Note 03-01
- Department of Health Environmental Design Guide

## 8. BIBLIOGRAPHY

- CCTV operational requirements manual Version 4.0. Publication No. 55/06. Home Office Scientific Development Branch 2007.
- UK Police requirements for digital CCTV systems. Publication No. 09/05. Home Office Police Scientific Development Branch.
- Management & Operation CCTV Code of Practice, BS 7958;1999. British Standards Institute 1999.
- BSMHT Non-Care Records Management Policy, IG04A.

## 9. GLOSSARY

|               |   |
|---------------|---|
| CCTV          | Closed Circuit Television                         |
| DPA           | Data Protection Acts 2018                         |
| DVR           | Digital Video Recorder                            |
| LSMS          | Local Security Management Specialist              |
| MHAC          | Mental Health Act Commission                      |
| PFI           | Private Finance Initiative                        |
| PTZ           | Pan, Tilt & Zoom (fully controllable CCTV camera) |
| BWC           | Body Worn camera systems                          |
| RIPA          | Regulation of Investigatory Powers Act 2000       |
| SAR           | Subject Access Request                            |
| MOU           | Memorandum of Understanding                       |
| LOP           | Local Operating Procedure                         |
| AWOL          | Absent Without Leave                              |
| LSMS          | Trust Security Manager                            |
| Covert Camera | Hidden Camera                                     |

## 10. Appendices

|            |   |
|------------|---|
| Appendix 1 | Equality Impact Assessment  |
| Appendix 2 | Local Operating Procedure for Body Worn CCTV                        |
| Appendix 3 | Information Leaflet   |
| Appendix 4 | Data Protection Act Definitions                                     |
| Appendix 5 | Assessment Framework for Mental Health Act Commissioners and Others |

## Appendix 1

### Equality Analysis Screening Form

A word version of this document can be found on the HR support pages on Connect

<http://connect/corporate/humanresources/managementsupport/Pages/default.aspx>

|   |                                      |                       |                                      |
|---|--------------------------------------|-----------------------|--------------------------------------|
| <b>Title of Proposal</b>  | <b>CCTV Policy</b>                   |                       |                                      |
| <b>Person Completing this proposal</b>  | <b>Stephen Laws</b>                  | <b>Role or title</b>  | <b>LSMS</b>                          |
| <b>Division</b>   | <b>Operations Directorate</b>        | <b>Service Area</b>   | <b>Acute &amp; Urgent Care</b>       |
| <b>Date Started</b>   | <b>30<sup>th</sup> November 2022</b> | <b>Date completed</b> | <b>16<sup>th</sup> December 2022</b> |
| <b>Main purpose and aims of the proposal and how it fits in with the wider strategic aims and objectives of the organisation.</b>   |                                      |                       |                                      |
| Review/update of existing CCTV Policy to ensure compliance with legislation (GDPR 2018) and Information Commissioners Guidance & Mental Health Units (Use of Force) Act 2018  |                                      |                       |                                      |
| <b>Who will benefit from the proposal?</b>  |                                      |                       |                                      |
| All users of Trust buildings. CCTV systems are provided to support a secure and safe environment for its Services Users, Staff, Authorised Visitors and Contractors.  |                                      |                       |                                      |
| <b>Do the proposals affect service users, employees, or the wider community?</b><br><i>Add any data you have on the groups affected split by Protected characteristic in the boxes below. Highlight how you have used the data to reduce any noted inequalities going forward</i> |                                      |                       |                                      |
| No. The Trust CCTV systems are passive systems (not monitored), that monitor and record images from external and internal areas of Trust buildings for the purposes of crime deterrence and detection, safety & security.   |                                      |                       |                                      |
| <b>Do the proposals significantly affect service delivery, business processes or policy?</b><br><i>How will these reduce inequality?</i>  |                                      |                       |                                      |
| No.   |                                      |                       |                                      |
| <b>Does it involve a significant commitment of resources?</b><br><i>How will these reduce inequality?</i>   |                                      |                       |                                      |
| No.   |                                      |                       |                                      |

|   |                          |  |                        |  |
|---|--------------------------|--|------------------------|--|
| <b>Do the proposals relate to an area where there are known inequalities? (e.g. seclusion, accessibility, recruitment &amp; progression)</b>  |                          |  |                        |  |
| CCTV systems will be installed within purpose-built Trust seclusion suites. These are installed to maintain the safety of service users and enable observing staff an ability to maintain therapeutic observations where attempts have been made to obscure vision panels.  |                          |  |                        |  |
| <b>Impacts on different Personal Protected Characteristics – Helpful Questions:</b>   |                          |  |                        |  |
| Does this proposal promote equality of opportunity?<br>Eliminate discrimination?<br>Eliminate harassment?<br>Eliminate victimisation?   |                          | Promote good community relations?<br>Promote positive attitudes towards disabled people?<br>Consider more favourable treatment of disabled people?<br>Promote involvement and consultation?<br>Protect and promote human rights? |                        |  |
| <b>Please click in the relevant impact box and include relevant data</b>  |                          |  |                        |  |
| <b>Personal Protected Characteristic</b>  | <b>No/Minimum Impact</b> | <b>Negative Impact</b>   | <b>Positive Impact</b> | <b>Please list details or evidence of why there might be a positive, negative or no impact on protected characteristics.</b> |
| <b>Age</b>  | <b>X</b>                 |  |                        |  |
| Including children and people over 65<br>Is it easy for someone of any age to find out about your service or access your proposal?<br>Are you able to justify the legal or lawful reasons when your service excludes certain age groups   |                          |  |                        |  |
| <b>Disability</b>   | <b>X</b>                 |  |                        |  |
| Including those with physical or sensory impairments, those with learning disabilities and those with mental health issues<br>Do you currently monitor who has a disability so that you know how well your service is being used by people with a disability?<br>Are you making reasonable adjustment to meet the needs of the staff, service users, carers and families? |                          |  |                        |  |
| <b>Gender</b>   | <b>X</b>                 |  |                        |  |
| This can include male and female or someone who has completed the gender reassignment process from one sex to another<br>Do you have flexible working arrangements for either sex?<br>Is it easier for either men or women to access your proposal?   |                          |  |                        |  |
| <b>Marriage or Civil Partnerships</b>   | <b>X</b>                 |  |                        |  |
| People who are in a Civil Partnerships must be treated equally to married couples on a wide range of legal matters<br>Are the documents and information provided for your service reflecting the appropriate terminology for marriage and civil partnerships?   |                          |  |                        |  |

|   |          |  |          |   |
|---|----------|--|----------|---|
| <b>Pregnancy or Maternity</b>   | <b>X</b> |  |          |   |
| This includes women having a baby and women just after they have had a baby<br>Does your service accommodate the needs of expectant and post-natal mothers both as staff and service users?<br>Can your service treat staff and patients with dignity and respect relation in to pregnancy and maternity?               |          |  |          |   |
| <b>Race or Ethnicity</b>  | <b>X</b> |  |          |   |
| Including Gypsy or Roma people, Irish people, those of mixed heritage, asylum seekers and refugees<br>What training does staff have to respond to the cultural needs of different ethnic groups?<br>What arrangements are in place to communicate with people who do not have English as a first language?              |          |  |          |   |
| <b>Religion or Belief</b>   | <b>X</b> |  |          |   |
| Including humanists and non-believers<br>Is there easy access to a prayer or quiet room to your service delivery area?<br>When organising events – Do you take necessary steps to make sure that spiritual requirements are met?  |          |  |          |   |
| <b>Sexual Orientation</b>   | <b>X</b> |  |          |   |
| Including gay men, lesbians and bisexual people<br>Does your service use visual images that could be people from any background or are the images mainly heterosexual couples?<br>Does staff in your workplace feel comfortable about being 'out' or would office culture make them feel this might not be a good idea? |          |  |          |   |
| <b>Transgender or Gender Reassignment</b>   | <b>X</b> |  |          |   |
| This will include people who are in the process of or in a care pathway changing from one gender to another.<br>Have you considered the possible needs of transgender staff and service users in the development of your proposal or service?   |          |  |          |   |
| <b>Human Rights</b>   |          |  | <b>X</b> | CCTV systems are provided to deter criminal behaviour, prevent crime, and protect staff and service users, helping to provide and support a safe and secure environment. The systems are also used within specific clinical areas to maintain therapeutic observations and the protection of service users from harm and danger. To protect individuals, where staff are found to be abusing their position and misusing CCTV, they will be subject to disciplinary proceedings under the Trust's disciplinary procedure and could face criminal proceedings. |

|   |             |               |            |           |
|---|-------------|---------------|------------|-----------|
| Affecting someone's right to Life, Dignity and Respect?   |             |               |            |           |
| Caring for other people or protecting them from danger?   |             |               |            |           |
| The detention of an individual inadvertently or placing someone in a humiliating situation or position?   |             |               |            |           |
| <b>If a negative or disproportionate impact has been identified in any of the key areas would this difference be illegal / unlawful? I.e., Would it be discriminatory under anti-discrimination legislation. (The Equality Act 2010, Human Rights Act 1998)</b>   |             |               |            |           |
|   | Yes         | No            |            |           |
| <b>What do you consider the level of negative impact to be?</b>   | High Impact | Medium Impact | Low Impact | No Impact |
|   |             |               |            | X         |
| <p>If the impact could be discriminatory in law, please contact the <b>Equality and Diversity Lead</b> immediately to determine the next course of action. If the negative impact is high a Full Equality Analysis will be required.</p> <p>If you are unsure how to answer the above questions, or if you have assessed the impact as medium, please seek further guidance from the <b>Equality and Diversity Lead</b> before proceeding.</p> <p>If the proposal does not have a negative impact or the impact is considered low, reasonable, or justifiable, then please complete the rest of the form below with any required redial actions, and forward to the <b>Equality and Diversity Lead</b>.</p> |             |               |            |           |
| <b>Action Planning:</b>   |             |               |            |           |
| How could you minimise or remove any negative impact identified even if this is of low significance?  |             |               |            |           |
| N/A   |             |               |            |           |
| How will any impact or planned actions be monitored and reviewed?   |             |               |            |           |
| N/A   |             |               |            |           |
| How will you promote equal opportunity and advance equality by sharing good practice to have a positive impact other people as a result of their personal protected characteristic.   |             |               |            |           |
| N/A   |             |               |            |           |
| Please save and keep one copy and then send a copy with a copy of the proposal to the Senior Equality and Diversity Lead at bsmhft.edi.queries@nhs.net. The results will then be published on the Trust's website. Please ensure that any resulting actions are incorporated into Divisional or Service planning and monitored on a regular basis   |             |               |            |           |

**Local Operating Procedure for Body Worn CCTV****1 Introduction**

- 1.1 BWCCTV equipment is an overt method of obtaining and securing evidence at the scenes of incidents and crimes. The following policy and procedure is intended to enable security officers to comply with legislation and guidance to create evidence for use in court proceedings, whilst protecting the Human Rights of individuals. Due regard has been given to the requirements of the BSMHFT and partner agencies to ensure that the equipment is practical and capable of producing evidence that can be used in a court.

**2 System Configuration**

- 2.1 The system will consist of a camera and microphone; it will be capable of being operated by one person and worn in such a way as to allow the user to retain full mobility to keep both hands free. It is intended as an overt recording system and therefore will not be concealed.
- 2.2 Image Quality: recording will be set to maximum frames a second, to ensure the best useable images are obtained.

**3 Physical/Environmental**

- 3.1 The camera and microphone unit will be attached to the chest area of a security officer's body vest to capture the same view as seen by the officer. The recording unit will either be attached to the security officer's belt or stored in a pocket/pouch on the officer's belt secured in turn by Velcro strip. The cable connections from the camera and microphone to the recording device will have a breakpoint as a safety feature to reduce the risk of injury to the officer.

**4 Training & Regulation**

- 4.1 In order to use the Body Worn Device, users should receive training in all necessary technical aspects of the specific equipment being used and its use. This will be the responsibility of the Trust contract provider, for the training of all new staff and ensuring existing staff are regularly updated on the operation and use of the equipment. CCTV licensing for operators of the equipment as per Security Industry Authority (SIA) regulations and the Private Security Industry Act (PSIA) is not legally required for public sector providers such as healthcare, but it is a requirement of the Trust that all contracted security staff hold a SIA CCTV licence, as this provides assurance and shows an understanding of the legislation.

**5 Recording**

- 5.1 Recording will be activated only when the conditions in Para 10 have been satisfied and turned off as soon as the incident has finished.

**6 Storage**

- 6.1 The recording device will be configured so as not to allow or permit editing or deletion of recordings by the operator. All data will be deleted automatically by set pre-set program after a 30-day period, in accordance with Trust CCTV Policy.

## **7 Access to BWC Recorded Media**

- 7.1 The process for obtaining access to and copies of recorded media from a BWC is as documented within the Trust CCTV Policy for the access to and obtaining CCTV footage.

## **9 Daily Check/Issue**

- 9.1 Security officers must have undertaken training in the use of the Body Worn CCTV Camera before using the system and officers will be required to have read and signed all relevant instructions for use of BWC.
- 9.2 Before using BWC equipment the following checks are to be undertaken and documented as completed:
- The unit is correctly assembled.
  - Recording picture / screen is correct way up.
  - Sound recording level is appropriate.
  - Date and Time is set correctly.
  - Battery is fully charged.

## **10 When to Activate**

- 10.1 The presence of a BWC alone is expected to have a significant preventative value. It is envisaged that when potential offenders or those whose behaviour is escalating are informed that their behaviour (actions and words) may be recorded many adverse situations will be avoided.
- 10.2 However, when a security officer is informed or believes an incident of the following type is about to commence or has commenced, recording should start regardless:
- Acts or threats of violence or aggression.
  - Acts of verbal or racial abuse.
  - Where the security officer believes there is a threat to him/herself, NHS staff, patients or visitors or contractors.
  - Criminal acts including acts of actual or attempted vandalism, criminal damage and/or anti-social behaviour.
- 10.3 Behaviour resulting from misuse of or overdose from alcohol or drugs is not deemed to be an excuse for bad or criminal behaviour. The security officer wearing the BWC must always where possible protect the dignity and confidentiality of any person or persons being recorded or in the immediate vicinity unless to do so would mean the images being recorded would not capture the criminal act or incident which was occurring.



## **11 Providing a Warning of Camera Activation**

- 11.1 It is crucial for the Security Officer to inform the individual(s) of concern that images, and audio footage are being recorded. Security officers must do this at the earliest practical and safest opportunity, irrespective of whether they have just arrived at the scene of an on-going incident and the equipment was turned on 'on-route' as a matter of expediency or in response to a 'no-notice' event or incident that unfolds in front of them. To this end the following words are to be said clearly and directed to the individual(s) of concern:

**'I must now inform you that your behaviour has now become/is unacceptable and your word and actions are now being recorded and the recorded footage so obtained may be used in evidence and may be passed to the police '**

- 11.2 Where possible all attending officers should record events or incidents, where it is the case two officers are attending it may be best practice for one officer to take a step back to ensure the whole incident and the surrounding area is being recorded albeit without causing unnecessary compromise or breach of confidentiality or dignity for other not involved patients/public.

## **12 Post Incident Management/Evidence Continuity**

- 12.1 Where incidents do occur that require recording, police assistance should be sought, and they should be asked to attend at the earliest opportunity to assist in the normal manner. Irrespective of when they attend i.e., during or after an incident, they should be briefed on what has taken place and shown recorded footage using the play back facility.
- 12.2 At that point and subject to a belief by police that an offence has taken place and action should/can be taken, the police should be advised to submit a request for the recorded footage to Trust Information Governance, in accordance with the guidance set out in this policy. The Security Officer should then ensure that the footage captured on the BWC is retained and downloaded for evidential purposes as detailed within this policy.
- 12.3 All requests for CCTV footage and subsequent decisions to provide disclosure are made at BSMHFT by the Head of Information Governance.

## **13 When Not to Activate**

- 13.1 A BWC should not be used in the following circumstances.
- To provide recorded images for any media forum.
  - Outside the line of duty.
  - To deliberately embarrass or take away the dignity of another.
  - At a location anywhere other than Trust premises.
  - If a warning of the recording has not been given.
  - Where aggression or bad behaviour is deemed to be because of a service users mental health.
  - Inpatient Wards
  - Where the service user is in a state of undress.

### Closed Circuit Television (CCTV) systems

#### Information leaflet

The processing of closed-circuit television (CCTV) images is governed by the Data Protection Acts 2018. The Data Protection Commissioner has issued a code of practice under this act relating to the use of CCTV systems. All CCTV operators employed by Birmingham and Solihull Mental Health NHS Foundation Trust must comply with the Act and Code of Practice.

Birmingham and Solihull Mental Health NHS Foundation Trust has installed CCTV systems within its premises throughout the estate for the prevention and detection of crime and the safety and security of staff, service users and authorised visitors to these premises.

These systems are registered with the Data Protection Office to be used for the following purpose of crime prevention and detection, apprehension, and prosecution of offenders, and may be utilised for the purposes of internal Trust investigations.

CCTV systems will not be used for any purpose other than that registered with the Data Protection Office. Images will not be retained for longer than necessary and will be removed or erased after this period has expired.

Images will not be disclosed to third parties unless the provisions of the Data Protection Act 2018 are met. Such circumstances may include:

- the investigation of crime
- the apprehension or prosecution of offenders
- a requirement for disclosure by or under any enactment
- a requirement for disclosure by rule of law or by order of the court
- a requirement for disclosure in connection with legal proceedings (including prospective legal proceedings)
- disclosure is otherwise necessary for the purposes of establishing, exercising, or defending legal rights.

If you have any questions or wish to make a complaint about the operation of Birmingham and Solihull Mental Health NHS Foundation Trust's CCTV systems, please contact:

*Information Governance Team*

*Unit 1*

*B1*

*50 Summer Hill Road*

*Birmingham.B1 3RB*

*0121 301 1111*



## DEFINITIONS

### **DATA CONTROLLER**

Data controller means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

### **APPLICATION TO BSMHFT**

Within BSMHFT the following applies:

The Trust is the Data Controller. Compliance with the provisions of the 2018 Act is, however, for all practical purposes, exercised by all managers and staff at all levels of the Trust.

Service Directors are responsible for ensuring compliance with the policy and are to disseminate it within their areas of responsibility, with any amplifying instructions/guidance relevant to their directorates.

Service Directors may devolve the day-to-day running of the scheme to a designated person, normally the manager of the facility or location, on larger or shared sites agreement will be reached as to who manages the system on a day-to-day basis.

If the Trust and any other body enter a partnership to install CCTV in and around a Trust site with a view to:

Preventing and detecting crime  
Apprehending and prosecuting offenders  
Protecting public safety.

Both the Trust and the other body will be data controllers for the purposes of the partnership scheme and will set out the purposes of the scheme and the policies on the use of the images.

If in the future the Trust employs a security company to run a CCTV system, then the company manager may be deemed a data processor. This is “any person (other than an employee of the data controller) who processes the personal data on behalf of the data controller”. The Trust will need to consider their compliance with the Seventh Data Protection Principle in terms of this relationship.

### **PERSONAL DATA**

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

### **SPECIAL CATEGORY PERSONAL DATA**

GDPR also refers to 'special categories of data'. Special consideration and justification needs to be given for the collection and disclosure of such data. Sensitive personal data according to the Data Protection Act is:

- ☐ Physical or Mental Health or condition
- ☐ Racial or ethnic origin
- ☐ Political opinions
- ☐ Religious beliefs or other beliefs of a similar nature
- ☐ Trade Union membership
- ☐ Sexual life
- ☐ The commission or alleged commission of any offence
- ☐ Genetic Data
- ☐ Biometric Data where processed to uniquely identify a person
- ☐ Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence any court in such

### **PROCESSING**

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

### **PURPOSE FOR WHICH PERSONAL DATA/IMAGES ARE PROCESSED**

Before considering compliance with the Data Protection Principles, a user of CCTV or similar surveillance equipment, will need to determine two issues:

What type(s) of personal data are being processed. Is there any sensitive personal data as defined by DPA 2018?

For what purpose(s) are both personal data and sensitive personal data being processed?

Users of surveillance equipment should be clear about the purposes for which they intend to use the information/images captured by their equipment. The equipment may be used for several purposes:

Prevention, investigation and/or detection of crime.

Apprehension and/or prosecution of offenders (including images being entered as evidence in criminal proceedings).

Public and employee safety.

Using information captured by a surveillance system will not always require the processing of personal data or the processing of sensitive personal data. For example, use of the system to monitor traffic movements, will not necessarily require the processing of personal data. It is envisaged that most CCTV systems in use within the Trust WILL result in the processing of personal data or sensitive personal data.

### Assessment Framework for Mental Health Act Commissioners and Others

|     | Question   | Regulatory Source or good practice guide.                                 |
|-----|--|---|
| 1.  | What is the object of installing CCTV?   | Code of practice on CCTV – Page 21  |
| 2.  | Was this a necessary and proportionate response to the identified need?  | Human Rights Act: Article 8 European Court of Human Rights.               |
| 3.  | Is the Code of Practice on CCTV issued by the Information Commissioner's Office being adhered to? (You might want to consider both whether this was used as a guide to the original installation and whether it is still being applied rigorously.)  | CCTV Code of Practice.  |
| 4.  | Is usage in line with PVH regulations?<br><b>N/A</b>   | Private & Voluntary Health Care Regulations 2001 – especially para. 16(4) |
| 5.  | Is there any evidence that CCTV is being used as a way of compensating for the lack of adequate staffing levels?   | Poor or inadequate quality of practise.                                   |
| 6.  | What is the process of decision-making which led to the installation of CCTV? What kind of service user consultation took place?   | Human Rights Act (ECHR Article 8)<br>Good Practice.                       |
| 7.  | Have the objectives of the installation been met? (Has any review or evaluation been undertaken to provide evidence to show this?)   | Code of Practice on CCTV – Page 21; and good practise.                    |
| 8.  | Who within the organisation has overall responsibility for information governance including the use of CCTV? Who has day-to-day responsibility for the use of CCTV (for example at Ward level)? Is this issue regularly considered at Board level?   | Code of Practice on CCTV – Page 19  |
| 9.  | What arrangements are in place to ensure that staff understand / receive training in the purpose and use of CCTV? Which staff are these (at what level)?   | Code of Practice on CCTV – Page 12  |
| 10. | Is there a formal system in place for raising concerns or making a complaint about the use of CCTV and is this advertised clearly?   | Code of Practice on CCTV – Page 18  |
| 11. | Is there a process in place to ensure that the continuing use of CCTV is reviewed and that patients are consulted on this?   | Good Practice.  |
| 12. | What arrangements are in place to ensure that patients understand the purpose of CCTV and have access to the policies governing installation and use? (For example, is there a readily accessible patient leaflet? Is there a multi-faceted and proactive approach to informing patients, having regard to their | Good Practice<br>Possibly, Section 132 of the MHA for detained patients.  |

|     |  |  |
|-----|--|--|
|     | mental state, on admission and at other times?   |  |
| 13. | What arrangements are in place to ensure that patients have access to any stored media which include images of themselves?   | Code of Practice on CCTV – Page 28   |
| 14. | What arrangements are in place to ensure that the images are kept securely and only viewed by those authorised to have access? (This includes accidental viewing of live images.)  | Code of Practice on CCTV - Page 11   |
| 15. | In the event of a request for access to the images by outside agencies, such as the police, what process is in place to assess and authorise the request? Who is the named person responsible for this?  | Code of Practice on CCTV – Page 12   |
| 16. | If a patient requests access to images of himself/herself, what arrangements are in place to ensure that 3 <sup>rd</sup> party confidentiality is not breached?  | Code of Practice on CCTV – Page 12   |
| 17. | What arrangements are in place for the disposal of recorded material after expiry of the permitted period of retention?  | Code of Practice on CCTV - Page 26   |
| 18. | What processes are in place to assess the need for and decide on implementation of changes in camera coverage?   | Good Practice.   |
| 19. | For uses which require explicit informed consent (for example, for filming as part of treatment or in normally private areas, such as bedrooms), what is the process for providing information to the individual about the process and for obtaining his or her consent? | Human Rights Act- Article 8, <i>GMC guidance on the making &amp; use of audio &amp; visual recordings of Patients, Part 3.</i> |
| 20. | Does the Policy allow for the use of covert CCTV? If so, is it in line with legislative requirements?  | Regulation of Investigatory Powers Act 2000  |