

Closed Circuit Television (CCTV) Code of Practice Policy

V5.0

June 2026

Summary

Main Objectives

The main objective of this code of practice is to assist with the provision of a pro-security culture amongst staff, professionals and the public – to engender a culture where the responsibility for security is accepted by all. This will be achieved using CCTV to assist with the deterrence, prevention and detection of security incidents, crime or breaches of public order whenever possible and to support subsequent investigations.

Key Objectives

To support the purpose and main objective of this code of practice key objectives have been identified and must be applied as follows:

- To assist patient, public and staff safety.
- To deter anti-social behaviour and public disorder.
- Assist in the prevention and detection of criminal activities.
- Assist in the detection of damage caused to Trust property.
- The prosecution of offenders.
- Reduce the fear of crime by promoting a safe environment.
- Traffic flow monitoring.
- Support Counter Fraud investigations or Legal Claims.

Table of Contents

Summary	2
1. Introduction	5
2. Purpose of this Code of Practice	5
3. Scope.....	6
4. Definitions / Glossary	6
5. Ownership and Responsibilities	7
5.1. The Director of Estates and Facilities	7
5.2. The Head of Facilities	7
5.3. Trust Security Lead (LSMS).....	7
5.4. Role of Authorised Security Officers	7
6. Standards and Practice.....	7
6.1. Data Protection.....	7
6.2. Public Information	8
6.3. Code of Practice.....	8
6.4. Breaches of this Code of Practice	8
6.5. Control and Operation of Cameras	8
6.6. Access to the CCTV Control Room and Equipment	9
6.7. Record Keeping and Log Sheets.....	10
6.8. Public Area Monitors	10
6.9. Control of Recorded Data.....	10
6.10. Statement of Intent on Use of Recorded Data	11
6.11. Ownership of Recorded Data	11
6.12. Accurate Recording of Data	11
6.13. Storage of Data and Data stored for Evidence	11
6.14. Release of Data for Investigations	12
6.15. Subject Access Requests – GDPR 2018	12
6.16. Dealing with Incidents	12
6.17. Future Development of the CCTV Scheme.....	13
6.18. Recording of Sound.....	13
6.19. Replica Cameras.....	13
7. Dissemination and Implementation	13
8. Monitoring compliance and effectiveness.....	13
9. Updating and Review.....	14
10. Equality and Diversity	14
Appendix 1. Governance Information.....	15

Appendix 2. Quality and Equality Impact Assessment (QEIA) Form	18
Appendix 3. Guiding Principles	19
Appendix 4. Guidance on the Operational Use of CCTV for Security Officers/CCTV Operators	20
Appendix 5. CCTV Operators Declaration of Confidentiality	22
Appendix 6. Record of CCTV System Review Sheet.....	23
Appendix 7. CCTV Monitoring Room – Visitors Record Sheet.....	25
Appendix 8. The Use of Body Worn Video (BWV) Cameras at the Royal Cornwall Hospitals NHS Trust.....	26
Appendix 9. Body Worn Video (BWV) Staff Operating Procedure	28

Data Protection Act 2018 (UK General Data Protection Regulation – GDPR) Legislation.

The Trust has a duty under the Data Protection Act 2018 and UK General Data Protection Regulations 2016/679 to ensure that there is a valid legal basis to process personal and sensitive data. The legal basis for processing must be identified and documented before the processing begins. In many cases we may need consent; this must be explicit, informed, and documented. We cannot rely on opt out, it must be opt in.

Data Protection Act 2018 and UK General Data Protection Regulations 2016/679 is applicable to all staff; this includes those working as contractors and providers of services.

For more information about your obligations under the Data Protection Act 2018 and UK General Data Protection Regulations 2016/679 please see the Information Use Framework Policy or contact the Information Governance Team.

Royal Cornwall Hospital Trust rch-tr.infogov@nhs.net

1. Introduction

- 1.1. The use of Closed-Circuit Television (CCTV) is viewed by the Royal Cornwall Hospitals NHS Trust (RCHT) as a key element in its promotion of a safer environment. CCTV systems are in use on all three of the Trusts hospital sites, Royal Cornwall Hospital, St Michaels Hospital, West Cornwall Hospital and birthing units at St Austell and Helston hospital sites.
- 1.2. This code sets out the minimum standards that are expected of all employees and users operating CCTV systems in the Trust. Our aim is always to provide a safe and secure environment.
- 1.3. Trust Security Lead (LSMS) in conjunction with the Head of Facilities and the Trusts Information Governance team will be responsible for ensuring all employees and any users of the CCTV system are properly trained to ensure that Data Protection and Human Rights principles and confidentiality are observed and followed.
- 1.4. The efficient operation of CCTV rests with the standards contained within this code of practice. It should be considered as a benchmark for good practice that will ensure accountability and provide public confidence of the system.
- 1.5. Further advice and guidance on the code of practice can be obtained from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf
- 1.6. This version supersedes any previous versions of this document.

2. Purpose of this Code of Practice

2.1. The Code of Practice

The code of practice has been developed to ensure that the CCTV system is operated fairly, within applicable law and only for the purpose for which it is established. That the scheme is operated with due regard to the privacy of the individual and the equipment is only operated and the recorded data viewed by those with a legitimate reason to do so. Use of the system by individuals and other authorities is dependent upon the willingness to comply with this code of practice and to be accountable under this Code and will follow the Home Office guiding principles (see [Appendix 3](#)).

2.2. Main Objectives

The main objective of this code of practice is to assist with the provision of a pro-security culture amongst staff, professionals and the public – to engender a culture where the responsibility for security is accepted by all. This will be achieved using CCTV to assist with the deterrence, prevention and detection of security incidents, crime or breaches of public order whenever possible and to support subsequent investigations.

2.3. Key Objectives

To support the purpose and main objective of this code of practice key objectives have been identified and must be applied as follows:

- To assist patient, public and staff safety.
- To deter anti-social behaviour and public disorder.
- Assist in the prevention and detection of criminal activities.
- Assist in the detection of damage caused to Trust property.
- The prosecution of offenders.
- Reduce the fear of crime by promoting a safe environment.
- Traffic flow monitoring.
- Support Counter Fraud investigations or Legal Claims.

3. Scope

This code of practice applies to authorised staff that will be responsible for the operation and management of the CCTV system used by the RCHT. This will include any contract or temporary member of staff and any authorised non-Trust staff such as Police Officers.

4. Definitions / Glossary

- **Information Asset Owner:** A person who determines the purpose for which and the way any personal data are, or are to be, processed.
- **Recorded Data:** Includes but is not limited to material such as all forms of disks, digital print or media on which images are recorded and can be reconstituted at a later date.
- **Data Subject:** The Data Subject is a living individual to whom personal data relates.
- **CCTV Scheme:** The totality of the arrangements for closed circuit television, including BWC, but not limited to, the technological system, staff, and the operational procedures.
- **LSMS:** Local Security Management Specialist / Trust Security Lead (LSMS).
- **BWC / BWV:** Body Worn Camera / Body Worn Video.

5. Ownership and Responsibilities

5.1. The Director of Estates and Facilities

The Director of Estates and Facilities shall ensure that there is compliance with the Purpose and Main Objectives of the scheme, the management and security of the scheme, and the protection of the interests of the public and of the individual.

5.2. The Head of Facilities

The Head of Facilities is nominated as the Information Asset Owner for the RCHT CCTV scheme.

5.3. Trust Security Lead (LSMS)

The Trust Security Lead (LSMS) shall ensure that security protocols are in place and are being observed in line with the Purpose and Main Objectives of this code of practice. The Trust Security Lead (LSMS) is also nominated as an Information Asset Administrator for the CCTV scheme.

5.4. Role of Authorised Security Officers

- 5.4.1. All Security Officers who work within, or have access to, the CCTV Control Room must sign a Confidentiality Agreement. This authorises them to be present in the CCTV environment but does not permit them to operate CCTV equipment, as they do not hold the relevant licences required by the Trust.
- 5.4.2. Security Officers must be familiar with, and adhere to, the procedures outlined in the Guidance on the Operational Use of CCTV for Security Officers/CCTV Operators (see [Appendix 3](#)). This requirement applies to ensure appropriate conduct within the CCTV Control Room, even though Security Officers are not authorised CCTV operators.

6. Standards and Practice

6.1. Data Protection

- 6.1.1. The RCHT is aware of the legal responsibilities placed upon it by the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Human Rights Act 1998.
- 6.1.2. The CCTV system will be operated in full compliance with this current code of practice.
- 6.1.3. The RCHT will maintain appropriate signage to identify that a CCTV scheme is being operated on its premises. These signs will provide the necessary information required to conform to the Data Commissioner's code of practice.
- 6.1.4. Further information in respect of Data Protection or Human Rights issues can be obtained from the Head of Information Governance.

6.2. Public Information

- 6.2.1. As far as it is consistent with the objectives of the system and to comply with the Data Protection Principles, the cameras are placed in public view and signs informing the public and staff that they are in an area covered by CCTV are erected and maintained.
- 6.2.2. The signs will identify the purpose and a telephone contact number and the Trust as owners of the CCTV scheme.

6.3. Code of Practice

This code of practice is a public document and will be available for inspection. The availability of the code of practice and Subject Access requests will be made clear within this code of practice.

6.4. Breaches of this Code of Practice

- 6.4.1. The code of practice sets out the principles by which the CCTV system is required to be operated. All staff who are involved in the operation and management of the system are required to work in accordance with it. Breaches of the code of practice may result in disciplinary action and, in certain circumstances, suspension and summary dismissal.
- 6.4.2. Breaches of the code of practice must be subject to proper investigation by an individual with relevant professional qualifications. This person shall be responsible for making recommendations to remedy any breach detected.

6.5. Control and Operation of Cameras

- 6.5.1. The CCTV system is a powerful means of observing members of the staff/public, going about their everyday duties/business. It is therefore only used for the express purposes set out in this code of practice, in order that the rights and civil liberties of members of the staff/public are protected.
- 6.5.2. The system is only used for surveillance in the hospitals and grounds and not to invade the privacy of any individual in residential, business, or other private premises, buildings or land. Operational procedures as well as technological measures should be employed to restrict surveillance into private premises.
- 6.5.3. Cameras are not to be targeted on individuals, except at the request of the police, or in circumstances when the CCTV operator considers that an unlawful activity is being, or is about to be carried out, or to follow such individual(s) after such activity has or is thought to have taken place. The cameras are not used specifically to view the interiors of private dwellings or offices.

- 6.5.4. CCTV operators should be aware that recordings made by controllable cameras will be subjected to routine audit and inspection and will be required to justify any reason to target an individual of private area.
- 6.5.5. When defects are found on any item of equipment that affect the control and operation of the CCTV system, they are to be reported immediately to the Security Systems Administrator or Trust Security Lead (LSMS), who will take the necessary action to have the defects rectified.
- 6.5.6. In conjunction with the Estates Operational Electrical team, the Trust Security Lead (LSMS) will monitor quality of the maintenance or repair work that is undertaken by the Trust's contractors.
- 6.5.7. Security Systems Administrator / the Trust Security Lead (LSMS) will keep an up-to-date record of all the functioning CCTV cameras that are covered by this code of practice.

6.6. Access to the CCTV Control Room and Equipment

- 6.6.1. Access into the control room whether to operate the equipment or view the images is limited to staff who have been authorised to do so. Others may be permitted to operate the equipment or view the images, but only by express permission from the Information Asset Owner or the Trust Security Lead (LSMS).
- 6.6.2. Security of the CCTV Control Room will be always maintained. Security Officers/CCTV Operators and authorised personnel who have signed a Confidentiality Agreement have free access to the Control Room.
- 6.6.3. Close liaison between the police and the Trust is encouraged. Police visits will normally be prearranged or maybe simply to collect recorded evidence or interview staff. Other visits by the police may take place from time to time in accordance with the provision of this code of practice.
- 6.6.4. Entry to the Control Room by any other person is by prior arrangements only. All visitors without exception are required to sign the visitors' record sheet immediately on entering the Control Room.
- 6.6.5. Unauthorised access to the Control Room may constitute a breach of the General Data Protection Regulation 2018 and must be reported to the Head of Information Governance and the Head of Facilities and the Trust Security Lead (LSMS).

6.7. Record Keeping and Log Sheets

A list of records and log sheets that are required to be maintained is as follows:

- 6.7.1. **Confidentiality Agreement**; to be signed by all Security/CCTV control Officers; nominated managers or any other person who will have regular access to the control room.
- 6.7.2. **Record of Access to the Control Room by Visitors**: to be signed by any visitor who has not completed a Confidentiality Agreement form.
- 6.7.3. **Data Released for Evidential Purposes Record**: to be completed on each occasion that evidence is archived or released as a result of requests made for evidential data in line with this code of practice.
- 6.7.4. **Subject Access Requests**: for requests made by the public or other body in line with the General Data Protection Regulation 2018. All Subject Access Requests are to be processed by the Head of Information Governance before data can be provided.
- 6.7.5. **CCTV playback Records Log**: a record log will be maintained for each occasion where recorded images are replayed. The log will record all details and reasons of each playback operation.

6.8. Public Area Monitors

The Trust has provided monitors to enable staff based in public receptions or wards to monitor entrances and waiting areas so that visitor and patient access or attendance for safety reasons can be monitored. There will be no ability to access any recorded material from these areas, and the monitors are purely installed for awareness purposes.

6.9. Control of Recorded Data

Within the RCHT CCTV Scheme recorded data relates to data recorded and stored on Digital Video Recorders (DVR), Network Video Recorders (NVR), data archived to computer hard drive, data saved to compact disk, digital prints or uploaded into encrypted systems. Several legally enforceable principles apply to this section, notably:

- 6.9.1. Recorded data may be used in court as evidence. It must be of good quality and be accurate in content. Recorded data must be treated according to defined procedures to provide continuity of evidence and to avoid contamination of the evidence.
- 6.9.2. Appropriate security measures shall be taken against unauthorised access to, alteration of, disclosure or destruction, and against accidental loss or destruction of recorded data.
- 6.9.3. Recorded data should only be held for the purposes provided by this code of practice.

- 6.9.4. Information recorded should be accurate, adequate, relevant and not exceed that necessary to fulfil the purposes and key objectives of the scheme.
- 6.9.5. Recorded data shall be kept no longer than is necessary for the purposes and key objectives of the scheme. It must then be safely destroyed (see 6.13).
- 6.9.6. Members of the public must be confident that the information recorded about their ordinary activities in the public area covered by the cameras is treated with regard their individual privacy.
- 6.9.7. Only data required as evidence for police or internal criminal investigation(s) will be retained. The data should only be retained for the duration of the investigation.

6.10. Statement of Intent on Use of Recorded Data

- 6.10.1. Recorded data will be used only for the purposes defined in this code of practice.
- 6.10.2. Access to recorded data will only take place as defined in this code of practice. Recorded data will not be sold or used for commercial purposes or the provision of entertainment.
- 6.10.3. The showing of recorded data to the public will only be allowed in accordance with the law; either in compliance with the needs of the police in connection with an investigation into crime, which will be conducted in accordance with The Police and Criminal Evidence Act, The Criminal Procedures and Investigations Act and The Criminal Procedure (Scotland) Act 1995; or in any other circumstance prescribed by Law.

6.11. Ownership of Recorded Data

Ownership of recorded data always remains the property of the Royal Cornwall Hospitals NHS Trust.

6.12. Accurate Recording of Data

Recording equipment should be checked regularly to ensure it is in good working order and that the date and time shown on the recordings is correct.

6.13. Storage of Data and Data stored for Evidence

- 6.13.1. Data will be retained on each DVR/NVR for a maximum of 31 days, before being over-written. The minimum number of days recorded is aimed at being 31 days.
- 6.13.2. The DVR located in the Mortuary had been programmed to store images for 62 days specifically to support evidence which may be required by HM Coroners Service.

- 6.13.3. Data is automatically recorded on the hard drive of each DVR/NVR. The recorded material is automatically overwritten as and when the hard drive reaches its capacity or at a maximum of 31 days recordings (62 for the RCHT Mortuary DVR). The hard drive recording capacity is determined by factors such as the capacity of the drive, the number of cameras the device has to record and the number of frames per second that the DVR/NVR is set at per camera. There is no requirement for any manual intervention in this process once the unit has been programmed.
- 6.13.4. Data of incidents that are required for evidence by the police must be archived to a secure drive on the Trust IT network. When requested the incident data should be saved to a compact disk or a printed digital photo produced. If the investigation is complete and the archived data has not been requested the data should be deleted from the Trust IT network.

6.14. Release of Data for Investigations

- 6.14.1. No data will be released for evidence without being recorded. Authority is required for any release of data from the Information Asset Owner or the Trust Security Lead (LSMS). Data can be released in a variety of media by the Trust Security Lead (LSMS) which may be by compact disk, USB, a hard copy or electronic digital still photograph or encrypted data transfer via the evidence portal.
- 6.14.2. When a request for evidence for an internal investigation is made in line with the Purpose and Main Aims of this code of practice the relevant data should be logged in the "Data Released for Evidential Purposes Record" by the Information Asset Owner or the Trust Security Lead (LSMS) prior to being released. Any request for evidence for an internal investigation which falls outside of the Purpose and Main Aims of this code of practice will not be supported.
- 6.14.3. Data released to the police or any other authority shall at no time be used for anything other than the purpose specified and identified when the data is released to the police by the Trust.

6.15. Subject Access Requests – GDPR 2018

Upon receipt of a data subject access request under the terms of the General Data Protection Regulation 2018, the request will be forwarded to the Disclosure Office / Head of Information Governance who will comply with the legal requirements of the request.

6.16. Dealing with Incidents

- 6.16.1. Incidents that clearly fall within the Purpose and Main Objectives of this code of practice will be provided with support by the provision of data from the CCTV scheme.

6.16.2. Requests to provide data for incidents that do not fall within the Purpose and Main Objectives of this code of practice will not be supported unless the request is made in line with the provisions of the General Data Protection Regulation 2018 or the Human Rights Act 1998 or the Freedom of Information Act 2000.

6.17. Future Development of the CCTV Scheme

Future installations and developments, including technological advances of the CCTV scheme, will only be made if they support the Purpose and Main Objectives of this code of practice.

6.18. Recording of Sound

Sound will not be recorded by the CCTV scheme. Sound will be recorded when Body Worn Video recordings are being made.

6.19. Replica Cameras

To ensure that staff and public confidence about the CCTV scheme is maintained, replica (dummy) cameras will not be used.

7. Dissemination and Implementation

- 7.1. Managers need to ensure that all staff they manage are aware of this policy. This should be achieved by discussion at departmental meetings and through the departmental processes for implementation of new policy.
- 7.2. Those members of staff who will directly be involved in the operation of the CCTV system will receive training to support and enable them to operate the system in line with relevant legislation and this code of practice.

8. Monitoring compliance and effectiveness

Information Category	Detail of process and methodology for monitoring compliance
Element to be monitored	Records.
Lead	Trust Security Lead (LSMS).
Tool	Software and camera function checks, CCTV room access sheet checks. User login and playback records.
Frequency	Software and camera faults will be checked by the Security / Systems Administrator.
Reporting arrangements	Completed reports will be sent to the Health and Safety Committee.

Information Category	Detail of process and methodology for monitoring compliance
	The report should where possible demonstrate the positive effects made in Crime Detection across the Trust. These results should be documented in the Health and Safety Committee meeting minutes.
Acting on recommendations and Lead(s)	Recommendations and action planning for any identified deficiencies or recommendations will be presented at the next appropriate meeting of The Health and Safety Committee. Identified actions will be completed in a specified timeframe according to the level of threat posed.
Change in practice and lessons to be shared	Any changes that are identified and require action will be taken to the Estates and Facilities Senior Leadership Team and the Health and Safety Committee. The Trust Security Lead (LSMS) will implement changes where identified. Any lessons learned will be shared with all relevant stakeholders.

9. Updating and Review

- 9.1. This Code of practice will be reviewed every three years or earlier if there are changes directed by National legislation or Policy.
- 9.2. Any revision activity is to be recorded in the Version Control Table as part of the document control process.

10. Equality and Diversity

- 10.1. This document complies with the Royal Cornwall Hospitals NHS Trust service Equality and Diversity statement which can be found in the [Equality Diversity And Inclusion Policy](#) or the [Equality and Diversity website](#).
- 10.2. Equality Impact Assessment

The Initial Equality Impact Assessment Screening Form is at Appendix 2.

Appendix 1. Governance Information

Information Category	Detailed Information
Document Title:	Closed Circuit Television Code of Practice V5.0
This document replaces (exact title of previous version):	Closed Circuit Television Code of Practice V4.0
Date Issued/Approved:	February 2026
Date Valid From:	June 2026
Date Valid To:	June 2029
Author/Owner:	Natasha Quick, Trust Security Lead (LSMS).
Contact details:	01872 25 2147.
Brief summary of contents:	The operation of the RCHT CCTV scheme is carried out in compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Human Rights Act 1998, and the guidance issued by the Surveillance Camera Commissioner.
Suggested Keywords:	Code of Practice, CCTV, CCTV scheme, BWV, Body worn video.
Target Audience:	RCHT: Yes CFT: No CIOB ICB: No
Executive Director responsible for Policy:	Director of Estates and Facilities
Approval route for consultation and ratification:	Health and Safety Committee
Manager confirming approval processes:	Natasha Quick, Trust Security Lead (LSMS)
Name of Governance Lead confirming consultation and ratification:	Melanie Seager, Administration and Service Support Co-Ordinator (Business)

Information Category	Detailed Information
Links to key external standards:	UK General Data Protection Regulation (UK GDPR). Data Protection Act 2018. Regulation of Investigatory Powers Act 2000 (RIPA). ICO CCTV Code of Practice. Surveillance Camera Code of Practice (Protection of Freedoms Act 2012).
Related Documents:	UK General Data Protection Regulation (UK GDPR). Data Protection Act 2018. Human Rights Act 1998. Protection of Freedoms Act 2012 – Surveillance Camera Code of Practice. Information Commissioner’s Office (ICO) – CCTV Guidance. Secured by Design (SBD) – Hospitals Guidance. Regulation of Investigatory Powers Act 2000 (RIPA).
Training Need Identified:	Yes
Publication Location (refer to Policy on Policies – Approvals and Ratification):	Internet and Intranet
Document Library Folder/Sub Folder:	Estates and Facilities / Security.

Version Control Table

Date	Version Number	Summary of Changes	Changes Made by
20 February 2013	V1.0	Initial issue.	Paul Dixon, Security Manager/LSMS
12 April 2016	V1.1	Reviewed for accuracy and currency.	Paul Dixon, Security Manager/LSMS
13 November 2018	V2.0	Reviewed for accuracy and amendments made to recording duration.	Paul Dixon, Security Manager/LSMS
September 2021	V3.0	Reviewed for accuracy and amendments made.	Paul Dixon, Head of Security

Date	Version Number	Summary of Changes	Changes Made by
January 2023	V4.0	Full review for accuracy and currency. Addition of Appendix 8 and 9.	Paul Dixon, Head of Security
June 2025	V5.0	Full reviewed for accuracy and amendments made.	Natasha Quick, Trust Security Lead (LSMS)

All or part of this document can be released under the Freedom of Information Act 2000.

All Policies, Strategies and Operating Procedures, including Business Plans, are to be kept for the lifetime of the organisation plus six years.

This document is only valid on the day of printing.

Controlled Document.

This document has been created following the Royal Cornwall Hospitals NHS Trust [The Policy on Policies \(Development and Management of Knowledge Procedural and Web Documents Policy\)](#). It should not be altered in any way without the express permission of the author or their Line Manager.

Appendix 2. Quality and Equality Impact Assessment (QEIA) Form

The QEIA process allows RCHT to monitor the impact of changes to its policies and services, ensuring that nobody is unduly disadvantaged.

Please ensure you have completed a Quality and Equality Impact Assessment (QEIA) using this link to complete the form:

[E11 QEIA Policy](#)

For guidance, please see the [QEIA Essentials – Quick Reference Guide](#) or contact as required below:

Equality, Diversity and Inclusion guidance, please contact: rcht.inclusion@nhs.net

Quality Governance guidance, please contact Jillian Tozer: jillian.tozer3@nhs.net

Appendix 3. Guiding Principles

System operators should adopt the following 12 guiding principles:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The use of a surveillance camera system must consider its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

Appendix 4. Guidance on the Operational Use of CCTV for Security Officers/CCTV Operators

1. Introduction

- 1.1. Each CCTV/Security Officers is responsible for their actions and of maintaining the integrity of the CCTV system. All CCTV operators are charged with operating the system within the guidelines set out in this code of practice.
- 1.2. CCTV/Security Officers will sign a confidential agreement and must understand the significance of the document.
- 1.3. The code of practice sets out the principles by which the CCTV system is required to be operated. All staff involved in the operation and management of the system are required to work in accordance with it. Breaches of the code of practice may result in disciplinary action and, in certain circumstances, suspension and summary dismissal.
- 1.4. The Purpose and Objectives of the CCTV scheme is to assist with the deterrence, prevention and detection of security incidents, crime or breaches of public order whenever possible and to support subsequent investigations.
- 1.5. The CCTV/Security Officer has a great deal of flexibility in the actual operation of the cameras, but it is essential that everyone's actions remain within the boundaries of the code of practice. As CCTV/Security Officers, you must be able to always justify your actions and demonstrate that no party has been favoured at any time, impartiality is essential to the operation of the system.

2. Duties of the CCTV/Security Officer

- 2.1. CCTV/Security Officers may be tasked with the day-to-day use of the system in line with the Purpose and Main Objectives of the code of practice. These tasks will include aspects such as system checks, checking data accuracy and the upkeep of records such as official and other visitors to the CCTV control room.
- 2.2. While undertaking CCTV scheme duties the CCTV/Security Officers are to use their secure password when they access the CCTV system. This will then begin a clear audit trail of the CCTV/ Security Officers' use of the system. As soon as the CCTV/Security Officers have completed their duties within the CCTV control room they are to log out of the system to end the audit trail.
- 2.3. Security officers should change their passwords regularly and at least every six months as a minimum.
- 2.4. CCTV/Security Officers are to sign a Confidentiality Agreement not to divulge information about the operation of the CCTV Scheme. This Confidentiality Agreement will be sufficient to allow the CCTV/Security Officer access to the CCTV control room at any time while on duty for the Trust. (see [Appendix 4](#)).

- 2.5. CCTV/Security Officers will be responsible for ensuring all visitors to the CCTV control room that have not signed a Confidentiality Agreement are recorded in the visitors' log. (see [Appendix 5](#)).
- 2.6. CCTV/Security Officers will be responsible for ensuring that they make a record of each time recorded CCTV footage is reviewed. The information recorded shall include the reason for the review, a description of what has been reviewed, who was present in the room during the review, which DVR/NVR and cameras were reviewed. This form shall be signed by the officer conducting the review. (see [Appendix 6](#)).
- 2.7. All CCTV/Security Officers must be fully conversant with the content of the Royal Cornwall Hospitals NHS Trust Closed Circuit Television code of practice.
- 2.8. Requests made to CCTV Administrators or Security Officers for data to be released for Evidential Purposes must be referred to in the first instance to the Trust Security Lead (LSMS). In the absence of the Trust Security Lead (LSMS) requests should be referred to the Head of Facilities, then the Head of Information Governance.
- 2.9. Requests made to CCTV Administrators or Security Officers for Subject Access under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 are to be forwarded to the Head of Information Governance, via the Disclosure Team who will comply with the legal requirements of the request.

Appendix 5. CCTV Operators Declaration of Confidentiality

This confidentiality agreement acknowledges that my duties allow me access to the Royal Cornwall Hospitals NHS Trust CCTV Control Room and the data processed by the system.

I agree that I have read the code of practice in respect of the operation and management of that CCTV system including [Appendix 3](#) of the code of practice. I hereby declare that:

- (a) I am fully conversant with the content of that code of practice, including [Appendix 3](#) of the code of practice, and understand that all duties which I undertake in connection with the Royal Cornwall Hospitals NHS Trust CCTV system must not contravene any part of the current code of practice, or any future amendments of which I am made aware. If now, or in the future, I am or become unclear of any aspect of the operation of the system or the content of the code of practice, I undertake to seek clarification of any such uncertainties.
- (b) I understand that I must not disclose or divulge to any individual, firm, company, authority, agency or other organisation, any information which I may have acquired in the course of, or for the purposes of, my position in connection with the Royal Cornwall Hospitals NHS Trust CCTV system, verbally, in writing or by any other media or mobile device, now or in the future, (including such time as I may no longer be retained in connection with the CCTV system).

In appending my signature to this declaration, I agree to abide by the code of practice at all times. I also understand and agree to maintain confidentiality in respect of all information gained during the course of my duties, whether received verbally, in writing or any other media format or mobile device - now or in the future.

Signed:	
Print Name:	
Position:	
Date:	

Appendix 6. Record of CCTV System Review Sheet

Reason for Reviewing CCTV Images:		
Description of Incident being reviewed:		
Name of all persons present in the CCTV room at the time of the review	Job Title	
1.		
2.		
3.		
4.		
5.		
Reviewing Officers Name (Printed)	Reviewing Officers Signature:	Date Images Reviewed
Confidential – by signing this sheet you agree to the following statement. In line with the Level 2 Award for Working as a CCTV Operator (Public Space Surveillance) within the Private Security Industry, and in accordance with relevant statutory legislation such as the Human Rights Act 1998, the UK General Data Protection Regulation (UK GDPR), and the Data Protection Act 2018, the content of any live or recorded images on this CCTV system must not be viewed or disclosed to anyone who is not part of the Trust Security Services team or a member of Devon and Cornwall Police, unless expressly authorised by a member of the RCHT Security Services Management		

The reverse of this form must be completed by the reviewing officer.

Record of reviewed images			
DVR/NVR Name	Camera Name/s	Date-time- incident start	Date-time incident Finish
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			

The first page of this sheet must be signed.

Appendix 7. CCTV Monitoring Room – Visitors Record Sheet

All entries should be neatly printed except for signatures

The on-duty Security Officers must ensure that this form is completed by ALL visitors Warning to Visitors - This is a Restricted Area.

In accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Human Rights Act 1998, by signing this visitors' sheet you agree - **not to disclose any information obtained, overheard, or observed during your visit. This includes anything you may see on the CCTV screens. Failure to comply may result in you committing a criminal offence.**

Date	Name of Visitor	Organisation / Company	Visitor Signature	Reason for Visit	Responsible Officer	Time In	Time Out

Appendix 8. The Use of Body Worn Video (BWV) Cameras at the Royal Cornwall Hospitals NHS Trust

1. Introduction

This document details how those members of staff who are authorised to use Body Worn Video (BWV) at the Royal Cornwall Hospitals NHS Trust should approach and use BWV to achieve the aims described below.

2. Aims of using BWV

2.1. The Aims of using BWV is to:

- Ensure high quality and standards of service.
- Prevent and defuse incident escalation.
- Increase the opportunity to capture accurate evidence.
- Reduce complaints.

2.2. Staff should follow this guidance when dealing with members of the public and when gathering any evidence or information to ensure that the quality and integrity of the evidence or information is preserved. This document and associated procedure must be followed during any incident where BWV is used.

3. Purpose of using BWV

- 3.1. The Royal Cornwall Hospitals NHS Trust is committed to providing a safe environment for our patients, staff and visitors. The use of BWV should be considered necessary to prevent or reduce difficult incidents or inter-actions that may occur.
- 3.2. The use of BWV will conform with the requirements of the UK General Data Protection Regulations (UK GDPR) and the Data Protection Act 2018 as described in the CCTV code of practice.

4. Scope of this Document

- 4.1. This document is intended to standardise the use of BWV and the use of evidence that may be produced as a result of using BWV.
- 4.2. The Royal Cornwall Hospitals NHS Trust is committed to maximising its effectiveness in helping to provide a safe environment for our patients, staff, and visitors.
- 4.3. The Royal Cornwall Hospitals NHS Trust will use BWV to clearly demonstrate its commitment to providing a safe environment for our patients, staff, and visitors in line with the CCTV code of practice.
- 4.4. BWV equipment should only be used in line with the guidance provided in this document. All staff authorised to use BWV should receive necessary training and support in its use and of the implications of breaching any relevant legislation.

4.5. All staff will use equipment in line with attached operating procedure.

5. Implications of this Document

- 5.1. This document provides guidance to the users of BWV at the Royal Cornwall Hospitals NHS Trust on the correct use of BWV cameras to record data for a variety of identified problems. The use of BWV should only be used to record footage assessed as being necessary by users of the equipment
- 5.2. Staff who are authorised to use BWV equipment will be provided with suitable training and instructions from an appropriate person before being allowed to use a BWV.
- 5.3. Staff who are authorised to use BWV equipment will sign to acknowledge that they have read and understood the Trust CCTV code of practice, [Appendix 8](#) and [Appendix 9](#).
- 5.4. The Royal Cornwall Hospitals NHS Trust will monitor the use of BWV to ensure the equipment is an appropriate support method and that its use is in line with policy and procedure.

6. Updating and Review

This document will be reviewed in line with any legal or procedural changes to ensure that the use of BWV is appropriate and adds value to the Royal Cornwall Hospitals NHS Trust objectives.

7. Related Policies

Royal Cornwall Hospitals NHS Trust Closed Circuit Television code of practice.

Appendix 9. Body Worn Video (BWV) Staff Operating Procedure

1. Introduction

The document explains the process by which The Royal Cornwall Hospitals NHS Trust will utilise the Body Worn Video (BWV) devices. It will ensure a consistent and effective approach is adopted throughout the organisation benefiting both members of the public and staff.

- 1.1. BWV Devices will be used by trained staff. BWV has the potential to significantly prevent, deter escalation, and record events involving conflict. In cases which involve legal redress it can improve the quality of evidence provided by members of the organisation. It also has the ability also raise standards of service.
- 1.2. BWV can be used across a wide range of operations and in all cases users and supervisors must use professional judgment with regard to the use of this equipment and the Human Rights Act 1998.
- 1.3. There are some examples of situations where the use of BWV is not appropriate; the following list is for guidance only and is not exhaustive.
 - **Legal privilege** – users must be careful to respect legal privilege and must not record material that is, or is likely to be, subject to such protections.
 - **Private dwellings** – users must consider the right to private and family life (Article 8 of the Human Rights Act 1998) and must not record beyond what is necessary for the requirements of the individual case.
- 1.4. The activation and use of BWV must be made clear by security staff who should make a verbal announcement to those people who may be recorded. In some cases, it will not be practical to make such an announcement, on these occasions this announcement must be made as soon as practicable.
- 1.5. BWV cameras might be small; however, they are not to be worn or used in a hidden or covert manner ensuring maximum impact on prevention and escalation of an incident.
- 1.6. The decision to record or not to record any incident remains with the user. The user must be mindful that failing to record an incident may require explanation. Therefore, if the user is present at an encounter where BWV can be used to record evidence the user should record the incident.
- 1.7. Recording should be incident-specific: users should not indiscriminately record entire duties and only use recording to capture video and audio at incidents that would normally require reporting, whether these are ultimately required for use in evidence.

2. Risk Assessments / Health and Safety Considerations

Each incident should be subjected to a dynamic risk assessment on its own merits. When using BWV the decision to record or not record forms part of this risk assessment. The assessment should include consideration of the health and safety, human rights, and welfare of all those involved.

3. Booking out equipment

- 3.1. All cameras should be kept in the CCTV control room along with any batteries and media cards (if used). A supervisor/manager will be responsible for maintaining the security of the cameras and the allocation to staff who have been instructed in its use. They should ensure that a suitable issue and returns log is available to show continuity of an audit if required.
- 3.2. When issued with the equipment the user should ensure that it is working correctly. This process should include the following basic checks:
 - Unit is correctly assembled.
 - Recorded image is the right way up.
 - Sound recording level is appropriate to use.
 - Date and time stamp is accurate.
- 3.3. Issues with the BWC should be reported as soon as possible to the security management and operations team.
- 3.4. Only trained personnel should be permitted to use BWV devices. On completion of training, trained staff will be authorised to use the equipment. Suitable staff will carry out the training. A record of instruction will be maintained.

4. Recording Events

- 4.1. Recordings should only be made in situations where the BWV wearer decides the incident is a recordable incident, or action has been taken to prevent an incident from escalating. All recordings have the potential to be used in evidence even if it appears at the time that this is unlikely. It is important to record as much of an incident as possible. Recording should begin at the earliest opportunity at the start of any event.

4.2. Image Capture Warnings

- 4.2.1. At the start of any recording, the user should, where possible, make a verbal announcement to indicate why the recording has been activated. If possible, this should include:
 - The date, time and location.
 - The nature of the incident.

- Confirmation to those present that the incident is being recorded using both video and audio recording.
- 4.2.2. If the recording has started prior to arrival at the scene of an incident, the user should, as soon as possible, announce to those present that recording is taking place and that actions and sounds are being recorded. Users should use straightforward speech that can be easily understood by those present, such as “I am video recording you”, “I am video recording this incident” or “everything you say and do is being recorded on video”.
 - 4.2.3. Users should attempt to minimise the intrusion of privacy on those people who are present and not involved in the incident, by keeping the camera focused on the incident and not bystanders.
 - 4.2.4. Unless circumstances dictate otherwise, recording must continue uninterrupted from the start of recording until the conclusion of the incident. It is advisable that the member of staff continues to record for a short period after any incident to clearly demonstrate to any subsequent viewer that the incident has concluded, and that the user has resumed other activities.
 - 4.2.5. Prior to stopping any recording, the user should make a verbal announcement to indicate the reason for ending the recording.

5. Selective Capture and Bookmarking

- 5.1. Selective capture occurs when the user makes a choice of when to record and when not to record. The nature of some incidents may make it necessary for the user to consider the justification for continuing to record throughout an entire incident. In cases where the user does interrupt or cease recording, they should record the decision including the grounds for making such a decision.
- 5.2. When recording an incident, it is likely that BWV users will encounter different people, as well as recording visual evidence at the incident itself. Selective capture is a means by which users may separate encounters with each person to allow for easier data retrieval at a later time. It is recognised that bookmarking (temporarily stopping and restarting recording) is not always practicable due to the nature of incidents; therefore, it should only be attempted if the situation is calm and the operator is easily able to undertake this action.
- 5.3. Prior to any temporary suspension for the purpose of bookmarking, the user should make a verbal announcement clearly stating the reason for suspending recording. Following any pause, when recording re-commences the user should also announce that they have recommenced recording.
- 5.4. The bookmarking process will be demonstrated on the final whole recording of the incident by a missing section of a few seconds.

6. Use of BWV in Private Dwellings

- 6.1. BWV used by trained security officers is not to be used in areas which are not owned or managed by the Royal Cornwall Hospitals NHS Trust.
- 6.2. In some circumstances staff may find that an incident which was recorded on Trust property may escalate off a main site. In such circumstances staff should consider the need to continue recording with care. Factors to consider in this decision-making process are:
 - The requirement to secure best evidence of any events that have occurred, whether this is in writing or on video, and that the video evidence will be more accurate and of a higher quality and therefore in the interests of all parties.
 - That continuing to record would safeguard both parties, with a true and accurate recording of events, any significant statement made by either party and of the scene.
- 6.3. These factors should be explained to any person objecting to the recoding of any incident.
- 6.4. It is recommended that staff continue to record where incidents occur and if it becomes clear that the incident is not a matter suitable for recording the user must make a verbal announcement that the recording is being stopped prior to stopping the recording.

7. Transfer of Images to BWV Evidence Management System

- 7.1. Before the completion of duty each BWV user will transfer any recorded data from the camera to the BWV Evidence Management software system for storage and retention.
- 7.2. Any transfer of recorded data to unauthorised storage facilities may result in legal or disciplinary proceedings.
- 7.3. Footage not requested as evidence by the Police or by Subject Access Requests (SAR) will be erased after 31 days in accordance with the Trust CCTV code of practice and in line with guidance from the Surveillance Camera Commissioners office.

8. Deletion of Images

- 8.1. There are no circumstances in which the unauthorised deletion by the user or other person of any images that have already been recorded can be justified, and any such action may result in legal and, or disciplinary proceedings.
- 8.2. All non-evidential data will be retained on BWV Evidence Management software for 31 days and then deleted through the system settings.
- 8.3. Once the transfer of the images has been completed all footage stored on a recording device or similar media will be deleted through the correct use of the BWV Evidence Management software.

9. Return of Equipment

- 9.1. At the end of each shift users should return the BWV unit to the appropriate storage facility. The user will ensure that all equipment is in working order and suitable for re issue.
- 9.2. Any damage or malfunctions must be escalated to the supervisor responsible for the equipment. or the management team.
- 9.3. Care should be taken to ensure that the device and any batteries are placed on charge ready for further use.

10. Responsibilities

The following guidance should be followed by all the below listed users of the BWV system;

10.1. Responsibilities of the BWV Camera User

It is the responsibility of the BWV user to ensure that:

- 10.1.1. Equipment is checked prior to deployment to ensure it is working correctly.
- 10.1.2. The batteries are charged prior to use and immediately recharged on return.
- 10.1.3. The time and date settings are accurate.
- 10.1.4. The camera lenses are clean, and the picture quality is suitable.
- 10.1.5. The camera lens is aimed and focused appropriately to capture evidence.
- 10.1.6. Compliance with legislation and guidance.
- 10.1.7. View only footage they have recorded for a relevant reason.

10.2. Responsibilities of the BWV Administrator

- 10.2.1. Administrators will be responsible for ensuring the BWV Evidence Management software is maintained and being used correctly.
- 10.2.2. They will carry out audit of the system to ensure standards are maintained. Findings will be reported to the appropriate line management.
- 10.2.3. They will also ensure that all documents associated with BWV use, such as booking in/out, viewing of footage, deletion and production of evidence conform to this procedure and the CCTV code of practice.
- 10.2.4. Ensuring that the access to and viewing of footage is appropriate and controlled in line with guidance and legislation.

- 10.2.5. Responsible for fault reporting and follow up action at the earliest opportunity to ensure that the equipment is available for use at all times.

10.3. Responsibilities of the BWV Managers

Identified managers are responsible for the implementation of this document within their own hospital site. They will ensure the use of BWV is ethical and correct in all areas of business.

11. Review of procedure

This document will be subjected to regular review, commencing one year from the date of publication, unless a change in procedure is identified earlier. The review will acknowledge changes in legislation and working practices, as well as the outcome of consultation with relevant internal departments and external agencies and any evaluation. Reviews will be carried out by the Royal Cornwall Hospitals NHS Trust.