

CCTV (Closed Circuit Television) Policy

Document Type:	Policy		
Secretariat Index Number:	CP100	Version No:	1.0
Document Owner:	Head of Risk Services & Security Manager		
Clinical/Non-Clinical:	Non-Clinical		
Directorate:	Corporate		
Team/Service:	Risk Services		
Target Audience:	All CPFT staff at all CPFT occupied sites.		
Standards, legislation and key related documents:	<p>Data Protection Act 2018 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 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 Records Management Code of Practice 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</p>		
APPROVAL			
<u>Level 1</u> Speciality Oversight Group:	Workplace Risk Group		
	Date Approved:	31/10/25	Review Date:
			31/10/28
<u>Level 2</u> Approval Group:	Health and Safety Committee		
	Date Approved:	25/11/25	Review Date:
			25/11/28
<u>Level 3</u> Ratification Committee:	Business and Performance Board Sub-Committee		
	Date Approved:	03/02/26	Review Date:
			03/02/29
Financial Implications:	Where a document has any financial implication on the Trust, the Local Counter Fraud Specialist (LCFS) has the authority to investigate and challenge this document with regards to current fraud and bribery		

	legislation and to ensure appropriate counter fraud measures are in place.			
Counter Fraud Approval:	Yes or No:	No	Date:	N/A
Equality and Diversity Impact Assessment: (Policies only)	The author has carried out an E&DIA and there are no negative or unknown impacts. The E&DIA Form is attached to this document.			
Staff Side Approval:	Yes or No:	Yes	Date:	17/09/2025

15.0 Authors Checklist

Document Title: CCTV (Closed Circuit Television) Policy

Secretariat Index Number: CP100

To be completed when reviewing existing published documents

Consideration for all documents		Y/N	Action to be taken	
			'Yes'	'No'
1.	Is the document still required?	Y	Go to question 2.	Arrange document removal with the Executive Lead/Approval Group and inform the Corporate Governance Team (corporateoffice@cpft.nhs.uk)
2.	Has there been any change in guidance or national policy since the previous version?	N	Go to question 4.	Go to question 3.
3.	Can Executive authorisation (only) be granted if minor changes have been made to the document?	N	Executive lead to approve new review date by email. Update dates on the document and send the updated document and Exec email to the Corporate Governance Team (corporateoffice@cpft.nhs.uk)	Go to question 3.
4.	Can formal ratification be granted if major changes have been made to the document?	Y	Agree content at Level 1 Specialty Oversight Group. Seek Approval at Level 2 Exec Led Approval Group. Seek Ratification at NED led Board Sub-Committee (via: corporateoffice@cpft.nhs.uk)	Go to question 3.

Version Control Summary

Formal Ratification Record

Version	Date	Author	Details of Previous Version:	Oversight Group	Approval Group	Ratifying Committee	Date:
1.0	10 th Sept 2025	Head of Risk Services & Security Manager	New policy.	Workplace Risk Group	Health and Safety Committee	Business & Performance	03/02/26

Minor Change Record

Version	Date	Author	Description of Change/s Made:	Authorising Executive	Date:

Content

Authors Checklist.....	1
Version Control Summary.....	1
Formal Ratification Record	2
Minor Change Record.....	2

CONTENTS

1.0 Introduction	6
2.0 Scope.....	6
3.0 Purpose.....	6
4.0 Definitions	7
5.0 Objectives	8
6.0 Rationale.....	9
7.0 Duties, Roles and Responsibilities	9
8.0 Ownership of Images – Data Controllers and Processors.....	10
9.0 Location of Cameras and Equipment.....	10
10.0 Access to Images and Security.....	11
11.0 Viewing and Disclosure of CCTV Footage.....	11
12.0 Releasing of CCTV Footage.....	13
13.0 Law Enforcement.....	13
14.0 Data Subject Access and Third-Party Requests.....	13
15.0 Retention and Disposal.....	13
16.0 Training.....	13
17.0 Processes	14
18.0 Associated Documents.....	14
19.0 Monitoring Compliance.....	15
20.0 Appendixes	
Appendix 1: Equality & Diversity Impact Assessment Form	16
Appendix 2: Quality Assurance Checklist.....	22
Appendix 3: CCTV Considerations – Out-Patient Services	23
Appendix 4: CCTV Considerations – In-Patient Services	24

The latest version of this document is on the Document Library. Any printed copies must be checked against the Document Library version to ensure that the latest version is being used.

1.0 Introduction

- 1.1 Cambridgeshire & Peterborough NHS Foundation Trust (CPFT) recognises the need to regulate the management, operation, and use of the Closed-Circuit Television (CCTV) systems monitoring staff, patients and visitors at premises occupied by CPFT. CPFT is the responsible owner and data controller of all CCTV services and conforms to the Data Protection Act and UK General Data Protection Regulation (GDPR).
- 1.2 The system comprises of a variety of fixed camera types (static and PTZ - pan, tilt, zoom), which can be monitored by assigned staff using HiKCentral on designated screens, or remotely by the Head of Risk Management, Security Manager or a nominated deputy. Access to view and manage historical/archive images/footage is limited to Head of Risk Management, Security Manager or a nominated deputy unless approved through the footage request process using a [Footage Request Form](#). Risk Services is not responsible for CCTV systems operated by other organisations on sites or spaces CPFT staff occupy.
- 1.3 This Policy adheres to the Data Protection Act 2018 and UK General Data Protection Regulation (UKGDPR) and is subject to annual review.

2.0 Scope

- 2.1 This policy applies to all persons employed by Cambridgeshire & Peterborough NHS Foundation Trust (CPFT), Coldwell Banker Richard Ellis (CBRE), NHS Shared Business Services (NHS SBS), private/public contractors or any other groups who access any CPFT occupied site i.e. visitors and patients.
- 2.2 This policy should be read in conjunction with all Trust risk management related policies.

3.0 Purpose

- 3.1 This policy describes the Trust's approach to managing CCTV services in respect of its employees, service users and other parties working in or around CPFT occupied premises.
- 3.2 This policy identifies the purpose of CCTV as increasing safety from both previously identified and potential unknown risks. Where areas are actively monitored via CCTV, patients, staff, visitors and private/public contractors (data subjects) are supported by ensuring that the recorded CCTV footage could be used in the investigation of any incidents and where actively monitored, staff can be alerted and provide a rapid response to incidents likely to cause injury or harm. It also supports safety, the delivery of patient care, environment and property.

The use of CCTV is limited to areas where:

- 3.2.1 Actions and behaviours may result in a risk of injury or harm.
- 3.2.2 Behaviours could result in violence, criminality, injury and intimidation of other service users, staff and visitors.

3.2.3 It assists in the prevention, detection and investigation of crime and assists law enforcement agencies in the apprehension of offenders and minimise the occurrence of unlawful activities.

3.2.4 If a patient is under observation in seclusion or the 136 Suite, watching remotely through use of a camera may be less intrusive and could assist in providing better patient care.

4.0 Definitions

CCTV: Closed-Circuit Television – commonly known as video surveillance, CCTV is an electronic surveillance system comprising cameras, monitors and, in some cases, image recording devices functioning within a closed circuit where the signal is not openly transmitted as it is with broadcast television. The video cameras transmit the surveillance information to a set number of monitors and, in some cases, recorders.

Communal areas: areas of a ward/residential unit that are shared, used routinely by staff, service users, and visitors. For example, corridors, gardens, TV lounges, dining rooms, activity rooms etc. In general, communal areas are quasi-public spaces, in that they are areas where there cannot be a reasonable expectation of total privacy. In such a space it is accepted that the use and function of that space is open to others to move about in freely, without restriction. Or in the case of visiting rooms, there would be limited access for the general ward population, but other members of the public (visitors) could be reasonably expected to be in the space at the same time as patients using the facility.

Data: is defined within the Data Protection Act 2018 and in the context of CCTV means information (images) which:

- a. are being processed by means of equipment operating automatically in response to instructions given for that purpose,
- b. are recorded with the intention that they should be processed by means of such equipment,
- c. are recorded as part of a relevant filing system or with the intention that they should form part of a relevant filing system,
- d. does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68; or
- e. are recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

Data controller: a person who (either alone or a nominated deputy) determines the purposes for which and the manner in which any personal data are, or are to be, processed. As a public authority, CPFT is registered as a data controller in respect of the Data Protection Act 2018.

Data Processor: a person or staff member viewing the footage and acting on behalf of a controller (CPFT), following the controller's specific instructions.

Data Protection Impact Assessment (DPIA): an assessment made before any significant new processing of person-identifiable information or change to existing processing to ensure it complies with data protection regulations and to identify any risks the processing presents. A template for DPIAs is available from the Information Governance Team. CCTV/surveillance camera installations will use the DPIA template provided by the Information Governance Team.

Data subject: an individual who is the subject of personal data. Within the context of CCTV, this relates to a person who is being recorded or monitored by one or more of the Trusts CCTV cameras.

Non-communal areas: These are areas where there would be a reasonable expectation of personal privacy for the person(s) occupying that space. For example, a person's bedroom, the lavatory, the shower/bathroom etc. In context of a mental health ward such private spaces might also include areas where staff have an individual under some form of observation; but that observation would be limited only to the staff assigned to attend to the patient - for example, de-escalation suites, seclusion rooms, or the observation windows in bedrooms. In cases where such close observation is required, privacy masking may be applied on specific sections of the camera's feed/field of view to maintain dignity. Non-communal areas are thus defined here as private, in so much as the person in that space can expect not to be observed by anyone other than the limited number of staff specifically assigned to care for them whilst in that setting.

Personal data: means information relating to an individual which can identify that individual either:

- a. from that data, or
- b. from that data and other information, which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Recorded CCTV: CCTV footage, which is stored on a recording device, which can then be viewed at a later date.

View Only CCTV: CCTV that provides video feeds only in real time to monitoring stations but does not record the footage captured by the camera.

Trust: refers to Cambridgeshire and Peterborough NHS Foundation Trust. (CPFT)

5.0 Objectives

5.1 Within Trust premises surveillance cameras are used for the following purposes only:

- To support overall protection for staff, patients and visitors.
- To protect Trust premises and Trust assets.
- To increase personal safety and reduce the fear of incidents.
- To reduce occurrences of violence and aggression to staff members, patients and visitors.
- To provide supporting data relating to internal and external inquiries.
- To support the reduction and detection of reportable incidents.
- To support the identification, apprehending and prosecuting of offenders.
- To provide a deterrent and reduce criminal or anti-social activity.

6.0 Rationale

- 6.1 In order to support the protection, safety, security and wellbeing of staff, patients, contractors and visitors, while deterring and detecting criminal activity, Cambridgeshire and Peterborough NHS Foundation Trust use CCTV, in accordance with the Data Protection Act 2018 and UKGDPR, to ensure lawful collection of specified, explicit and legitimate data.
- 6.2 CCTV (recorded or view only) provides a means to monitor areas of risk, communal and external areas, so that staff can quickly identify and respond to incidents, potentially preventing injuries or damage, and as evidence in investigations of criminal activity, aiding in the prosecution of offenders.
- 6.3 This policy sets out the actions and procedures for the use of CCTV in communal and external areas which complies with national guidance and legal requirements shown above on p1 under 'Standards, legislation and key related documents.'

7.0 Duties, Roles and Responsibilities

The Chief Executive Officer (CEO)

The CEO is accountable for the implementation of the CCTV policy and compliance with national guidance, standards and legislation.

The Security Management Director (SMD)

The SMD is responsible for promoting security at Board level and for monitoring and ensuring compliance with the requirements and directions issued by the Secretary of State, Department of Health and the Local Counter Fraud Management Specialist (LCFMS) relating to security.

The Senior Information Risk Owner (SIRO)

The SIRO has overall responsibility for the Trust information risk policy. The SIRO is accountable and responsible for information risk across the Trust. The SIRO is responsible for assisting in the overall management of the Trust's CCTV systems, the information risk aspects and compliance around using CCTV systems.

The Data Protection Officer (DPO)

The DPO is responsible for advising on the application of the Data Protection Act 2018 and UK General Data Protection Regulation. The DPO supports Trust-wide data & information governance in accordance with UK GDPR, NHS Digital & England guidance, and in conjunction with the Information Governance Team

Information Governance Team (IGT)

The IGT are responsible for ensuring the Trust is compliant with legal standards and demonstrate good practice in ensuring information is handled in a secure, efficient and effective manner. They must support staff working with sensitive and confidential information, including CCTV footage recorded at Trust locations, which we have a responsibility to hold, use and share securely and safely.

Risk Services - Security

Risk management is the process of systematically identifying risks, analysing the likelihood and impact of their occurrence, and then deciding what action to take to prevent, minimise, accept or transfer these risks in a way that will enable the Trust to minimise losses and maximise opportunities. CPFT are responsible for assisting in the identification, prioritisation and locating of CCTV services to provide assurance that the Trust is taking all reasonable steps to manage risks of all kinds in line with the Risk Management Strategy.

Each CCTV/surveillance camera system constitutes an Information Asset, and Risk Services are responsible as the Information Asset Owner. They are responsible for ensuring that this policy is fully implemented across CPFT locations where areas of risk have been identified and CCTV equipment installed. They must ensure that the policy is available to all staff at all times. They must ensure that relevant documentation and auditing is completed in line with the policy. They must respond appropriately to any concerns regarding the implementation of this policy across the areas of risk where CCTV is installed. They must ensure regular review of the operation and functioning of the CCTV system.

Staff and Contractors

All members of staff have a responsibility to ensure that they comply with relevant security policies and procedures. It is also essential that all security incidents involving or observed by staff are reported in accordance with the Trust's incident reporting procedure (DATIX).

8.0 Ownership of Images – Data Controllers and Processors

- 8.1 As the data controller, CPFT determines the purpose and manner in which any personal data is processed. As a public authority, CPFT is registered as a data controller in respect of the Data Protection Act (2018).
- 8.2 As the data controller, CPFT owns all images/footage captured on any CCTV surveillance system that it owns and controls and retains access to footage for limited purposes and emergencies.
- 8.3 Access to footage from any site with CPFT CCTV installed, is strictly controlled by nominated staff in the Security Team. This [process](#) must be followed by staff when submitting requests to view footage.
- 8.4 Responsibility for the maintenance and repair of all CPFT CCTV systems on owned sites/premises is held by Coldwell Banker Richard Ellis (CBRE).
- 8.5 CPFT are ultimately responsible for all CCTV footage, how it will be used and to whom it can be disclosed, when recorded on equipment it owns.

9.0 Location of Cameras and Equipment

- 9.1 The equipment used, camera settings and locations will be evaluated following the kick-off call shown in these processes for [new installations](#) or [changes to existing installations](#). These evaluations take into account factors such as the cameras required field of view, environment, risks around potential damage and technical aspects around it's required operation and management. This process ensures the use of appropriate cameras that are correctly located to maximise effectiveness and efficiency. However, CPFT can't guarantee that all incidents will be recorded due to a variety of potential causes – damage to cameras, no available power etc

- 9.2 When evaluating the locations of cameras, their proximity to patient bedrooms must be taken into account to ensure the dignity of patients. Cameras can be in communal areas including gardens, common areas such as lounges and corridors in in-patient settings.
- 9.3 CCTV monitors will not be within view of patients or members of the public, including visitors, and will only be located in secure locations i.e. Nursing Stations or staff only areas.
- 9.4 To ensure transparency and raise awareness of the use of CCTV at CPFT locations, signage will be displayed in prominent locations to inform staff, patients, visitors, contractors and members of the public that they are entering an area where CCTV is in operation. The signage will indicate how to contact the Data Owner & Controller can be contacted. The latest CCTV Posters can be found on the CPFT intranet.
- 9.5 The recording of audio on all CCTV cameras is disabled ensuring that clinical or other sensitive communications are not recorded. The only exception to this would usually be the consequence of directed surveillance (more commonly as part of a Police Investigation) that has been subject to a strict RIPA (Regulation of Investigatory Powers Act 2000) submission. The primary function and set-up of CCTV cameras are to monitor and record the movements and actions of patients, staff, contractors and visitors.
- 9.6 Where CCTV cameras are installed in in-patient settings, they will only be located in areas which are deemed necessary following risk assessment, other than when being used for direct observation, such as seclusion suites, CCTV should not replace observation activities by staff.
- 9.7 Where CCTV is installed in in-patient settings, the presence of CCTV cameras must be shared in admission packs and similar documents.

10.0 Access to Images and Security

10.1 Direct access to view historical CCTV footage is restricted to those authorised below. Beyond those listed below, the CCTV footage request process must be followed.

- Head of Risk Services
- Trust Security Manager
- Nominated Deputy
- Fulbourn Hospital DNO (applicable to external site wide CCTV only)
- Fulbourn Hospital 136 Suite
- PICU / Poplar Ward

Locations at Fulbourn Hospital and at The Cavell Centre as listed above have been provided Additional access rights due to the specific nature of their service.

10.2 CPFT staff authorised to export and archive footage from CPFT owned CCTV services, at the locations shown in the process for [footage requests](#), is restricted to:

- Head of Risk Services
- Trust Security Manager
- Nominated Deputy

10.3 CPFT staff authorised to request, access, review and extract footage from 3rd party CCTV services i.e. Medirest, NHSPS, FWD-IP, at the locations shown in the process for [footage requests](#), is restricted to:

- Head of Risk Services
- Trust Security Manager
- Nominated Deputy

11.0 Viewing, Logging and Disclosure of CCTV Footage

11.1 All CCTV screens showing live video footage, are located in a secure room, out of the sight of anyone not directly involved in the monitoring of the cameras. When visitors are permitted to enter these rooms, monitors will be switched to standby mode or if deemed necessary, due to the sensitive nature of patients activities, switched off.

11.2 CCTV will be used to establish the whereabouts of absconder's and/or criminal activity as required but will not be actively monitored on a 24-hour basis. Where footage has been provided through the Formal CPFT footage request process, authorised persons may view the footage using VLC software available through the CPFT App Portal.

11.3 The disclosure of historical CCTV footage will only be provided from the HiK Central system, provided the correct request process has been completed, and is consistent with the purpose for which the system was established:

- To ensure overall protection for staff, patients and visitors.
- To protect Trust premises and Trust assets.
- To increase personal safety and reduce the fear of incidents.
- To reduce occurrences of violence and aggression to staff members, patients and visitors.
- To provide supporting data relating to internal and external inquiries.
- To support the reduction and detection of reportable incidents.
- To support the identification, apprehending and prosecuting of offenders.
- To provide a deterrent and reduce criminal or anti-social activity.

11.4 Requests from patients or other persons for access to CCTV footage concerning them as subject matter must complete a subject access request via CPFTAccessToRecords@cpft.nhs.uk and in line with Access to Health Records, Personnel Records, and CCTV Data Protection Act 1988 Policy. Following subject access requests, and provision to third parties such as insurance companies, the use of redaction software will be applied to protect the identity of persons captured within the footage as appropriate.

11.5 Permission to view historical CCTV footage will not be granted to anyone whose role is not explicitly identified in this guidance.

11.6 Any archiving and provision of CCTV footage by authorised persons will be logged on the dedicated CCTV Footage Release Register held by the Security Service.

11.7 Any viewing of historical CCTV footage by those identified below as authorised, are required to log the relevant details on the viewing log provided by the Security Service.

- Fulbourn Hospital DNO (applicable to external site wide CCTV only)
- Fulbourn Hospital 136 Suite
- PICU / Poplar Ward

11.8 If the request is out of hours, urgent, and cannot wait until the next working day (Monday to Friday between the hours of 0800 and 1800), then the request should be escalated to the on-call manager, if deemed appropriate, the on-call Director can then be contacted via the Trust Switchboard on 01223 219400. The on-call Director may then contact a security representative to facilitate the CCTV request.

11.9 At Fulbourn and Ida Darwin site, the DNO may be contacted if in relation to site/grounds footage and not for within a ward footprint.

- 11.10 Non-urgent requests will be processed within 10 working days (Monday to Friday between the hours of 0800 and 1800).
- 11.11 All requests MUST be made to the Security Team through completion of the CCTV [footage request form](#).
- 11.12 CCTV recordings must be viewed in a closed area by the requestor of the CCTV footage only, unless the Head of Risk Services or Trust Security Manager explicitly give permission for another individual to be there. However, their presence must be documented, and must be to have a direct impact on the purpose for which the CCTV footage is being viewed
- 11.13 Where CPFT occupy areas in leased premises, at sites owned by other organisations, the Head of Risk Services or Trust Security Manager will be responsible for liaising with the relevant team to access CCTV footage if required e.g. Cavell Centre via Medirest.

12.0 Releasing of CCTV Footage

- 12.1 In relation to requests, the Head of Risk Services or Trust Security Manager will liaise with the relevant manager once the request is received. Arrangements can then be made to obtain and review footage if approved.
- 12.2 Whenever footage is released, this will primarily be via the Trust secure file transfer system, however, when not practicable, alternative secure methods will be arranged.

13.0 Law Enforcement

- 13.1 Should CPFT receive a request from any law enforcement agency, the Head of Risk Services, Trust Security Manager or nominated deputy may review, export and release the CCTV footage where the content may assist with detection/prevention of crime/terrorism, or locating a missing person as required.
- 13.2 Law enforcement agencies must provide proof of legitimacy for their request with proof of permission to seek the footage via a formal GDPR Request Form.

14.0 Data Subject Access and Third Party Requests

- 14.1 The Data Protection Act (2018) gives individuals the right to access personal data held in relation to them by CPFT, including CCTV footage. All Subject Access Requests must be made in compliance with CPFT's Data Protection Policy. The Head of Risk Services or Trust Security Manager, with an Information Governance Manager, will arrange to view the images to assess if the release of footage would breach the Data Protection Act (2018) and apply CCTV redaction as and where appropriate.
- 14.2 Please refer to the Access to Health Records, Personnel Records and CCTV Data Protection Act (1988) and make requests to CPFTAccesstoRecords@cpft.nhs.uk
- 14.3 Requests for CCTV footage from 3rd parties e.g. solicitors or insurance companies .Direct their request to information Governance at CPFTAccesstoRecords@cpft.nhs.uk, who will arrange to view the footage to assess if its release would breach the Data Protection Act (2018).

15.0 Retention and Disposal

15.1 All CPFT CCTV footage will be retained for a maximum of 28-days unless CPFT is made known of footage which may assist with the investigation of an incident/crime. In such cases the Trust will export relevant footage and retain it until the investigation and any subsequent procedures are complete. At this time the exported footage will be securely disposed of.

16.0 Training

16.1 Managers are responsible for ensuring their staff are aware of and comply with this CCTV policy, follow [CCTV guidance](#), Data Protection Act 2018 and CCTV Code of Practice. In addition, they must be appropriately trained to use the CCTV systems – the Trust can arrange training if applicable.

17.0 Processes

- 17.1 All staff are responsible, when working in areas where CCTV is installed, for reporting damaged or faulty CCTV equipment to CBRE (0333 015 0430).
- 17.2 All staff responsible for using CCTV equipment must ensure they are appropriately trained and familiar with the system in their working area. Whenever CCTV equipment is changed, they are to ensure they are up to date with these changes and how they will need to operate the CCTV equipment in the future.
- 17.3 The view of any CCTV camera must not be obstructed by equipment/items being used by staff or patients.
- 17.4 Regular review with Estates to ensure obstruction of external cameras is limited from factors such as overgrowth or other lens obstructions.
- 17.5 Potential damage to CCTV equipment must be mitigated against when there is potential risk to its operation.
- 17.6 All staff requiring a change to CCTV equipment in their working area should provide these details using the [Existing CCTV - Change Request Form](#) e.g. additional cameras or changes to cameras settings.

18.0 Associated Documents and Resources

- 18.1 [New Installation Request Form](#)
- 18.2 [Existing CCTV - Change Request Form](#)
- 18.3 [Footage Request Form](#)

16.0 19. MONITORING COMPLIANCE

Document Section		Control	Check to be carried out	How often will the check be carried out	Responsible for carrying out the check	Results of check reported to	Frequency of reporting
Page	Section	WHAT?	HOW?	WHEN?	WHO?	WHERE?	WHEN?
10	8.4	Monitoring, and where required investigation, into CBRE tickets concerning CCTV.	Monthly report CBRE tickets with “CCTV” in the title or body can be filtered and provided by CBRE in a monthly report and quarterly Service Review Meetings.	Monthly	Trust Security Manager.	Head of Risk Services.	Annually.
10	7	Monitoring of security incidents via the DATIX management system to identify the frequency of CCTV footage requests and reliability of this CCTV equipment.	As per the Security Management Policy, the monitoring of security incidents enables the Trust to report and identify any common themes in relation to security incidents – the use of CCTV footage should be included.	Annually.	Trust Security Manager.	Head of Risk Services.	Annually.
10	8.1, 8.2	Monitoring through the Trust Information Security & Confidentiality Audit.	That data is being managed in accordance with the Data Protection Act 2018 and UK General Data Protection Regulation (UKGDPR) 2018.	Annually.	Information Governance (IG) Team.	Head of Risk Services.	Annually.

Equality & Diversity Impact Assessment Form

Introduction

The general equality duty that is set out in the Equality Act 2010 requires public authorities, in the exercise of their functions, to have due regard to the need to:

- Eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by the Act.
- Advance equality of opportunity between people who share a protected characteristic and those who do not.
- Foster good relations between people who share a protected characteristic and those who do not.

The general equality duty does not specify how public authorities should analyse the effect of their existing and new policies and practices on equality, but doing so is an important part of complying with the general equality duty. It is up to each organisation to choose the most effective approach for them. This standard template is designed to help CPFT staff members to comply with the general duty.

Training on undertaking Equality Impact Assessment can be made available for individuals or teams on request. If there is something that is not clear regarding the EIA process or you need help to complete the EIA form please contact:

EDI@cpft.nhs.uk

Sue Rampal - Equality and Diversity Lead

Sharon Gilfoyle – Associate Director of Inclusion

Equality Analysis Form

Name of Proposal - policy, strategy, function, service being assessed:	CCTV (Closed Circuit Television) Policy
Is this a new or existing policy, practice or change to a service?	New Policy
Directorate, Department / Service:	Risk Services
Details of the person completing this impact assessment form. Name, Job Title, Telephone / Extension:	Louise Sheldon-Tabor Head of Risk Services 07889 466056
Those involved in the assessment:	Marcus Speed - Project Manager Sam Ellsworth – Trust Security Manager
Date:	10/09/2025

What are the intended outcomes of this work)? (Include outline of objectives and function aims)	To ensure the protection, safety, security and wellbeing of staff, patients, contractors and visitors, while deterring criminal activity at CPFT occupied locations.
Who will be affected? (e.g. staff, patients, service users etc.)	All CPFT staff, and those accessing any CPFT occupied site e.g. Coldwell Banker Richard Ellis (CBRE), NHS Shared Business Services (NHS SBS), visitors, patients and private/public contractors.
What are the desired outcomes?	<ul style="list-style-type: none"> • To support overall protection for staff, patients and visitors. • To protect Trust premises and Trust assets. • To increase personal safety and reduce the fear of incidents. • To reduce occurrences of violence and aggression to staff members, patients and visitors. • To provide supporting data relating to internal and external inquiries. • To support the reduction and detection of reportable incidents. • To support the identification, apprehending and prosecuting of offenders. • To provide a deterrent and reduce criminal or anti-social activity.
What does this policy, function, process link to in terms of wider Business plans and objectives?	<ul style="list-style-type: none"> • <u>Information Security Policy</u> • <u>Security Management Policy</u>

Evidence considered

When looking at the impact on the equality groups, you must consider the following points in accordance with General Duty of the Equality Act 2010:

In summary, those subject to the Equality Duty must have due regard to the need to:

- eliminate unlawful discrimination, harassment and victimisation;
- advance equality of opportunity between different groups; and
- foster good relations between different groups

Consider how your assessment has been able to demonstrate **Positive Impact**, **Negative / Adverse Impact** or **Neutral Impact**?

What evidence have you considered?

List the main sources of data, research and other sources of evidence This can include national research, surveys, reports, research interviews, focus groups, pilot activity evaluations etc.

Disability Consider and detail on attitudinal, physical and social barriers.

No direct differential impact identified.

CCTV is needed to ensure the overall protection of staff, patients and visitors, in addition to Trust premises and assets and so applies consistently to those with or without a disability.

Neutral impact

Section 2.1 ensures uniform application across all Trust premises. Section 3.0 states CCTV assists where "actions/behaviours of patients may result in a risk of injury or harm" - this provides enhanced safety monitoring for patients who may be unable to easily summon assistance. The oversight controls for footage requests described in section 1 and training requirements in section 8.0 provide assurance that monitoring serves legitimate safety purposes and does not promote disproportionate monitoring. The CCTV policy provides the opportunity to enhance safety and security for disabled people, including protection from harassment or abuse, it also supports identification and resolution of accessibility barriers, providing evidence to support reasonable adjustments and investigations into concerns.

Sex Consider and detail on men and women (potential to link to carers below).

No direct differential impact identified.

CCTV is needed to ensure the overall protection of staff, patients and visitors, in addition to Trust premises and assets and so applies consistently to all sexes.

Neutral impact

Section 2.1 states the policy applies to "all persons" without gender-based distinctions. The privacy masking provisions defined in section 4.0 protect dignity in observation areas regardless of gender. Section 5.0 objectives to reduce violence and aggression provide equal protection for male and female patients, staff and visitors. The monitoring of communal areas supports safety for all genders, as defined by the Supreme Court Ruling April 2025. The consistent application outlined in section 2.1 and oversight controls for footage requests described in section 1 ensure monitoring decisions are not influenced by gender-based assumptions.

Race Consider and detail on difference ethnic groups, nationalities, Roma gypsies, Irish travellers, language barriers. See Trust website for the Patient and Carer Race Equality Framework for more information on how to identify potential impacts for racialised communities. [Patient and Carer Race Equality Framework | CPFT NHS Trust](#)

No direct differential impact identified.

CCTV is needed to ensure the overall protection of staff, patients and visitors, in addition to Trust premises and assets and so applies consistently to all races.

Neutral Impact

Section 2.1 applies the policy uniformly to "all persons" regardless of ethnic background. The footage request oversight process prevents discriminatory access to recordings. Section 3.0's focus on preventing violence and criminality provides equal protection across all ethnic groups accessing Trust services. The transparent footage request process described in section 1 and staff training requirements in section 8.0 support confidence that monitoring serves legitimate safety purposes rather than targeting specific groups.

Age *Consider and detail across age ranges on old and younger people. This can include safeguarding, consent and child welfare.*

No direct differential impact identified.

CCTV is needed to ensure the overall protection of staff, patients and visitors, in addition to Trust premises and assets and so applies consistently to those of any age.

Neutral impact

Section 2.1 applies to "all persons" without age-based distinctions in monitoring arrangements. The policy's focus on preventing violence and supporting patient care outlined in section 3.0 provides protection for both younger and older service users who may be particularly vulnerable. Consistent monitoring standards across all age groups builds trust that decisions are based on safety needs rather than age-based assumptions.

Gender reassignment (including transgender) *Consider and detail on transgender and transsexual people. This can include issues such as privacy of data and harassment.*

No direct differential impact identified.

CCTV is needed to ensure the overall protection of staff, patients and visitors, in addition to Trust premises and assets and so applies consistently to those of all sexes, including transgender.

Neutral impact

The policy applies consistently under section 2.1 regardless of gender identity. Privacy masking capabilities defined in section 4.0 can protect dignity. The safety monitoring objectives listed in section 5.0 provide equal protection for transgender patients, staff and visitors using Trust premises. Uniform application of monitoring standards and oversight procedures build confidence that surveillance decisions are based on safety requirements rather than personal characteristics.

Marriage and Civil Partnership *Consider and detail on married people and civil partners, and how the policy may impact them differently from single people. This can include considerations around visiting rights, next of kin arrangements, and data sharing permissions.*

Neutral impact

The policy applies CCTV monitoring consistently regardless of marital or civil partnership status. The footage request process outlined in section 1 provides equal oversight protections for all individuals captured on CCTV. The policy's objectives in section 5.0 to reduce violence and aggression provide equal protection for patients, staff and visitors regardless of relationship status. The consistent application of CCTV policy as stated in section 2.1 builds confidence that monitoring decisions are based on safety requirements rather than assumptions about individuals' personal relationships.

Sexual orientation *Consider and detail on heterosexual people as well as lesbian, gay and bi-sexual people.*

No direct differential impact identified.

CCTV is needed to ensure the overall protection of staff, patients and visitors, in addition to Trust premises and assets and so applies consistently to those with any sexual orientation.

Neutral impact

Section 2.1 ensures universal application across all Trust premises regardless of sexual orientation. The violence prevention objectives in section 3.0 provide equal safety protections for people of all sexual orientations accessing services. The oversight mechanisms for footage access described in section 1 prevent misuse that could disproportionately affect any particular group.

Religion or belief *Consider and detail on people with different religions, beliefs or no belief.*

No direct differential impact identified.

CCTV is needed to ensure the overall protection of staff, patients and visitors, in addition to Trust premises and assets and so applies consistently to those of all religions or beliefs.

Neutral impact

Section 2.1 applies uniformly to all service users without reference to religious or belief systems. Section 4.0 definitions limit monitoring to communal areas only. The safety objectives in section 5.0 provide equal protection for people of all faiths and beliefs using Trust facilities. The limitation of monitoring to communal areas as defined in section 4.0 respects privacy expectations while maintaining necessary safety oversight.

Pregnancy and maternity *Consider and detail on working arrangements, part-time working, infant caring responsibilities.*

No direct differential impact identified.

CCTV is needed to ensure the overall protection of staff, patients and visitors, in addition to Trust premises and assets and so applies consistently to those staff currently pregnant or on maternity.

Neutral impact

Section 2.1 applies equally to pregnant women and new mothers. Privacy protections in non-communal areas defined in section 4.0 whilst is not specifically addressing activities related to pregnancy or maternity the process identified would maintain dignity for this group. The safety monitoring provisions outlined in section 3.0 provide protection for pregnant women and new mothers who may be particularly vulnerable in healthcare settings. The clear limitations on monitoring scope and oversight procedures support confidence that surveillance respects personal circumstances.

Carers *Consider and detail on part-time working, shift-patterns, general caring responsibilities, protected characteristics of the carer themselves and if this makes seeking help from services more challenging.*

No direct differential impact identified.

CCTV is needed to ensure the overall protection of staff, patients and visitors, in addition to Trust premises and assets and so applies consistently to carers.

Neutral impact

Section 2.1 treats all visitors equally without distinction based on caring responsibilities. Oversight procedures prevent discriminatory access to footage. The safety objectives in section 5.0 provide equal protection for carers visiting or working in Trust premises. Consistent application of monitoring standards supports confidence that surveillance serves legitimate safety purposes for all users of Trust facilities.

Other identified groups *Consider and detail and include the source of any evidence on different socio-economic groups, area inequality, income, resident status (migrants) and other groups experiencing disadvantage and barriers to access.*

No direct differential impact identified.

CCTV is needed to ensure the overall protection of staff, patients and visitors, in addition to Trust premises and assets and so applies consistently to all groups.

Neutral impact

No direct differential impact identified.

CCTV is needed to ensure the overall protection of staff, patients and visitors, in addition to Trust premises and assets and so applies consistently to all groups.

- The policy includes explicit commitment to non-discriminatory use of CCTV.
- Access to CCTV footage is restricted, proportionate, and in line with GDPR.

Engagement and involvement

<p>Have you consulted on the proposal?</p> <p>If so with whom? Head of Risk Services, Trust Security Manager</p> <p>If not why not?</p>
<p>How have you engaged stakeholders in gathering evidence or testing the evidence available?</p> <p>N/A</p>
<p>For each engagement activity, please state who was involved, how and when they were engaged, and the key outputs:</p> <p>N/A</p>

Action planning for improvement:

<p>Outline key actions based on any gaps, challenges, and opportunities you have identified and will be addressed through consultation or further research.</p>			
Category	Actions required to address gaps and issue/s	Target date	Person responsible and their division
Gaps and Challenges	We will make sure information about CCTV is easy to understand and available in different formats, so it is accessible for people with disabilities, people who are neurodiverse, and people who use different languages.	Ongoing as will be on case-by-case basis	Trust Security Manager / Head of Risk Services.
Monitoring, evaluating & reviewing	N/A		

Signed off by EDI Team	Name: 	Date: 02/09/2025
------------------------	--	---------------------

Completed form should be sent to:

EDI@cpft.nhs.uk

Sue Rampal - Equality and Diversity Lead

Sharon Gilfoyle - Associate Director of Inclusion

17.0 APPENDIX 2: QUALITY ASSURANCE CHECKLIST

TO BE COMPLETED BY THE CORPORATE GOVERNANCE TEAM

		Y/N	Comments
1.	Title of document		
	Is the title clear and unambiguous	Y	
2.	Type of document (e.g. policy, guideline etc)		
	Is it clear whether the document is a policy, guideline or procedure?	Y	
3.	Introduction		
	Is the introduction clear?	Y	
	Are reasons for the development of the document clearly stated?	Y	
4.	Content		
	Is the correct corporate template used?	Y	
	Is the document in the correct format?	Y	
	- Paragraphs numbered consecutively?	Y	
	- Headers: logo on front page only?	Y	
	- Footers: on every page except front page?	Y	
	Are the version control numbers correct on the front page and in footer?	Y	
	Are objectives/aims clearly stated?	Y	
	Are duties, roles and responsibilities clearly explained? (Policies only)	Y	
	Are definitions of terms clearly explained?	Y	
	Does this document concern the handling, moving or storage of personal identifiable or commercially sensitive information? If yes, has there been engagement with the Information Governance Team?	N/A	
5.	Evidence Base		
	Is the type of evidence to support the document explicitly identified?	Y	
	Are associated documents referenced?	Y	
6.	Approval		
	Does the document identify which Oversight Working Group is responsible for reviewing the content?	Y	
	Does the document identify which Exec Led Approval Group is responsible for approval?	Y	
	Does the document identify which NED led Ratification Group is responsible for formal sign off?	Y	
7.	Review Date		
	Is the review date identified and 3 years (max) following initial development (sign off by Oversight Working Group)?	Y	
8.	Equality and Diversity		
	Is a completed Equality Impact Assessment attached?	Y	
9.	Monitoring Compliance		
	Has section 'Monitoring Compliance' been completed?	Y	

If answers to any of the above questions is 'no', then this document is not ready for approval and needs further review.

APPENDIX 3: CCTV CONSIDERATIONS – OUTPATIENT SERVICES & PUBLIC AREAS

Is there a plan to install or is there currently an operating CCTV system in an outpatient service or public area?

YES

NO

Is this CCTV needed for one of the following reasons listed in Section 5 of this policy?

Consideration to public areas applies.

YES

NO

A CCTV system on an outpatient's department or public area is unlikely to be justifiably needed.

- CCTV cameras on an outpatient's department or public area, need to be lawful, justified and proportionate in terms of the Human Rights Act 1998.
- Each CCTV system will need to have a specific Standard Operating Procedure.
- The camera must be situated in a place that is clearly visible and positioned in such a way that does not monitor areas not intended to be monitored.
- Move to next section....

Is the / will the proposed CCTV system situated in a non-communal area? A non-communal area is where service users would have a reasonable expectation of personal privacy.

YES

NO

A CCTV system on an outpatient ward in a non-communal area is unlikely to be justifiably needed.

Move to next section....

Is the CCTV footage to be recorded?

If recording is deemed necessary, a separate additional assessment must be conducted to determine: that recording CCTV footage is lawful, justified and proportionate in context of Article 8 to the Human Rights Act 1998. The Trust's recording procedure must be followed to maintain human rights and data governance:

- Recordings are stored on the internal hard drives of the network video recorder (NVR) or digital video recorder (DVR).
- Only the Security Team are authorised to gain access to the NVR or DVR.
- All other staff can only view live footage.
- All recordings on any NVR or DVR will be overwritten/deleted after 31-days. This is set by the DVR or NVR. Recordings are not backed up.

Cameras should be monitored live and sited and operated as per 9.1-9.3

An inventory of all CCTV cameras is to be kept and updated by Coldwell Banker Richard Ellis (CBRE). Risk Services must periodically monitor these records to review the ongoing requirement for CCTV equipment based on Estates plans or the movement of patients or services.

End.

18.0 APPENDIX 4: CCTV CONSIDERATIONS – IN PATIENT SERVICES

