NHS
Bridgewater
Community Healthcare
NHS Foundation Trust

Closed Circuit Television (CCTV) Policy and Access Guidance

Policy Number	**IG/Pol/016**
Target Audience	**All staff including bank, agency and learners in practice**
Lead Executive Director	**Director of Finance**
Recommending Committee/Group	**Digital Information Governance and Information Technology Group**
Approving Committee(s)	**Corporate Clinical Policy Group**
Ratifying Committee	**Corporate Clinical Policy Group**
Date First Ratified	**February 2022**
Last Full Review Date	**March 2024**
Next Full Review Date	**March 2027**
Extension agreed to	**n/a**
Lead Author(s)	**Senior Information Governance Officer**
Version Number	**2.0**

Applicable Statutory, Legal or National Best Practice Requirements	Biometrics and Surveillance Camera Commissioner (2021) Update to Surveillance Camera Code of Practice Care Act 2014 c. 23 Care Quality Commission (CQC) (2021) The Care Act 2014 and the 'easements' to it Data Protection Act 2018, c.12 Department of Health and Social Care Code of practice: Mental Health Act 1983 Department of Health and Social Care (2016) Records management: code of practice for health and social care Equality and Human Rights Commission (2021). Article 8 Freedom of Information Act 2000 Health and Safety at Work etc Act 1974, c37 Mental Health Act 1983 c. 20 Modern Slavery Act 2015, c30 [online]. NHS Counter Fraud Authority (2021) NHS England Transformation Directorate (2023) Updates to the Records Management Code of Practice NHSx (2021) Records Management Code of Practice

Document retention – lifetime of the Trust or 20 year review
Document owner – Senior IG Officer

	Protection of Freedom Act 2012, c9 Regulation of Investigatory Powers (2000), c23 Surveillance Camera Commissioner (2014) Surveillance camera code of practice Human Rights Act (1998) c. 42 UK General Data Protection Regulation (UKGDPR) (2018) Freedom of Information Act 2000

The Trust is committed to an environment that promotes equality, embraces diversity, and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the Trust's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Version Control Sheet

Version	Date	Reviewed By	Comment
1.0	July 2021 Nov 2021 Dec 2021 3rd February 2022	Jackie McKay DIGIT Corporate Clinical Policy Group Trust Board (e-governance)	New document Signed-off Approved, submitted for ratification by the Trust Board Ratified – Policy Officer notified 28/02/2022
1.1	September 2022	J. McKay	Amendments made to sections 2, 3, 6, 9 and 15.1
1.2	October 2022	S. Mackie	Approved by chair action
1.3	Dec 2023	Jackie Mckay	Full review
1.4	December 23	M. Corkery	Reviewed, comments made
1.5	Feb 2024	DIGIT	Policy review approved
1.6	March 2024	Corporate Clinical Policy Group	Approved subject to minor amendments and final chair approval
1.7	March 2024	J. McKay	Amendments completed
2.0	March 2024	J. Cheung	Approved by chair action

Equality impact assessment

Consider if this document impacts/potentially impacts:

- Staff
- Patients
- Family members
- Carers
- Communities

Yes [ ] **complete box A**	**No** [x] **complete box B**
Box A Contact the Trust's equality & inclusion manager at: **Email: ruth.besford@nhs.net** **Date contacted:**	**Box B** Complete details below: **Name: Jackie McKay** **Email: jacquelinemckay@nhs.net** **Date: 10/1/24**

Education & professional development (EPD) question

To ensure that any training requirements are discussed, and resources planned and allocated to meet the needs of the service, you must consider whether this document has additional training requirements. Please answer the following question by entering a cross in the Yes or No box below:

	Yes	**No**
Does this document have any additional training requirements or implications?		x

If you have answered **YES** you must forward a copy of this document to EPD **before** submitting to the policy officer.

Date submitted to EPD: ……

No further action is required if you have answered NO.

This table below must be completed in full for audit and governance purposes. Please note documents will be returned if section 1 in the table below is not completed fully. This will result in a delay in listing the document for approval.

Name of document	Closed Circuit Television (CCTV) Policy and Access Guidance
Document number	IG/Pol/016
Document author	Jackie McKay

Section 1 - actions required by author	**Authors response**
Date proposal form submitted to policy officer (new documents)	N/A
Date proposal form presented to CCPG (new documents)	N/A
Date proposal approved by CCPG (new documents)	N/A
Date literature search/reference review requested	16.1.24
Date EqIA considered	9/1/24
Date additional training requirements considered	N/A
Date fraud-proofed by the Anti-Fraud Specialist (AFS) if applicable	10/1/24
Date template accessed on the Hub Add 'OFFICIALSENSITIVE: COMMERCIAL' to front cover if the document can be shared on the internet Add 'OFFICIALSENSITIVE: PERSONAL' to appendices if they include or will include personally identifiable information (PID)	December 23
Date literature review completed (check references are formatted correctly, and hyperlinks working)	March 2024
Date first draft submitted to policy officer for initial review	13/12/23
Date returned by policy officer following initial review	21/12/23
Date submitted to key individuals/groups/subject matter experts for comments (add names and designations of responders to consultation table)	10/1/24
For clinical documents, date document submitted to consultation group for sign-off i.e., IPC, Medicines Management (this applies if the document contains medication or medical gases - update version control sheet to confirm sign-off)	N/A
Name of Recommending Committee/group	DIGIT
Date sent to Recommending Committee/group for sign-off	7th Feb 2024
Date signed-off by the Recommending Committee/group (update version control sheet once signed-off)	14th Feb 2024
Date submitted to policy officer for listing at CCPG	20th Feb 2024
Section 2 – for completion by the policy officer	
Date approved by CCPG	15th March
The following policies require Board approval and must be submitted to Board following CCPG approval: • Risk Management Framework Policy • Health & Safety Policy • Policy and procedure for the production, approval and ratification of Trust-wide policies and procedures ("Policy for Policies") Date submitted for Board approval: Date approved by Board:	N/A

Contents

The appendix 1 to 3 can be accessed under the policy on MyBridgewater. Appendix 4 can be accessed electronically by clicking on the link below:

Appendix 1 Patient information leaflet Closed Circuit Television (CCTV)

Appendix 2 Patient information leaflet about Closed Circuit Television (CCTV) (easy read)

Appendix 3 CCTV police request form

Appendix 4 Data Protection Impact Assessment guidance

1 Introduction

Closed circuit television (CCTV) surveillance has become a common feature of our daily lives. Whilst the use of CCTV continues to enjoy general public support, it necessarily involves intrusion into the lives of ordinary individuals in the course of their day-to-day business. The public expect CCTV to be used responsibly with effective safeguards in place.

CCTV can be used to enhance security and can be used to investigate an incident. It can be used to reduce crime and anti-social behaviour and support the safety of Bridgewater Community NHS Foundation Trust (hereafter the Trust) staff and people who use Trust services.

CCTV systems consist of devices which view and record images of individuals. They also cover other information derived from those images that relate to individuals (for example vehicle registration). Therefore, the use of CCTV systems is covered by the Data Protection Act (DPA) 2018, with guidance provided by codes of practice issued by the Information Commissioner's Office (ICO). Data protection legislation not only creates obligations for organisations, it also gives individuals rights, such as the right to gain access to their details, and to claim compensation when they suffer damage as a result of misuse of data.

CCTV can be used for:

- Reducing fear of crime and reassure people who use services and staff
- Assisting in managing sites
- Aiding detection, deterrence, and prevention of crime and in this regard to provide evidence to the police and other bodies with prosecuting powers
- Improving the speed with which the Trust can alert the police to unlawful activity or other emergency services to matters of health and safety
- Providing police with recordings or image of person who has gone absent without leave and where they have concerns for their safety
- Preventing access by unauthorised individuals or third parties
- Preventing and detecting crime
- Public and employee safety
- Employee disciplinary investigations
- Apprehension and prosecution of offenders.

The Trust currently controls and manages five freehold and three specific leasehold sites that have CCTV systems installed, and it is clear that these systems can assist in the prevention, detection and deterrence of crime, the apprehension and prosecution of offenders.

The CCTV systems also provide assurance to staff working on the sites, particularly those who work alone or are required to work during the hours of darkness. It is essential that the Trust uses CCTV in a manner that complies with the law and continues to enjoy the support of staff, patients, and the public.

This policy sets out the appropriate actions and is supported by a procedure which includes accessing and viewing footage and must be followed to comply with the relevant data protection legislation in respect of the use of CCTV surveillance systems managed by the Trust.

1.1 Objective

This policy has been developed to provide a safer and more secure environment for people using Trust services, including visitors, staff, learners in practice, and the public; it is supported by a patient leaflet - see appendix 1 and 2.

The policy aims to offer clarity on when and where CCTV should be used and how to do so within current guidance and legislative frameworks.

This policy intends to:

- Inform all who come onto the Trust site that CCTV is in use
- Keep CCTV data secure and controlled by authorised personnel
- Maintain all CCTV equipment in working order

  Provide retention of CCTV data within the stated purpose only
- State the manner and means of destroying stored CCTV data.

By the means of this policy, associated procedures and arrangements, the Trust aims to:

- Ensure no footage or images of staff, patients or visitors will be released or viewed by unauthorised person
- The system is regularly checked to certify that, if required, it is of an evidential quality to allow the Trust to pursue a prosecution
- Ensure the use of CCTV within the Trust is in accordance with local and national guidance and legislation
- Ensure systems are in place for monitoring, maintenance, and audit of such systems
- Ensure CCTV is correctly and appropriately installed and operated and not abused or misused.

1.2 Scope

This policy applies to all Trust staff including bank, agency, learners in practice and volunteers.

2 Definitions

The definitions applicable to this policy are as follows:

CCTV	CCTV is the use of video cameras to transmit a signal to a specific, limited set of monitors. It differs from broadcast television in that the signal is not openly transmitted.
Surveillance Camera Commissioner (SCC)	The role of the SCC is to encourage compliance with the surveillance camera code of practice (Surveillance Camera Commissioner, 2014).
Data protection Impact Assessment	A data protection impact assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project.
Protection of Freedom Act (POFA) 2012	POFA 2012 is a parliament Act of the United Kingdom (UK). As the protection of freedoms bill, it was introduced in February 2011
UK General Data Protection Regulation (GDPR)	The UK continues to use GDPR Legislation 2018. However, it is now referred to as UK GDPR. The legislation a sets out the rights of individuals in relation to their data.
Data Protection Act 2018	The DPA 2018 sets out the framework for data protection law in the UK. It updates and replaces the DPA 1998 and came into effect on 25 May 2018. It was amended on 01 January 2021 by regulations under the European Union (EU) (withdrawal) Act 2018, to reflect the UK's status outside the EU.
Local security management specialist (LSMS)	LSMS means the person appointed by the Trust pursuant to carry out the responsibilities and functions set out in the NHS Standard Contract: https://www.england.nhs.uk/nhs-standard-contract/
Regulation of Investigatory Powers Act (RIPA) 2000	The RIPA 2000 is an act of parliament, regulating the powers of public bodies to carry out surveillance and investigation, and covering the interception of communications.

3 Abbreviations

The abbreviations applicable to this policy are as follows:

ANPR	Automatic Number Plate Recognition
BWV	Body Worn Video
CCTV	Closed Circuit Television
CD	Compact Disc
DIGIT	Digital Information Governance and Information Technology Group
DPO	Data protection officer
DPA	Data Protection Act
DPIA	Data Protection Impact Assessment
DTAC	Digital Technology Assessment Criteria
DVD	Digital video disc
EU	European Union
ECHR	European Court of Human Rights
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
IG	Information Governance
IT	Information Technology
LNCSOP	Local Non-Clinical Standard Operating Procedure
LSMS	Local Security Management Specialist
POFA	Protection of Freedoms Act
RIPA	Regulation of Investigatory Powers Act
SIRO	Senior information risk owner
SCC	Surveillance Camera Commissioner
SRA	Security Risk Assessment
UK GDPR	United Kingdom General Data Protection Act
USB	Universal Serial Bus

4 Other relevant procedural documents

This policy should be read in conjunction with the following documents:

Anti Fraud, Bribery and Corruption Policy

Clinical Photography, Audio/Video Recording and Remote Video Consultation within Healthcare Policy

Corporate Records (including Document Management) Policy

Data Protection and Confidentiality Policy

Dignity and Respect at Work Policy and Procedure

Disciplinary Policy and Procedure

Fire Safety Policy

Freedom of Information and Environment Information Regulations Policy

Handling of Complaints, Compliments, Comments and Concerns Policy and Procedure

Health and Safety Policy

Information Asset and Systems Audit Policy

Information Governance Framework Policy

Policy and Procedure for the Development and Review of Policy and Procedural Documents

Procurement Policy

Risk Assessment and Risk Register Process Guideline

Risk Management Framework

Security Policy

Subject Access/Access to Records Policy

Third Party Supplier Policy

Violence and Aggression Policy

5 Roles and responsibilities

5.1 Chief executive

The chief executive, as accountable officer has ultimate accountability for:

- Ensuring the provision of high quality, safe and effective services within the Trust
- Ensuring resources are available to ensure effective implementation.

5.2 Chief nurse/caldicott guardian

The chief nurse is the Trust caldicott guardian and is responsible for:

- The confidentiality of person identifiable information as designated in the caldicott report and for the information governance (IG) agenda which incorporates DPA 2018 legislation
- Ensuring patient identifiable information is shared in an appropriate and secure manner according to the eight caldicott principles – see section 8.2.

5.3 Senior information risk owner

The senior information risk owner (SIRO) is currently the director of finance and is responsible for:

- Information risk throughout the organisation
- The overall ownership of the organisation's Information Risks and risk management strategy and processes within the Trust
- Advising the Board on the effectiveness of information risk management across the Trust
- Providing an essential role in ensuring that identified information security risks are followed up and incidents managed.

5.4 Data protection officer

The data protection officer (DPO) is the Trust secretary. The DPO must have expert knowledge of data protection law and practices and the ability to acquire detailed understanding of the Trusts business, the purposes for which it processes, or intends to process personal data.

The DPO has responsibility to ensure the Trust is correctly protecting individuals' personal data to ensure compliance with this policy, the Information Commissioner's Office (ICOs) code of practice on CCTV (2023) and the DPA 2018, and the UK General Data Protection Regulation (GDPR) 2018.

5.5 Associate borough directors, heads of Corporate Services, operational managers and service managers

All Associate borough directors, heads of Corporate Services, operational managers and service managers are responsible for:

- Ensuring this policy is implemented across their area of their managerial responsibility.
- Ensuring their staff are aware of and comply with this policy
- Implementing this policy across their area of managerial responsibility
- Ensuring all clinical staff including bank, agency and learners in practice understand why CCTV is used across the Trust, its impact, and individual rights.

5.6 Local security management specialist

The LSMS is responsible for:

- Advising on systems and procedures that need to be in place to ensure compliance with this policy.

- The control and processing of the images obtained from the Trust's CCTV cameras
- Deciding how images can be used in accordance with DPA and GDPR guidance
- The day-to-day management of CCTV at Trust sites
- In consultation with the head of estates and the IG team, ensuring CCTV is to be used in accordance with the Trust's registration with the ICO, complies with the DPA 2018, UK GDPR (2018) and ICOs code of practice on CCTV (2023)
- Ensure the CCTV is in working order.

5.7 Head of estates

The head of estates is responsible for:

- Ensuring all CCTV equipment in working order
- Along with the CCTV provider, ensuring appropriate signage is displayed in Trust sites where CCTV is in operation
- Ensuring any third party CCTV suppliers have undergone the appropriate IG and procurement due diligence checks
- Ensuring the CCTV system and installation is compliant with DPA 2018 and GDPR (2018)
- Ensuring a security risk assessment for intrusion is undertaken
- Consider the 12 guiding principles of the updated Surveillance Camera Code of Practice (Biometrics and Surveillance Camera Commission, 2021) before installing CCTV – see section 8.3
- Ensuring there is a contract in place and that it includes appropriate confidentiality clauses and is up to date
- Ensuring the CCTV is fit for purpose
- Ensuring the safe storage and security of the equipment and media
- Ensuring RIPA applies if CCTV captures private property
- Assisting the LSMS with DPIAs and DPA risk assessments to ensure compliance with DPA 2018 and UK GDPR (2018)
- Providing retention of CCTV data within the stated purpose only
- Stating the manner and means of destroying stored CCTV data

- Preventing access by unauthorised individuals or third parties
- Ensuring any risks are identified and appropriately escalated
- Reporting incidents on the Trust online risk management reporting system (Ulysses)
- Reporting breaches of identifiable personal information
- Advising how individuals can ask for a copy of footage which they are identified
- Advising how third parties such as the police can access the footage in the event of an investigation or prevention of a serious crime.

5.8 Information Governance team

The IG team is responsible for:

- Providing advice and guidance on all aspects of privacy and confidentiality in relation to CCTV
- Ensuring CCTV and individual rights is included in the staff, adult and children's privacy notices
- Ensuring a security risk assessment for intrusion us undertaken
- Consider the 12 guiding principles of the surveillance camera code of practice (updated updated Surveillance Camera Code of Practice (Biometrics and Surveillance Camera Commission, 2021) before installing CCTV – see section 8.3
- Assisting the LSMS with DPIAs and DPA risk assessments to ensure compliance with DPA 2018 and UK GDPR (2018)
- Advising on the ICOs code of practice on CCTV (2023) and the DPA 2018, and the GDPR (2018).

5.9 Assistant director of communications

The assistant director of communications is responsible for:

- Producing notification in way of posters for those areas that have CCTV – see section 8.1
- Assisting the LSMS in producing other public facing information.

5.10 Procurement team

The Procurement team is responsible for:

- Liaising with the IG team when approached to procure any items, systems and third-party supplier where identifiable personal data is being processed for example CCTV

- Ensuring any CCTV contracts entered have been through the appropriate ICO due diligence.

5.11 All staff including bank, agency, learners in practice and volunteers

All staff including bank, agency, learners in practice and volunteers are responsible for:

- Adhering to this policy and any related procedures

- Familiarising themselves with the violence and aggression policy and procedure

- Knowing how to report an incident using the online risk management reporting system (Ulysses)

- Escalating any potential risks to the IG team and LSMS

- Report any issues with CCTV for example, faults, vandalism to the LSMS or the head of estates.

6 Equipment

Monitors

Portable storage - example, universal serial bus (USB)

Appropriate information technology (IT) equipment

CCTV

Patient leaflet (appendix 1 and 2)

CCTV police request form (appendix 3)

DPIA template (appendix 4)

7 CCTV considerations

CCTV is a control measure and will assist in deterring intruders, violence and aggression and acts of vandalism. CCTV can be used from a health and safety perspective, such as:

- Monitoring an area which is not usually managed

- Where a person may be in need of assistance for an unacceptable period of time without the ability to summon help.

Effective use of CCTV must encompass the following considerations:

- Impact assessment
- Siting of equipment
- Functionality of the equipment and image quality
- Installation, maintenance and decommissioning of equipment
- Management of data collected including IG considerations
- Skill and training of people who use CCTV
- Compliance with best practice, guidance and legal frameworks
- Cost benefit analysis of installing CCTV.

With these considerations in mind, any decision making should be supported by a framework that has been designed to help understand where and how to install CCTV.

8 Information governance considerations

8.1 CCTV, GDPR and Data Protection Act 2018

When considering making an application for a new or upgrade of a CCTV system, the data rights and freedoms of individuals should be respected. These data rights are set out in GDPR Article 5 'Principles relating to processing of personal data'.

Under the GDPR, it is not enough to say that we are collecting personal data; we also need to explain why we are using it and what we will do with it. A poster should form part of the public notification and should have on it for example: "CCTV is in operation for the purpose of public safety".

Under GDPR Article 6 (1) processing shall be lawful only if and to the extent that at least one of the following applies:

a) The data subject has given consent to the processing of his or her personal data for one or more specific purposes

b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

c) Processing is necessary for compliance with a legal obligation to which the controller is subject

d) Processing is necessary in order to protect the vital interests of the data subject or of another natural person

e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

To be able to use CCTV on Trust premises, we rely on Article 6 (1) (f) of GDPR. We use this legal basis but must understand that we should respect the interests and fundamental rights and freedom of individuals who visit or work in locations where this is CCTV including our staff.

8.2 Caldicott principles

The eight Caldicott Principles must be adhered to when sharing patient identifiable information to ensure it is shared in an appropriate and secure manner.

Principle 1: Justify the purpose(s) for using confidential information.
Principle 2: Use confidential information only when it is necessary.
Principle 3: Use the minimum necessary confidential information.
Principle 4: Access to confidential information should be on a strict need-to-know basis.
Principle 5: Everyone with access to confidential information should be aware of their responsibilities.
Principle 6: Comply with the law.
Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality.
Principle 8: Inform patients and service users about how their confidential information is used.

8.3 Surveillance camera code of practice

The 12 guiding principles of the surveillance camera code of practice (Surveillance Camera Commissioner, 2014) must be considered by the head of estates, LSMS and the IG team before installing CCTV:

1	What is the system used for?
	Does the Trust review its use?
2	Has the Trust carried out a privacy impact assessment?
	Does the Trust publish the privacy impact assessment?
3	Does the Trust have signage in place to say surveillance is taking place?
	Is there a published point of contact for people to raise queries or complaints with?
4	Who is responsible for the Trusts system?
	Are Trust staff aware of their responsibilities?

5	Does the Trust have clear policies and procedures in place?
	Do Trust staff know what the policies and procedures are?
6	How long does the Trust keep images/information?
	How does the Trust make sure images/information is deleted once they are no longer needed?
7	Does the Trust have a policy on who has access to the stored information?
	Does the Trust have a policy on disclosure of information?
8	Does the Trust follow any recognised operational or technical standards?
9	Does the Trust make sure that the images captured by the system are kept securely?
	Are only authorised people given access to the images?
10	Does the Trust evaluate the system regularly to make sure it's still required?
	Could there be an alternative solution to a surveillance camera system?
11	Can the criminal justice system use the images and information produced by your surveillance camera system?
	Does the Trust have a policy on data storage, security and deletion?
12	Does the Trust use any specialist technology such as automatic number plate recognition (ANPR), facial recognition, body worn video (BWV) or remotely operated vehicles (drones)?
	Does the Trust have a policy in place to ensure that the information contained on any database is accurate and up to date?

9 Data protection impact assessment

The SCC, in conjunction with the ICO, have developed a DPIA template – see appendix 3. A DPIA must be undertaken before an application is made to install CCTV at any Trust site. The DPIA must be completed by the head of estates and the LSMS with support from the IG team.

The DPIA should include/consider:

- Contract and third-party details
- Digital Technology Assessment Criteria (DTAC)
- The name of the person responsible for the CCTV within the Trust
- The purpose and benefits to be gained from using CCTV
- If less privacy-intrusive solutions such as improved lighting could achieve these benefits

- Security Risk Assessment (SRA)
- Are images required to identify the identifiable individuals, or could the scheme use other images not capable of identifying the individual?
- The views of people in areas where CCTV is installed
- Could intrusion be minimised for those that may be monitored, particularly if specific concerns have been expressed?
- Is the proposed system established on a proper legal basis and operated in accordance with the law?
- How are staff, service users and the public made aware of their data rights under GDPR
- How will the footage be stored?
- Most CCTV footage is deleted 30 days after it's recorded, once this period expires the image is re-recorded over - this should be added to a local non-clinical standard operating procedure
- Who will have access?
- If images are being store on a portable device, such as a compact disc (CD), USB, it should be named with the date, time, camera location and recording equipment used
- Will footage be audited for data quality? Images should be as clear as possible otherwise they are not effective for the purpose.

10 Siting of CCTV equipment

Locations where CCTV cameras are sited must be risk assessed by the head of estates and the LSMS to ensure it is not breaching an individual's fundamental freedoms and rights.

CCTV equipment must be sited in such a way that it monitors those spaces which are intended to be covered. No camera should be hidden from view. Use of covert techniques will only be authorised if considered legal, necessary, and proportionate. There is no reason why this would be used in a healthcare setting.

CCTV cameras must not be pointed at private property including gardens.

10.1 CCTV and Human Rights

The RIPA 2000 provides a framework to ensure techniques are used in a way that is compatible with Article 8 of the Human Rights Act 1998. It allows the right to respect individuals private and family life and ensures that techniques are used in a regulated way and provides safeguards against the abuse of such methods.

The Human Rights Act 1998 is the main law in the UK which protects our human rights. Everyone in the UK has human rights which belong to us. Our rights can never be taken away, but they can sometimes be restricted in very specific circumstances.

There must be a good reason why cameras or other recording equipment are needed; these reasons are written in the Human Rights Act 1998. Often a good reason to install recording equipment might be to protect our rights (for example, our right to life) or the rights of others, to protect national security or for the prevention of crime, or to give patients and staff peace of mind that they are safe.

Before siting CCTV, the LSMS and/or head of estates include the human rights aspect of the risk assessment.

- Is the use to fulfil a legitimate aim?
- Is this a justified response?
- Is it a proportionate response or could something else be done?

10.2 Use of CCTV in clinic areas

The use of CCTV in clinic areas must be given careful consideration in terms of the extent to which it is necessary for safety and security purposes, balanced against the level of interference with the individual's privacy which it would involve.

CCTV must not be installed in areas where clinical assessments take place.

11 CCTV installation and maintenance

Installation of CCTV must be approved by the head of estates where there is likelihood that the use of CCTV will achieve the aims and objectives of the CCTV, in terms of detection, monitoring, investigation and learning from security incidents.

The head of estates, with support from the LSMS, must authorise the installation and agree to the proposed scheme. The Estates team will manage the installation and involve the LSMS in signing off the installation to ensure all requirements have been met.

- Prior to any CCTV installation the head of estates, LSMS and IG team must ensure the CCTV is be used in accordance with the Trust's registration with the ICO and complies with the DPA 2018, UK GDPR (2018) and ICOs code of practice on CCTV (2023).

The process for approving the installation of new CCTV is:

1. Incident occurs/need for CCTV cameras identified

2. Incident/area assessed by the LSMS to see if surveillance is appropriate

3. The LSMS ensures a risk assessment is completed

4. Siting of CCTV camera approved by head of estates and LSMS

5. Consideration of area of use, i.e., public, communal or private

6. Installing CCTV signage, for example, a poster that may say, “CCTV is in operation for the purpose of public safety”

7. Keeping CCTV data secure and controlled by authorised personnel.

Cameras should be located at strategic points on the site, primarily to monitor the perimeter of the site, access and egress points, reception areas, car parks, gardens and other public places, and areas where there have been repeated security or health and safety incidents. Security risk assessment must be undertaken by the LSMS.

Upon installation, all equipment must be tested to ensure only designated areas are monitored and high-quality images are available in live and play back mode.

The CCTV equipment must record the location of the camera, the date and time. The LSMS must ensure these features are audited regularly.

All CCTVs systems must be installed and maintained only by appropriately certificated contractors and the detailed brief provided by the Trust head of estates.

All CCTV equipment must be serviced and maintained on an annual basis. A maintenance log must be kept by the Estates department.

12 Signage

Once CCTV is installed, signage must be erected at entrance points to the Trust premises and throughout the site, to ensure staff and visitors are aware that they are entering an area which is covered by CCTV surveillance equipment. Signage must include the following details:

- Name of the organisation
- Purpose of the surveillance
- Contact details of the appropriate person if there are any queries
- State that the CCTV is registered with the ICO under the terms of the DPA 2018 and ICOs code of practice on CCTV (2023).

13 CCTV operation

All CCTV systems is the responsibility of the head of estates and will be managed in accordance with the principles and objectives expressed in the DPA 2018, the UK GDPR (2018), and the ICOs code of practice on CCTV (2023).

14 Access to view monitors, digital video disc and digital images

Access to view monitors or digital video disc (DVD) and digital images activity will only be granted to persons with a main impact reason (see UK GDPR, 2018) or those who individuals who have followed the subject access procedures.

Subject access request to view footage/images must be made following the process that is available on the staff intranet and/or the public facing website.

IG considerations should always be considered when reviewing any images – see section 8.

15 Disclosure to external parties (anti-fraud specialist, police, court etc)

The police may have access to the CCTV system with the LSMS present in a private area for purposes of aiding detection, deterrence, and prevention of crime. They should submit their own DPA 2018 2.1.2 form, which will provide the purpose of the request and what information is required. The CCTV police request form (appendix 3) must also be completed and signed off by the LSMS before handing over images.

CCTV images will also be potentially disclosed to the Trust's anti-fraud specialist for the purposes of investigating allegations of fraud, bribery and corruption and subsequently may be used as evidence in criminal proceedings. Any queries regarding fraud, bribery and corruption should be directed to the trusts anti-fraud specialist phillip.leong@miaa.nhs.uk

CCTV images also being potentially disclosed to the Trust's anti-fraud specialist for the purposes of investigating allegations of fraud, bribery and corruption and subsequently used as evidence criminal proceedings.

Access and disclosure to images is permitted only if it supports the purpose of the investigation. Under these circumstances, the request will be made to the LSMS as to whether disclosure is appropriate and whether there is a duty of care to protect the images of any third parties, taking advice from the IG team.

It is important that access to, and disclosure of, the images recorded by CCTV is restricted and carefully controlled. This will ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes e.g., a police enquiry or an investigation being undertaken as part of the Trust's disciplinary procedure.

Access to the medium on which the images are displayed and recorded is restricted to Trust staff and third parties. Access and disclosure to images is permitted only if it supports the purpose of the investigation and has been approved by the head of estates or LSMS.

Viewing of the recorded images must take place in a restricted area away from service users and the public.

When CCTV images have been identified for use in legal/disciplinary proceedings or Trust enquiries, the LSMS or head of estates must ensure that they have documented:

- The date on which the images were removed from the system

- The reason why they were removed from the system
- Any crime incident number to which the images refer
- The location of the images
- The appropriate signature is obtained for example - consent/police/court.

The LSMS and head of estates must control access to recorded images.

15.1 When CCTV is provided by a third party

When considering procuring a CCTV system from a third-party supplier, which will be also be operated by a third party, the procurement process must be followed to ensure any third party supplier complies with GDPR (2018) and DPA 2018. Please follow the Third-Pary Supplier Policy.

The third party will be processing personal information on behalf of the Trust and as such, is required to provide the Trust with assurance that all personal information will be processed securely, and that data subjects data rights and freedoms are adhered to as outlined in Article 5 of GDPR 'Principles relating to processing of personal data'; this is to ensure the third-party supplier can meet the GDPR and DPA 2018 requirements.

The DPIA (appendix 4) should be completed by the head of estates and LSMS with support from the IG team. The DPIA will ensure any contract with a third party contains the correct UK GDPR (2018) and DPA 2018 clauses.

The head of estates is responsible for the contract and is responsible for the third-party compliance. The CCTV will be registered on the Trusts information asset register and the contract owner will become the IAO. The IAO is responsible for contract reviews, monitoring third party compliance and reviewing the DPIA regularly and should undertake Trust training every 3 years.

15.2 Subject access request

If an individual submits a subject access request, the Trust process must be followed; the IG team can be contacted for guidance and support. The request should be logged on the Trust SAR log and evidence of anything released to a data subject should be retained. Send any request received to bchft.accesstorecords@nhs.net and request access to the SAR teams folder.

The Trust will accept applications from the data subject, and those acting on their behalf (usually a solicitor) if signed consent is provided.

An application can be made on behalf of a child/ young person under 16 years of age by someone who has parental responsibility for the child. However, a child 12 years old and over is deemed old enough to decide who sees their information and this must be considered before releasing information to the person with parental responsibility. Where children have the capacity to understand the implications and make an informed decision about access to

their recorded image, it would be appropriate to seek their consent in addition to that of the person with parental responsibility.

Care must be taken when dealing with requests for recorded images of children from someone with parental responsibility for the child.

The subject access request may be sent to the service at the location of the CCTV or to the Trust headquarters but will be processed by estates and LSMS with support from the IG team.

16 Use of CCTV footage for disciplinary purposes

Any breach of the ICOs code of practice on CCTV (2023) by staff will be reported using the Trusts risk management reporting system (Ulysses).

Where there is an allegation of a breach in disciplinary rules, as outlined in the Trust's disciplinary policy and procedure, the relevant CCTV footage may be considered during the investigatory stages of the disciplinary processes, and later used in formal disciplinary hearings, if relevant to the allegations raised against the employee.

If such CCTV footage is identified, it will be presented to the employee during the course of the investigation, pursuant to the Disciplinary Policy and Procedure and/or Dignity and Respect at Work Policy and Procedure. The employee will be given the opportunity to review the CCTV footage and explain or challenge its content. The employee will also be permitted to make reference to the CCTV footage in any subsequent disciplinary hearings, if applicable.

If the Trust identifies CCTV footage relevant to formal proceedings, then the timescale for the retention of CCTV footage for initially 6 months shall apply.

CCTV footage retained for the purposes of disciplinary processes will be retained until the expiry of two years following completion of all disciplinary procedures, including any appeals process and statutory reporting to professional bodies.

Activity where CCTV can be provided requested by the human resources business partner may include:

- Acts which constitute gross misconduct in accordance with the Trust disciplinary policy practices which seriously jeopardise the health and safety of others.
- Inappropriate treatment of people who use our services
- Breaches of this policy.

The Trust reserves the right to take disciplinary action against any employee who breaches this policy in accordance with the Trust's disciplinary procedures.

As a major purpose of CCTV is in assisting to safeguard health and safety of staff, the intentional or reckless interference with any part of the any monitoring equipment, including cameras/monitor/back up media/records, may be a criminal offence and will be regarded as a serious breach of Trust policy.

17 Storage of CCTV images/footage

Any hard drives which store CCTV images/footage and require disposal must be done in line with the Trust IT Security Policy.

18 Complaints regarding CCTV

Complaints regarding the operation of the Trust's CCTV system may be progressed through the Trust's patient services – see the Handling of Complaints, Compliments, Comments and Concerns Policy and Procedure.

Staff should direct their own complaints to their manager for escalation to the Human Resources department.

19 Training

Trust staff will not operate the CCTV and no training is required. However, staff should familiarise themselves with this policy and the Data Protection and Confidentiality Policy.

Third party supplier will ensure appropriate training of their staff to include DPA 2018 and UK GDPR.

20 Consultation

Key individuals/groups involved in the development of the policy to ensure it is fit for purpose once approved:

Name	Designation
Digital Information Governance and Information Technology Group (DIGIT)	Director of Finance/SIRO Associate Director of Halton Adult Community Services Deputy Director of Finance Programme Manager Digital Training Manager and Registration Authority Lead (Access Control)
Ruth Besford	Equality & Inclusion Manager
Michaler Kan	Health, Safety, Fire and LSMS
Mary Corkery	Policy Officer
Razia Nazir	Knowledge and Library Services Manager
Phillip Leong	Anti-Fraud Specialist Mersey Internal Audit Agency
John Morris	Head of Estates

Name	Designation
Kristine Brayford-West	Director for Safeguarding Services
Jim Eatwell	Head of Safeguarding Adults
Corporate Clinical Policy Group	

21 Dissemination and implementation

21.1 Dissemination

The head of estates will disseminate this policy to associate borough directors for disseminating to staff via team meetings.

The policy will be made available on MyBridgewater and published in the team brief.

21.2 Implementation

Associate borough directors will ensure this policy is implemented within their areas of responsibility.

All Trust staff will be made aware of their personal and organisational responsibilities regarding handling of NHS confidential records through the Trust training program, and local induction and monitoring audits.

New employees will be made aware of this policy through the local Induction process.

22 Process for monitoring compliance and effectiveness

Process for reviewing compliance and effectiveness i.e., audit, review, survey, incident reporting	Responsible	Frequency of monitoring	Assurance group
Security Risk Assessment	LSMS	Annual	DIGIT
Number of requests to review CCTV	LSMS	Quarterly	DIGIT

23 Standards/key performance indicators

Security risk assessment	LSMS	Annual	DIGIT
Number of requests to review CCTV	LSMS	Quarterly	DIGIT

24 References

Biometrics and Surveillance Camera Commissioner (2021) Update to Surveillance Camera Code of Practice. [online] Available at: https://www.gov.uk/government/publications/update-to-surveillance-camera-code

Biometrics and Surveillance Camera Commissioner (2018) Data protection impact assessment guidance [online]. Available at: https://www.gov.uk/government/publications/data-protection-impact-assessments-for-surveillance-cameras

Care Act 2014 c. 23 [online]. Available at: https://www.legislation.gov.uk/ukpga/2014/23/contents/enacted

Care Quality Commission (CQC) (2021) The Care Act 2014 and the 'easements' to it [online]. Available at: https://www.cqc.org.uk/guidance-providers/adult-social-care/care-act-easements-it

Care Quality Commission (webpage) Using surveillance in your care service [online] Available at: https://www.cqc.org.uk/guidance-providers/all-services/using-surveillance-your-care-service
Accessed January 2024

Data Protection Act 2018, c.12 [online]. Available at: http://www.legislation.gov.uk/ukpga/2018/12/contents

Department of Health and Social Care (2016) Records management: code of practice for health and social care [online]. Available at: https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care

Department of Health and Social Care Code of practice: Mental Health Act 1983 [online]. Available at: https://www.gov.uk/government/publications/code-of-practice-mental-health-act-1983

Equality and Human Rights Commission (2021). Article 8: Respect for your private and family life [online] Available at: https://www.equalityhumanrights.com/human-rights/human-rights-act/article-8-respect-your-private-and-family-life

Freedom of Information Act 2000. [online] Available at: https://www.legislation.gov.uk/ukpga/2000/36/contents

Health and Safety at Work etc Act 1974, c37 [online]. Available at: https://www.legislation.gov.uk/ukpga/1974/37/contents

Human Rights Act 1998 c. 42 [online]. Available at: https://www.legislation.gov.uk/ukpga/1998/42/contents

Information Commissioner's Office (webpage) CCTV and video surveillance. [online] Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/
Accessed January 2024

Mental Health Act 1983 c. 20 [online]. Available at: https://www.legislation.gov.uk/ukpga/1983/20/contents

Modern Slavery Act 2015, c30 [online]. Available at: https://www.legislation.gov.uk/ukpga/2015/30/contents/enacted

NHS Counter Fraud Authority (2021) [online]. Available at: https://cfa.nhs.uk/

NHS Counter Fraud Authority: *Latest NHSCFA news* [online] Available at: https://cfa.nhs.uk/
Accessed: January 2024

NHS England Transformation Directorate (2023) Updates to the Records Management Code of Practice [online]. Available at: https://transform.england.nhs.uk/information-governance/guidance/records-management-code/updates-to-the-records-management-code-of-practice/

NHSx (2021) Records Management Code of Practice [online]. Available at: https://transform.england.nhs.uk/media/documents/NHSX_Records_Management_CoP_V7.pdf

Protection of Freedom Act 2012, c9 [online]. Available at: https://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

Regulation of Investigatory Powers 2000, c23 [online]. Available at: https://www.legislation.gov.uk/ukpga/2000/23/contents

Surveillance Camera Commissioner (2014) Surveillance camera code of practice [online]. Available at: https://www.gov.uk/government/publications/surveillance-camera-code-of-practice

UK General Data Protection Regulation (GDPR) (2018) [online]. Available at: https://uk-gdpr.org/