

# SURVEILLANCE POLICY

<b>Department / Service:</b>	Health and Safety
<b>Originator:</b>	Fiona Dwyer Local Security Management Specialist and Julie Noble Head of Health & Safety and Fire Manager
<b>Accountable Director:</b>	Director of Estates and Facilities
<b>Approved by:</b>	Health and Safety Committee
<b>Date of approval:</b>	7 <sup>th</sup> November 2024
<b>First Revision Due:</b>	7 <sup>th</sup> November 2027
	<b>This is the most current document and should be used until a revised version is in place</b>
<b>Target Organisation(s)</b>	Worcestershire Acute Hospitals NHS Trust
<b>Target Departments</b>	Health and Safety/ISS
<b>Target staff categories</b>	Operational Health and Safety Managers/ISS Management /CCTV Operators

## Policy Overview:

This policy aims to identify the management of surveillance cameras covered by Worcestershire Acute Hospitals NHS Trust's to include Worcestershire Royal Hospital, Alexandra Hospital and Kidderminster Treatment Centre sites. This includes Closed Circuit television (CCTV), Body Warn Cameras (BWC) and automated number plate recognition (ANPR) cameras (where applicable).

This Policy outlines the procedures that must be followed by the Trust and their security service providers in setting up and operating all surveillance camera systems.

It also outlines the legal obligations to comply with the:

- Data Protection Act 2018 /
- UK GDPR (collectively "Data Protection legislation") and ensuring compliance to the
- Principles of the Freedom of Information Act 2000 (FOIA),
- Human Rights Act 1998 (HRA),
- Regulation of Investigatory Powers Act (RIPA) 2000,
- Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012 (POFA code) and
- Body Worn Video Guidance 2014 issued by the College of Policing.

The intention of this policy is to ensure staff, visitors and patients are secure whilst on the premises.

Date	Amendment	By:
1 <sup>st</sup> Feb 21	Original (revision 1)	J.Spells with advice from CW Audits
April 2024	Review of whole document to also include body Warn Cameras and Automated Number Plate Recognition cameras	Fiona Dwyer and Julie Noble

## Contents:

1. Introduction
2. Scope of this document
3. Definitions
4. Responsibility and Duties
5. Policy detail
6. Implementation of key document
  - 6.1 Plan for implementation
  - 6.2 Dissemination
  - 6.3 Training and awareness
7. Monitoring and compliance
8. Policy review
9. References
10. Background
  - 10.1 Equality requirements
  - 10.2 Financial Risk Assessment
  - 10.3 Consultation Process
  - 10.4 Approval Process

## Appendices

- 1 Operational Procedures
- 2 Installation Checklist
- 3 Internal CCTV Request Form
- 4 External CCTV Request Form (Police/Public)

## Supporting Documents

Equality Impact Assessment  
Financial Risk Assessment

## 1. Introduction

**1.1** The overall purpose of this policy is to regulate the management, operation and use of the Surveillance systems covering Trust premises. The Trust is committed to protecting the safety and security of Trust staff, service users/carers and visitors () and protecting Trust premises and assets from criminal and malicious activities.

**1.2** It also outlines the Trust's legal obligations to comply with:

- Data Protection Act 2018 (DPA)
- General Data Protection Regulations UK GDPR (collectively "Data Protection legislation")
- Human Rights Act 1998 (HRA)
- Ensuring compliance to the principles of the Freedom of Information Act 2000 (FOIA)
- Regulation of Investigatory Powers Act (RIPA) 2000 and
- Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012 (POFA code).

**1.3** Within the Trust premises surveillance is operated 24 hours a day, 7 days per week, and is used for the following purposes only:

- To protect Trust premises and Trust assets.
- To increase personal safety and reduce the fear of crime.
- To support the Police in reducing and detecting crime.
- To assist in identifying, apprehending, and prosecuting offenders.
- To protect staff, patients and visitors.
- To provide a deterrent effect and reduce criminal activity.
- To assist in the traffic management scheme.

**1.4** Prior to the installation of any CCTV system and the siting of cameras and, as part of the annual compliance review, the Trust considers the potential impact on those whose images may be captured by the system and whether the use of surveillance cameras remains the most appropriate and proportional security/surveillance measure that can be deployed to achieve the identified objective.

**1.5** The Trust's Surveillance systems comprise of a variety of camera types. This includes Closed Circuit television (CCTV), Body Worn Cameras (BWC) and automated number plate recognition (ANPR) cameras (where applicable).

**1.6** The Information Commissioners Office (ICO) CCTV Code of Practice requires that Surveillance signs be placed so that the public are aware that they are entering a zone which is covered by surveillance equipment.

**1.7** The signs should contain the following information:

- Identity of the person or organisation responsible for the scheme.
- The purposes of the scheme.
- Details of whom to contact regarding the scheme.

**1.8** The Trust will investigate any breaches of the policy, using appropriate mechanisms. As a major purpose of these schemes is in assisting to safeguard the health and safety of staff, service users and visitors, it should be noted that intentional or reckless interference with any part of

any monitoring equipment, including cameras/monitor/back up media, might be considered a criminal offence.

## 2. Scope of this document

**2.1** The policy is binding on all employees of Worcestershire Acute Hospitals NHS Trust and applies to other persons who may, from time to time, and for whatever purpose, be present on any of its premises.

**2.2** Surveillance cameras can assist in the robust monitoring of areas that may need observing to maintain levels of safety and security to those people utilising the Trust's facilities. Surveillance cameras alone will not prevent staff or patients being assaulted or property being stolen or damaged. However, combined with good local security systems and procedures, it can help to prevent and detect security related incidents, as well as provide evidence to assist the investigation of incidents.

**2.3** Body worn cameras (BWC) are worn by the Trust's Security Officers at Worcestershire Royal Hospital (WRH) and Alexandra Hospital (ALX), additionally BWC are worn by Trust staff at WRH, ALX and Kidderminster Treatment Centre (KTC). All usage must be in line with the Body Worn Video Guidance 2014 issued by the College of Policing; therefore, reference to CCTV images and recordings within this policy will also include any footage captured by body worn cameras.

**2.4** Worcestershire Acute Hospitals NHS Trust is only responsible for surveillance systems in respect of which it is the data controller for the purposes of the Data Protection Act 2018 and the General Data Protection Regulations 2018 (GDPR).

## 3. Definitions

Title	Definitions
<b>Body Worn Camera (BWC)</b>	Surveillance camera worn by members of security or staff for the purpose of recording interactions with members of the public or patients.
<b>Caldicot Guardian (CG)</b>	A Caldicott Guardian is a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly.
<b>Close Circuit Televisions (CCTV)</b>	A self-contained surveillance system, comprising cameras, recorders and displays for monitoring activities in the Trust
<b>Collateral Intrusion</b>	Capturing of images of individuals not covered by the stated purpose of the system. Background images.
<b>Covert Surveillance</b>	Recording of images of individuals without their knowledge or consent
<b>Data Protection Act 2018 (DPA)</b>	Is a UK Act of Parliament designed to protect personal data stored on computers or an organised paper filing system. It enacted the EU's Data Protection Directive 1995's provisions on the protection, processing and movement of data.

<b>Data Protection Impact Assessment (DPIA)</b>	Is a process that helps organisations identify and minimise risks that result from data processing. DPIAs are usually undertaken when introducing new data processing processes, systems or technologies.
<b>Data Protection Officer (DPO)</b>	Legally mandated position within the Trust responsible for ensuring that the Trust is compliant with all EEA/UK data protection legislation.
<b>Freedom of Information Act 2000 (FOI)</b>	Provides the public access to information held by public authorities. The Act covers any recorded information that is held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland.
<b>Information Commissioner's Office (ICO)</b>	Is the independent regulatory office in charge of upholding information rights in the interest of the public. The organisation covers the Data Protection Act, the Freedom of Information Act and the Environmental Information Regulations.
<b>Regulation of Investigatory Powers Act (RIPA)</b>	Is an Act of the Parliament of the United Kingdom, regulating the powers of public bodies to carry out surveillance and investigation, and covering the interception of communications.
<b>Subject Access Request (SAR)</b>	Is a statutory right that patients/staff have under the Data Protection Act 2018 to obtain from the Trust a copy of the information that is held about them.

## 4. Responsibility and Duties

### 4.1 Managing Director

The Managing Director has the ultimate management responsibility for security within the Trust. The Trust as the overall owner of all Surveillance schemes (excluding ISS Body Worn Cameras) on Trust sites has the responsibility to:

- to ensure compliance with this policy;
- to ensure that the operating procedures for all schemes are complied with at all times;
- to ensure that the purposes and objectives of all schemes are not exceeded;
- to notify all persons on the Trust property where CCTV is installed and that a CCTV scheme is in operation;
- to facilitate formal subject access requests of any images captured under the terms of the Data Protection Act 2018 & the General Data Protection Regulations;
- to provide copies of this policy when required to do so;
- to ensure that all CCTV schemes have appropriate signage to inform people entering and leaving buildings/car parking that CCTV is in operation;
- to ensure CCTV screens cannot be seen by individuals who are not authorised to do so;
- to ensure ISS who operate CCTV on the Worcestershire Royal Hospital site for the Trust and the Trust staff at ALX and KTC comply with all legislation contained within this policy.

### 4.2 The Director of Facilities and Estates

The Director of Facilities and Estates has strategic responsibility for:

- ensuring that there is a consistent and co-ordinated approach to health and safety throughout the Trust.
- bringing the policy to the attention of all Trust staff.
- advising the Managing Director of any health and safety matters that compromise the effectiveness of the organisational structure, procedures, or systems.

All cameras, monitors and data collection and retention processes are maintained operationally by Facilities staff and further maintained by third party provider organisations under separate maintenance contract to the Trust in accordance with this policy. The Local Security Management Specialist will monitor the use of all CCTV, undertake regular audits to ensure compliance with relevant legislation and guidance and provide advice and guidance on their use.

#### 4.4 Caldicott Guardian

Each NHS Trust and Board has an appointed Caldicott Guardian. The Caldicott Guardian has a strategic role for the management of patient information. The Guardian's key responsibilities are to oversee how staff use personal health information and ensure that service users' rights to confidentiality are respected.

#### 4.5 Data Protection Officer

The Data Protection Officer is the title given to the person with the legal obligations for compliance in respect of the handling of personal data and faces two obligations in relation to the personal data they hold.

Firstly, a data controller is required to comply with the eight principles of good information handling (the Data Protection Principles), and secondly to let the Information Commissioner know certain details about themselves including the types of information held and the purposes for which they process personal data.

#### 4.6 Local Security Management Specialist (LSMS)

A nationally accredited post that has responsibility for all security issues within an NHS Trust. The LSMS should:

- have oversight of the output specification and procedures supporting the operational use of all surveillance in the health body to ensure compliance with all relevant guidance and provide assurance to the Director of Estates & Facilities with legal responsibility for all cameras, that these requirements are being met.
- lead on the development of existing cameras systems as well as any new or replacement installations. There should be due regard to the appropriateness of this technology in a healthcare setting - informed by risk assessments and crime prevention surveys - and the need to support it with effective policies on its use.
- in conjunction with estates and facilities leads, should also ensure that the surveillance systems are properly maintained. Requirements and procedures for system maintenance should be considered as an essential element in the design and procurement of the system.
- ensure that all recorded images should be viewed in a restricted area, such as a designated secure office and this area be restricted to authorised persons. A list of authorised persons is retained by them for audit purposes and reviewed at least annually or when circumstances change.

#### 4.7 CCTV System's Processors

The Trust is responsible for completing a DPIA to assess the appropriateness of, and reasons for using surveillance cameras or similar surveillance equipment.

At WRH the Trust's PFI Partner is the Surveillance Camera System's Processors. They are responsible for:

- Ensuring they comply with the provisions of the Data Protection Act 2018, CCTV Code of Practice 2000 and Security Industry Authority licensing requirement
- Ensure that suitably trained members of staff are nominated and responsible for the day to day administration and operation of the system
- Ensuring any identified problems are notified to the servicing contractor for remedial action as soon as is reasonably possible and to the LSMS for information.

- Ensuring all system staff are aware of how to process:
  - Form 1: Request to Confirm CCTV / BWC Images exist and are Safely Stored – NOT INCLUDING POLICE see APPENDIX 3
  - Form 2: EXTERNAL CCTV REQUEST FORM (POLICE/ SOLICITOR) APPENDIX 4
- Record all incidents and complaints and any actions taken. To be reported to the Trust yearly
- Record all requests for access to the images by either the Data Subject or the Police, including the time taken to respond to the request. To be reported to the Trust quarterly.
- Ensure the images captured are usable and stored in a way that is secure and maintains the integrity of the image and information especially the meta data (time, date, location is reliable).

At Alexandra Hospital (ALX) and Kidderminster Treatment Centre (KTC) this responsibility falls to the licensed CCTV operators.

#### 4.8 All CCTV Installers and Security Service Providers

All CCTV Installers and Security Service Providers on Trust sites will comply with applicable contracts with the Trust in relation to the installation of CCTV, including the provision of documented operational requirements, risk and data protection assessments. Once the CCTV system is installed the Security Manager, whether contracted or in house, will ensure the day-to-day compliance with the Data Protection Act.

#### 4.9 All Staff

All Staff have the responsibility to:

- Comply with this policy.
- Report all crimes and breaches of surveillance security including near misses in line with Incident Management Policy, including the Management of Serious Incidents.

Reportable incidents will include, but not be restricted to:

- CCTV Procedure failures; any failure of CCTV security systems that has or could have led to a breach of security in line with this strategy and policy.
- Suspected Fraud; in line with the Trust's Counter Fraud, Bribery and Corruption Policy.

Significant threats to Surveillance security, as described in this document, including instances of repeated offence, shall be recorded on a relevant appropriate risk register, in line with the Risk Management Strategy.

### 5. Operation of Surveillance Cameras

**5.1** Security Officers and CCTV Licensed Trust staff are licensed to operate the CCTV system and the ability to zoom, manoeuvre, play back and record images is limited to these licensed officers.

**5.2** Regular checks are to be carried out to ensure that the recorded images are of good quality. Any problems with CCTV systems or cameras impacting on their normal operation should be immediately logged and rectified as soon as is practicable by requesting a service engineer.

**5.3** A CCTV Maintenance Log should be completed whenever any maintenance work takes place, giving the date and time of work.

**5.4** The aim of the Trust's CCTV system is to maintain the safety and security of individuals and property; and for prevention and detection of crime and disorder, to facilitate the apprehension and prosecution of offenders and apprehension of suspected offenders; or as necessary in the public interest such as preventing or detecting unlawful acts or protecting the public against dishonesty.

**5.5** Covert surveillance is not permitted. Only for specifically defined instances in accordance with the declared purposes and objectives of these schemes, may such surveillance equipment be used for targeted observation. The Regulation of Investigatory Powers Act (RIPA) 2000 regulates the use of covert/directed surveillance of this type and is subject to a strict code of practice. Use of CCTV in these instances or for any other reason other than that authorised, in accordance with this policy is not permissible at any time or circumstance.

**5.6** No directed surveillance can be undertaken without specific authorisation from an authorising officer within a 'relevant authority'.

## **6. Policy Detail**

**6.1.** No surveillance scheme should be initiated, installed, moved or replaced without prior approval by the Caldicott Guardian, or delegated officer to approve such schemes. The Data Protection Officer, the Local Security Management Specialist and Head of Health and Safety and Fire Manager must also be informed.

### **6.2 Principles**

- 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.
- The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
- 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.
- There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
- 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.
- 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.
- Access to retained images and information should be restricted and there must be clearly defined rules (See Appendix 1 Operational Procedures for the Control and Use of CCTV) 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.
- 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.
- Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use. All requests to access any images must be authorised by the Data Protection Officer or delegated team.
- There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and an annual report submitted to the Information Governance Steering Group.
- 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.
- 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.



### 6.3 Data Protection Legislation

All schemes will operate in accordance with the guidelines set out in the 'CCTV Code of Practice' and additional guidance published by the Information Commissioner, a copy of which is available from the Data Protection Officer or direct from the Information Commissioner's website: <https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/>

The Trust must adhere to the following guidelines, to conform to the Data Protection Act 2018 and the General Data Protection Regulations 2018 (GDRP) and CCTV Code of Practice:

- LSMS will be responsible for overseeing that monitoring of all images are done so in accordance with this policy and that suitable operation, backup, retention, destruction and maintenance of all storage media is conducted in accordance with the written standard operational procedures (see Appendix 1 Operational Procedure for the Control and Use of CCTV).
- CCTV cameras will not be hidden from view.
- Appropriate steps must be taken, eg by signing and displaying posters, to inform the public of the presence of the various surveillance systems operating within the Trust and its ownership at all times.
- To ensure privacy, the CCTV and ANPR cameras are fixed and focused only upon Worcestershire Acute Hospitals NHS Trust property, which must be demonstrable upon specific request.
- Images from ALL cameras are appropriately recorded in accordance with existing standard operational procedures.

### 6.4 The General Data Protection Regulations (GDPR) 2018:

Due regard will be given to the data protection principles contained in Article 5 of the GDPR which provide that personal data shall:

- processed lawfully, fairly and in a transparent manner.
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- accurate and, where necessary, kept up to date.
- kept in a form which permits identification of the data subjects for no longer than necessary for the purposes for which the personal data are processed.
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The above guidelines are not an exhaustive list of what must be done to comply with the CCTV Code of Practice and Body Worn Video Guidance 2014 issued by the College of Policing.

Those involved in the implementation, operation or management of surveillance schemes will need to be familiar with the requirements of the Data Protection Act 2018, the CCTV Code of Practice, Body Worn Video Guidance 2014 issued by the College of Policing and other relevant legislation and guidance and the General Data Protection Regulations (GDPR).

## 7. Recording and Retention

7.1 All CCTV systems are recorded, and images retained for 31 days.

**7.2** Where images need to be retained beyond 30 days these must be promptly copied into a secure network folder and retained in line with Trust guidance.

**7.3** All recordings must be logged and traceable.

**7.4** A decision to use Surveillance images as evidence will be based on a case-by-case basis and on the issues surrounding the case; and if criminal offences have been committed or suspected or it is in the public interest then the use would be proportionate and appropriate.

## **8 Viewing and Disclosure of Recordings (Subject Access)**

**8.1** Images of individuals captured by cameras constitute as their personal data. Under the Data Protection Act 2018 and the General Data Protection Regulations (GDPR) individuals have the right to obtain copies of their personal data and a description of such data, the purposes for which it is being processed and the recipients (or classes of recipients) to whom it may be disclosed.

**8.2** A valid request must be made in writing to the DPO, however, it does not need to refer to the Data Protection Act 2018 and can be made by any employee or officer of the Trust. Therefore, any written request by an individual for images of him or herself should be treated as a subject access request and followed in accordance with the Trust's Data Protection Policy and the General Data Protection Regulations (GDPR).

**8.3** Only the Data Protection Officer, in response to a formal request from the data subject, will permit viewing. In instances where no recorded images are retained (instantaneous viewing only) data subjects will be informed that the system produces no recordable images and that subject access in these particular instances can only be granted for the purposes of determining the extent of the monitoring.

**8.4** Individuals or their authorised representative wishing to access images from the system or formal subject access requests specifically relating to CCTV or BWC must contact the Trust's Data Protection Officer. The Data Protection Officer will confirm or deny authorisation on Form 1 (Request to confirm CCTV/BWC images exist and are stored).

**8.5** Judgments about disclosure of surveillance images (whether under subject access or otherwise) should be made by the trust. The Trust has discretion to refuse any request for information unless there is an overriding legal obligation, such as a court order or valid subject access request. The privacy of third parties who are included in the images should be protected at all times.

## **9 Access to Images**

### **9.1 Requests by staff to view images or have a permanent copy.**

Should a staff member be subject to a disciplinary investigation, it may be appropriate to grant them or their staff side representatives access to CCTV, BWC and / or ANPR images pertinent to the investigation, providing the investigation is associated with the stated purpose of the Surveillance scheme and in accordance with and subject to the principles of the Data Protection Act 2018. Only the images relating to the specific events at the centre of the allegation or incident will be accessed. All requests for access must be made in writing to the system administrator, who will subsequently authorise access to facilitate the request to view the images, to facilitate the making of a permanent copy. The Data Protection Officer must also be consulted in the event that the footage in question includes other individuals.

## 9.2 Requests by the Police (or Other Third Party Agencies) to access images

Some incidents may constitute criminal acts, e.g. theft or assault, and the surveillance images may be useful in the prosecution of individuals committing such acts. In these circumstances, all necessary co-operation will be given to the police in pursuit of their duties (subject to Section 29 of the Data Protection Act 2018). During the course of criminal investigations, it may be appropriate to permit the police to view images recorded by the system.

Such requests should be formally made in writing to the Data Protection Officer, Worcestershire Acute Hospitals NHS Trust. The police may also require a permanent record of the image. Once a case has been concluded, the police need to ensure that their copy of the data is destroyed.

## 9.3 Timescales

All responses to those requesting access to the images should be provided within 30 days in accordance with the Data Protection Act 2018.

## 9.4 Manipulation of images

All images provided to third parties as a permanent copy will have third-party faces blurred out (i.e. pixelated) to maintain confidentiality.

## 9.5 Decision making

In considering requests for access to images, the Data Protection Officer will use the guidance issued by the Information Commissioner.

## 10 Registered Users of Surveillance Cameras

The Trust is responsible for the registering and de-registering of users and keeping an up-to-date record of staff that are registered to operate CCTV or BWC. This will be delegated to the appropriate line manager who will ensure that staff are able to use the system competently and are conversant with these operational procedures.

They will ensure the maintenance of an accurate administration system for CCTV in line with standard operating procedures including storing, viewing, copying, issuing permanent records, equipment testing and fault reporting. They will also be responsible for the keeping of all requests to access images.

## 11 Complaints

Any complaints about the use of Surveillance Equipment should be made through the Trust's complaints procedure. Alternatively, individuals are entitled to make a complaint direct to the Information Commissioners Office.

## 12 System Evaluation and Audit

A report will be prepared by the Local Security Management Specialist on the Trust's CCTV system on an annual basis for the attention of the Information Governance Steering Group (IGSG) and Health and Safety Committee. The report will include summaries of all requests for data, instances of its use, its impact on the level and type of incidents, audit records and a commentary on its effectiveness.

## 13 Consultation

This Policy has been developed by the Local Security Management Specialist in conjunction with the Head of Health and Safety and Fire. As part of its development the Trust has also involved the:

- Information Governance Team
- Deputy Director of Estates and Facilities (Soft FM),
- ISS Site Services Manager,
- Head of Facilities and Director of Estates and Facilities.
- Portering & Transport Team – ALX

## 14 Related Policies & Codes of Practice

- Data Protection Act 2018
- Information Governance Policy
- Information Commissioner's Office CCTV Code of Practice
- The General Data Protection Regulation (2017 –May 2018)
- Body Worn Video Guidance 2014 issued by the College of Policing
- Surveillance Camera Code of Practice 2022
- Grievance Procedures.
- Security Policy
- Mobile Device Policy
- SOP regarding the use of Body Worn Camera's

## 15 Training

With regards to CCTV, relevant staff will be fully briefed and trained in respect of all functions; operational and administrative, relating to CCTV control operation, by the installer of the system. In addition, SIA training for CCTV Operators will be a requirement.

Training by camera installers will also be provided as appropriate to authorised staff.

With regards to Trust BWC, training will be provided by the camera company as well as the system administrators, which are currently the Local Security Management Specialist and Head of Health and Safety and Fire. The PFI will provide training for all security guards.

## 16 Monitorin

This policy, its operation and the operation of Worcestershire Acute Hospitals NHS Trust's Surveillance schemes will be reviewed annually by the trust's nominated Local Security Management Specialist providing an annual report to the Information Governance Committee.

## 17. Implementation

### 17.1 Plan for implementation

The implementation of this policy will be achieved through Health and Safety Committee.

### 17.2 Dissemination

To all staff via Trust Intranet site.

### 17.3 Training and awareness

See Appendix 1

18. Monitoring and compliance

Page/ Section of Key Document	Key control:	Checks to be carried out to confirm compliance with the Policy:	How often the check will be carried out:	Responsible for carrying out the check:	Results of check reported to: <i>(Responsible for also ensuring actions are developed to address any areas of non-compliance)</i>	Frequency of reporting:
	<b>WHAT?</b>	<b>HOW?</b>	<b>WHEN?</b>	<b>WHO?</b>	<b>WHERE?</b>	<b>WHEN?</b>
	Surveillance Policy	Review	3 Years	H/S	Document uploaded to Intranet.	Every 3 years
	SOP	Review	3 Years or following incident	System Administrator	Document uploaded to Intranet.	Every 3 years
	Training	Licence Check	3 Yearly	System Administrator	System Administrator Licence List	Yearly
	Incidents	Review	Quarterly	Local Security Management Specialist	Report to Information Governance	Quarterly

## 19. Policy Review

Health and Safety Committee every 3 years.

## 20. References

### References:

Code:

Health and Safety	
Information Governance	
General Data Protection Regulations 2018	

## 21. Background

### 21.1 Equality requirements

There are no equality issues associated with this policy.

### 21.2 Financial risk assessment

There may be financial implications associated with this policy to ensure compliance with legislation.

### 21.3 Consultation Process

This policy will be consulted via Health and Safety Committee.

## 22. Contribution List

This key document has been circulated to the following individuals for consultation;

Designation
Fiona Dwyer – Local Security Management Specialist
Matthew Thurland – Health Records Manager
Emma King - Deputy Director of Estates and Facilities (Soft FM)
Julie Noble – Head of Health and Safety and Fire Manager
Annie Osborne-Wylde – Information Governance Manager
Andrew Williams - Portering & Transport Co-Ordinator
Stuart Close – Site Services Manager
Scott Dickinson - Director of Estates and Facilities

This key document has been circulated to the chair(s) of the following committee's / groups for comments;

Committee
Health and Safety
Security Meeting
Information Governance Committee

## 23 Approval Process

Health and Safety Committee and Information Governance.

**Appendix 1: OPERATIONAL PROCEDURES FOR THE CONTROL AND USE OF CCTV**

In accordance with the Surveillance Policy all installation and use of CCTV must be conducted in accordance with:

- (a) the current Surveillance Policy;
- (b) the Information Commissioner's CCTV Code of Practice;
- (c) the following Standard Operational Procedures.

**Standards****Cameras**

- (a) cameras must always be operated so that they will only capture the images relevant to the purpose for which the particular scheme has been established and approved; if cameras are capturing areas outside the scheme, these areas must be masked out
- (b) cameras and recording equipment should be properly maintained in accordance with manufacturer's guidance to ensure that clear images are recorded and must be secure using password protection;
- (c) cameras should be protected from vandalism in order to ensure that they remain in good working order;
- (d) if a camera/equipment is damaged or faulty there should be a separate local procedure for:
  - (i) defining the individual(s) responsible for ensuring the camera is fixed,
  - (ii) ensuring the camera / equipment is fixed within a specific time period,
  - (iii) monitoring and overseeing the quality of the maintenance work;
- (e) Cameras should not ever be allowed to view any areas outside of the boundaries of Worcestershire Acute Hospitals NHS Trust properties without prior permission and involvement of the Data Protection Officer.

A detailed log of cameras and locations for Worcestershire Acute Hospitals NHS Trust is provided in each CCTV location of the Alexandra Hospital and Kidderminster Treatment Centre and Worcestershire Royal Hospital sites.

**Operators**

- (a) all operators of CCTV equipment should be trained in their responsibilities in accordance with Worcestershire Acute Hospitals NHS Trust's policy and this procedure;
- (b) all staff involved in the handling of the CCTV equipment, both directly employed and contracted, will be made aware of the sensitivity of handling CCTV images and recordings.

**Training**

- (a) Guidance in the requirements of the law on Data Protection and then General Data Protection Regulations, will be given to staff that are required to manage and work the CCTV systems;
- (b) They will be fully briefed and trained in respect of all functions, both operational and administrative relating to CCTV control operation; by Installer of system and through the SIA Operators course.

(c) Training by camera installers will also be provided as appropriate to authorised staff.

## Maintenance

- (a) a comprehensive maintenance log will be kept which records all adjustments / alterations / servicing / non-availability of all individual schemes;
- (b) any data storage on which images have been recorded will be replaced when it has become apparent that the quality of images has deteriorated;
- (c) if the system records location/time/date these will be periodically checked (at least weekly) for accuracy and adjusted accordingly. In the case of alterations due to 'British Summer Time' the system should, as a matter of course, must be checked for accuracy;
- (d) in the event that CCTV footage records an incident to be subject to further investigation, or is subject to a data subject access request, a copy of the data media in question should be preserved;
- (e) subject to the above, data will not be retained on the DVR/NVR Server for longer than 31 days from the date of recording;
- (f) a review must be undertaken at least annually to continually assess against the stated purpose of the identified scheme, the result of which should be made publicly available should they be requested.

## Access

- (a) all staff should be made aware of the procedures for granting subject access requests to recorded images or the viewing capabilities of CCTV and Body Warn Camera schemes (as per the Surveillance Policy). All such requests (in the first instance) should be notified promptly to the Data Protection Officer in writing; including all Police/Public and staff requests
- (b) Criteria for the viewing of data material by non-security related personnel.  
At the discretion of the responsible officer individuals may be allowed to view data material:
  - (i) if they are investigating an untoward incident,
  - (ii) in the case of a missing patient,
  - (iii) to identify persons relating to an incident.

Areas which would normally result in permission being refused include:

- (i) where the person wishing to view has no legitimate interest or purpose for doing so (for example, they have no connection with the incident or have no management role relating to an incident),
- (ii) where the performance of a member of staff not relating to crime, fraud or the investigation of untoward incidents is involved;
- (c) access to the recorded images must be restricted to a manager or designated member of staff. All accessing or viewing of recorded images should only occur within a restricted area and other employees should not be allowed to have access to that area or the images when a viewing is taking place;
- (d) if images are to be specifically retained for evidential purposes, i.e., following an incident, break-in etc, then these images must be saved;



Requests to access recordings by third parties may be granted in certain circumstances and will arise in a number of ways, including:

- (i) requests for a review of recording, in order to trace incidents that have been reported to the Police,
- (ii) immediate action relating to live incidents, e.g. immediate pursuit.
- (iii) individual police officer seeking to review images
- (iv) Local Security Management Specialist seeking to review images

Any such requests must always be justified under relevant legislation and guidance and in accordance with the Data Protection Act 2018 & the General Data Protection Regulations 2018. The justification for any disclosure must be recorded in the 'Access Log' and all appropriate documentation used.

If data collection materials are to be handed over to the Police or to Solicitors, in the process of their enquiries, the name and station of that police officer together with a crime incident or reference number and signature must be acquired and retained prior to release (Appendix 4). The name, address and telephone number of the Counter Fraud Specialist must also be acquired. If copies are required of the footage on data capture materials, two copies must be made. One copy to be retained by Worcestershire Acute Hospitals NHS Trust and the other given to the Police / Solicitors. The event will be noted in the log and the details and signature of the recipient obtained. In the event of the data capture material being required for evidence, it will be retained for a period recommended by those involved with the case; all evidence provided by Worcestershire Acute Hospitals NHS Trust must be saved securely on a hard drive or the cloud.

- (e) monitors displaying images from areas in which individuals would have an expectation of privacy must not be viewed by anyone other than an authorised employee of the user of the equipment;
- (f) when disclosing surveillance images of individuals, particularly when responding to subject access requests, the Trust must consider whether the identifying features of any of the other individuals in the image need to be obscured. In most cases the privacy intrusion to third party individuals will be minimal and obscuring images will not be required. However, consideration should be given to the nature and context of the footage and decisions should be made on a case-by-case basis by the Data Protection Officer.

## **Digital CCTV**

- (a) all digital CCTV systems installed onto Worcestershire Acute Hospitals NHS Trust premises must have the storage capacity to hold a minimum of 31-day footage. In certain circumstances it may be considered appropriate to retain data for a longer period, a full risk assessment must be taken before making a decision for a longer retention period re: the Storage/Memory capability of the DVR/NVR/Server
- (b) where digital CCTV is installed all sites must have local access to a DVD recorder/USB ability that is compatible with the system in use;
- (c) all sites must hold a stock of blank, write once DVDs and Encrypted USB's;
- (d) where there is access to CCTV footage via the network, controls should be put into place so only authorised users are able to use it be password protecting the access to the DVR/Server/ Web access point.

**Appendix 2 : INSTALLATION CHECKLIST**

<ul style="list-style-type: none"> <li>The Chief Executive or persons with delegated responsibility has approved the installation/alteration to the citation of the camera.</li> </ul>	•	•
<ul style="list-style-type: none"> <li>The purpose for the installation/adjustments have been clearly documented.</li> </ul>	•	•
<ul style="list-style-type: none"> <li>The organisation that is legally responsible for the CCTV scheme has been established.</li> </ul>	•	•
<ul style="list-style-type: none"> <li>Equipment is situated so it can only monitor the intended area of coverage as defined in scheme proposal.</li> </ul>	•	•
<ul style="list-style-type: none"> <li>The cameras are not positioned anywhere that would be considered private eg office, toilet.</li> </ul>	•	•
<ul style="list-style-type: none"> <li>Signs are in place showing that CCTV systems are in operations and that the owner of the systems name and contact details are clearly displayed.</li> </ul>	•	•
<ul style="list-style-type: none"> <li>Cameras have been positioned to avoid capturing the images of persons not visiting the premises.</li> </ul>	•	•
<ul style="list-style-type: none"> <li>The recorded images are stored securely with strictly controlled access procedures in place.</li> </ul>	•	•
<ul style="list-style-type: none"> <li>The recorded images are stored for no longer than 31 days.</li> </ul>	•	•
<ul style="list-style-type: none"> <li>A procedure is in place for operational equipment to be checked regularly to ensure it is in working order.</li> </ul>	•	•
<ul style="list-style-type: none"> <li>Images will only be made available to law enforcement agencies involved in the prevention and detection of crime, appropriate procedures in place.</li> </ul>	•	•
<ul style="list-style-type: none"> <li>A procedure in place for dealing with individuals requesting access to CCTV footage (other than law enforcement agencies).</li> </ul>	•	•
<ul style="list-style-type: none"> <li>An appropriate confidential disposal procedure in place.</li> </ul>	•	•
<ul style="list-style-type: none"> <li>CCTV installer to carry out an Impact Assessment</li> </ul>	•	•

## Appendix 3:

## Form 1 – REQUEST TO CONFIRM CCTV/BWC IMAGES EXIST AND ARE STORED

(To be used for all requests, with the exception of police /solicitor requests when form 2 should be used)

All requests must be made on this proforma.

No CCTV images should be shown to anyone without approved permission.

Details of Incident (brief description of incident)

Date of Request	
Date of Incident	
Time of Incident	
Location	
Reason for Viewing Images	
Description of events e.g what happened	
Full description of subject so they can be identified from the captured images e.g. glasses, hair colour etc	

**Requestors Details**

Name	
Staff or Public	
Contact Details	Email: _____ Telephone: _____
Location / Site	
Reason for Request	

**Details of Security Officer / Porter Viewing Images**

Name	
Signature	
Position	
Site	
Date	
Images Available	YES / NO
Images Saved	YES/NO
Has Requester been contacted	YES / NO

**ONLY** In event of footage needing to be seen **immediately e.g. crime being committed or immediate danger to public / patient safety or threat to life.**

In these circumstances **In and Out of Hours** – the Clinical Site Manager / Matron should be contacted via switchboard who can authorise viewing. Datix should also be completed.

For routine requests the form should be sent to [healthrecords@nhs.net](mailto:healthrecords@nhs.net) for authorisation by the [Data Protection Officer](#).

**NO VIEWING CAN OCCUR WITHOUT AUTHORISATION.**

# Trust Policy



Worcestershire  
Acute Hospitals

NHS Trust

<b>Denied / Authorised by: Print Name</b>		<b>Signature:</b>	
<b>Time:</b>	<b>Date:</b>		
<b>Reason for Approval / Denial</b>			

**Appendix 4: EXTERNAL CCTV REQUEST FORM (POLICE/ SOLICITOR)**

**Request to external organisation for the disclosure of personal data to the police**  
 Under Schedule 2 Part 1 Paragraph 2 of the Data Protection Act 2018 and GDPR Article 6(1)(d) & 9(2)(c)

This request for information does not include a request for any Communications Data, and you should not send Communications Data in response unless it is inextricably linked to other data. If it is inextricably linked, please ensure this is recorded in your reply.

<b>To:</b>	
Position:	
Organisation:	
Address:	

I am making enquiries which are concerned with (mark as appropriate):

The prevention or detection of crime

The prosecution or apprehension of offenders

Protecting the vital interests of a person

- I confirm that the personal data requested below is needed for the purposes indicated above and a failure to provide that information will be likely to prejudice those matters.
- I confirm that the individual(s) whose personal data is sought should not be informed of this request as to do so would be likely to prejudice the matters described above.

**Information required:**

--

**Why the information is necessary for the purpose:**

Beware of disclosing information which is excessive or may pose operational risks to your investigation, but also be aware that failure to explain the necessity clearly may delay or prevent disclosure.

--

**Police reference:**

--

**From:**

Rank/number/name:	
Station:	
Date/time:	
Tel no(s):	
Email:	
Signature:	

Counter signature: **	
Rank/number/name:	

### Undertaking of lawful use of data disclosed to the police service:

Information disclosed to the police service is protected against unlawful reuse by the second data protection principle<sup>1</sup>, which prohibits data collected for one purpose being reused for another. If data disclosed to the police service is needed for another purpose, it will be reused only if the new purpose is lawful or a lawful exemption applies, and only data necessary and proportionate to that new purpose will be used.

Therefore, the police service undertakes to ensure that any use or reuse of the data disclosed is lawful, compliant with the data protection principles and processed using appropriate safeguards to the rights and freedoms of the data subject.

Please be aware that we cannot comply with a request to limit use of data which is overridden by a statutory or common law duty or obligation. However, the reuse will be subject to the safeguards described above.

We respectfully request that the same or equivalent measures are observed in your handling of this request for information.

### Additional information you may wish to provide to the police service:

In order to help us safeguard against risk to the data subjects, your organisation, and the police service, please provide with your disclosure any additional information you believe necessary to best handle the data you choose to disclose. This may include, but is not limited to:

- Risks we could not reasonably anticipate
- Any expectation to consult with your organisation should reuse be necessary
- Legally enforceable restrictions on reuse of the data

### Explanatory Note

This form is used by the police when making a formal request to other organisations for personal data where disclosure is necessary for the purposes of the prevention or detection of crime or the apprehension or prosecution of offenders. It places no compulsion on the recipient to disclose the information, but should provide necessary reassurance that a disclosure for these purposes is appropriate and in compliance with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

**Crime and Taxation** - The GDPR regulates the processing of personal data where it is done so for non-Law Enforcement purposes. Article 23 of the GDPR permitted the UK Parliament to create, via legislation, exemptions from particular elements within the GDPR which would otherwise compromise the public interest. The Data Protection Act 2018 sets out exemptions from the GDPR which apply in some circumstances. They mean that some of the data protection principles and subject rights within the GDPR do not apply at all or are restricted when personal data is used or disclosed for particular purposes.

The most relevant exemption for Law Enforcement is that within the Data Protection Act 2018 at Schedule 2 Part 1 Paragraph 2 (Crime & taxation: general). This applies where personal data is disclosed by an organisation subject to the GDPR to the police for the purposes of *the prevention or detection of crime or the apprehension or prosecution of offenders*.

It restricts the application of the GDPR data protection principles and subject rights (as listed in the Data Protection Act 2018 at Schedule 2 Part 1 Paragraph 1) to the extent that the application of those provisions would be likely to prejudice *the prevention or detection of crime or the apprehension or prosecution of offenders*.

In effect the exemption means that an organisation can provide personal data to the police where necessary for the prevention or detection of crime or the apprehension or prosecution of offenders without fear of breaching the GDPR or Data Protection Act 2018.

<sup>1</sup> General Data Protection Regulation Article 5(1)(b) and Data Protection Act 2018 Part 3 Section 36

Organisations already processing data for the prevention and detection of crime may wish to consider compatibility with their conditions for processing instead of using this exemption. For example, Schedule 1 Part 2 Paragraph 10 provides the condition for processing (including disclosure) for purposes compatible with this request.

**Vital Interests** – To protect life or prevent an immediate and credible risk to life, GDPR Article 6(1)(d) provides a lawful basis for organisations to disclose personal data to the police where the disclosure *is necessary in order to protect the vital interests of the data subject or of another natural person*. Article 9(2)(c) provides for processing of special category data to the same ends, where the data subject is legally or physically incapable of consent.

Further guidance on the use of this form may be obtained from your Data Protection Officer.

---

### Completion Guidance

Police officers or staff completing this form should type and tab between the fields on the form. The information required field should provide the recipient with sufficient information to allow them to locate the information sought. Where a signature and/or counter signature are required the form will need to be printed off and signed manually. Some organisations may require a counter signature to be added to the form. Normally this should be the supervisor or line manager of the person completing the form, but may be a higher rank if reasonably required by the recipient.



## Supporting Document - Equality Impact Assessment Tool



### Herefordshire & Worcestershire STP - Equality Impact Assessment (EIA) Form Please read EIA guidelines when completing this form

#### Section 1 - Name of Organisation (please tick)

Herefordshire & Worcestershire STP		Herefordshire Council		Herefordshire CCG	
Worcestershire Acute Hospitals NHS Trust	x	Worcestershire County Council		Worcestershire CCGs	
Worcestershire Health and Care NHS Trust		Wye Valley NHS Trust		Other (please state)	

<b>Name of Lead for Activity</b>	<b>Julie Noble</b>
----------------------------------	--------------------

<b>Details of individuals completing this assessment</b>	<b>Name</b>	<b>Job title</b>	<b>e-mail contact</b>
	Fiona Dwyer	Local Security Management Specialist	<a href="mailto:Fiona.dwyer@nhs.net">Fiona.dwyer@nhs.net</a>
<b>Date assessment completed</b>	<b>25<sup>th</sup> September 2024</b>		

#### Section 2

Activity being assessed (e.g. policy/procedure, document, service redesign, policy, strategy etc.)	<b>Title: Policy</b>			
What is the aim, purpose and/or intended outcomes of this Activity?	Ensure compliance			
Who will be affected by the development & implementation of this activity?	x	Service User	x	Staff
	x	Patient	x	Communities
	<input type="checkbox"/>	Carers	<input type="checkbox"/>	Other _____
	x	Visitors	<input type="checkbox"/>	
Is this:	<input type="checkbox"/> Review of an existing activity <input checked="" type="checkbox"/> New activity <input type="checkbox"/> Planning to withdraw or reduce a service, activity or presence?			
What information and evidence have you reviewed to help				

inform this assessment? (Please name sources, eg demographic information for patients / services / staff groups affected, complaints etc.	
Summary of engagement or consultation undertaken (e.g. who and how have you engaged with, or why do you believe this is not required)	
Summary of relevant findings	

### Section 3

Please consider the potential impact of this activity (during development & implementation) on each of the equality groups outlined below. **Please tick one or more impact box below for each Equality Group and explain your rationale.** Please note it is possible for the potential impact to be both positive and negative within the same equality group and this should be recorded. Remember to consider the impact on e.g. staff, public, patients, carers etc. in these equality groups.

Equality Group	Potential <u>positive</u> impact	Potential <u>neutral</u> impact	Potential <u>negative</u> impact	Please explain your reasons for any potential positive, neutral or negative impact identified
Age		X		
Disability		X		
Gender Reassignment		X		
Marriage & Civil Partnerships		X		
Pregnancy & Maternity		X		
Race including Traveling Communities		X		
Religion & Belief		X		
Sex		X		
Sexual Orientation		X		
Other Vulnerable and Disadvantaged Groups (e.g. carers; care leavers; homeless; Social/Economic deprivation, travelling communities etc.)		X		

Equality Group	Potential <u>positive</u> impact	Potential <u>neutral</u> impact	Potential <u>negative</u> impact	Please explain your reasons for any potential positive, neutral or negative impact identified
<b>Health Inequalities</b> (any preventable, unfair & unjust differences in health status between groups, populations or individuals that arise from the unequal distribution of social, environmental & economic conditions within societies)		X		

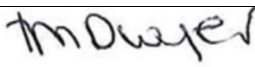
## Section 4

What actions will you take to mitigate any potential negative impacts?	Risk identified	Actions required to reduce / eliminate negative impact	Who will lead on the action?	Timeframe
<b>How will you monitor these actions?</b>	<b>Incidents</b>			
<b>When will you review this EIA?</b> (e.g in a service redesign, this EIA should be revisited regularly throughout the design & implementation)				

## Section 5 - Please read and agree to the following Equality Statement

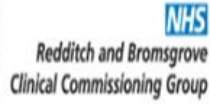
### 1. Equality Statement

- 1.1. All public bodies have a statutory duty under the Equality Act 2010 to set out arrangements to assess and consult on how their policies and functions impact on the 9 protected characteristics: Age; Disability; Gender Reassignment; Marriage & Civil Partnership; Pregnancy & Maternity; Race; Religion & Belief; Sex; Sexual Orientation
- 1.2. Our Organisations will challenge discrimination, promote equality, respect human rights, and aims to design and implement services, policies and measures that meet the diverse needs of our service, and population, ensuring that none are placed at a disadvantage over others.
- 1.3. All staff are expected to deliver services and provide services and care in a manner which respects the individuality of service users, patients, carer's etc, and as such treat them and members of the workforce respectfully, paying due regard to the 9 protected characteristics.

<b>Signature of person completing EIA</b>	
<b>Date signed</b>	23/10/2024

# Trust Policy

<b>Comments:</b>	
<b>Signature of person the Leader Person for this activity</b>	Julie Noble
<b>Date signed</b>	23/10/2024
<b>Comments:</b>	



## Supporting Document 2 – Financial Impact Assessment

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

	Title of document:	Yes/No
1.	Does the implementation of this document require any additional Capital resources	no
2.	Does the implementation of this document require additional revenue	no
3.	Does the implementation of this document require additional manpower	no
4.	Does the implementation of this document release any manpower costs through a change in practice	no
5.	Are there additional staff training costs associated with implementing this document which cannot be delivered through current training programmes or allocated training times for staff	no
	Other comments:	n/a

If the response to any of the above is yes, please complete a business case and which is signed by your Finance Manager and Directorate Manager for consideration by the Accountable Director before progressing to the relevant committee for approval