Barnsley Hospital NHS
NHS Foundation Trust

Trust Surveillance Camera Policy & Procedures

(CCTV, Security & Clinical Body Worn Video)

February 2023

Document Control

Author / Contact	Lead Healthcare Security Manager Head of Business Security. Ext.1386	
Equality Impact Assessment	Yes Date 1st January 2023	
Version	v.7	
Status	Policy Revision: 1. Revision of objectives 2. Key responsibilities 3. Use of BWV by clinical & reception staff 4. Covert use of BWV considered illegal 5. Responsibilities for Trust surveillance systems	
Publication date	February 2023	
Review date	February 2026	
Approval recommended by	Health & Safety Group	Date: February 2023
Approved by	Quality & Governance Committee	Date February 2023
Distribution	Barnsley Hospital NHS Trust-intranet Please note that the Intranet version of this document is the only version that is maintained. Any printed copies must therefore be viewed as “uncontrolled” and as such, may not necessarily contain the latest updates and amendments	

Table of Contents

1 Introduction

The purpose of this Policy is to regulate the management, operation, and use of the surveillance camera CCTV & Body Worn Video (BWV) systems monitored and deployed security and clinical staff on duty at Barnsley Hospital NHS Foundation Trust premises. Barnsley Hospital NHS Foundation Trust is the responsible owner of both systems on the site and conforms to the Data Protection Act, GDPR, Surveillance Camera Commissioners and Home Office Camera Codes of Practice

The systems comprise of a variety of fixed camera types (static, PTZ, IP and hemispheric) and mobile (BWV) cameras carried by members of the Trust security team (both Trust and Contractor) alongside clinical and reception staff in identified locations. The majority of fixed CCTV cameras are monitored within the Security Control Room and access to view images is limited to SIA licensed staff only (Security Team & Business Security Unit) (see Appendix 1 for guidance only). The Business Security Unit is not responsible for CCTV systems operated by other organisations on site or the assets deployed within the material management area.

This policy also includes the use of unmanned aerial vehicles (UAVs or drones) which can be deployed for safety, photographic, video and survey tasks but could, if required, be used for patient and staff safety, security management or major incident responses. Their use is strictly controlled by Civil Aviation Authority (CAA) permissions to fly which includes operating distances and heights. For the purposes of this policy the UAV is not classed as a surveillance asset but is included as it carries a high resolution camera as part of its payload. It would only be deployed for surveillance purposes in the case of an emergency or serious incident.

This Policy adheres to the Data Protection Act 2018, EU General Data Protection Regulation and the above mentioned Surveillance Commissioner Codes of Practice, CAA procedures and is subject of annual and dynamic review

Ownership of the CCTV systems is listed separately.

2 Objectives

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

- To provide an overall protection for staff, patients and visitors
- To protect Trust premises and Trust assets
- To increase personal safety and reduce the fear of incidents
- To reduce occurrences of violence and aggression to staff members
- To provide supporting data relating to internal and external inquiries
- To support in reducing and detecting reportable incidents
- To assist in identifying, apprehending and prosecuting offenders
- To provide a deterrent effect and reduce criminal or anti-social activity
- To assist in the traffic management and car parking schemes

3 Scope of the Policy

. This policy applies to all persons employed by Barnsley Hospital NHS Foundation Trust, Barnsley Facilities Services (BFS), other contractors and any other groups, who access any hospital site, i.e.: visitors, patients, private/public contractors.

4 Policy

All associated information, documents, and recordings obtained by surveillance cameras are held and used in accordance with the Data Protection Act 2018 and GDPR. They are available on the Trust public internet web site.
Images obtained from any surveillance camera recordings will not be used for any commercial purpose. Recordings will only be released to the media for use in investigation of a specific crime and with the written consent of the police. Recordings will not be released to the media for purposes of entertainment.

Archived camera images will not be kept for longer than is necessary for the purposes of legal process or for evidential purposes. Once there is no longer a need to retain the images, they will be deleted from the system. All data will be retained in accordance with NHS and Trust retention schedules.

All associated information, documents, and recordings obtained and used by surveillance assets are protected by the Data Protection Act 2018.

Cameras monitor activities on all Trust premises, car parks and other public areas to identify criminal or unauthorised activity whether occurring, anticipated, or perceived in order to enhance the safety and well-being of staff, patients, and visitors. All security officers have explicitly been made aware of this requirement and acknowledged their understanding.

Except when specifically authorised by the police, HMRC or security services using specific Directed Surveillance as stipulated in the Regulation of Investigatory Powers Act 2000 (RIPA), staff must not direct cameras at an individual, their property, or a specific group of individuals. (See Trust procedures for directed surveillance).

The planning and design of the Trust surveillance camera systems has endeavoured to ensure maximum effectiveness and efficiency but cannot guarantee to cover or detect every incident occurring within the areas covered. This will be reviewed annually.

Warning signs, as required by the Code of Practice of the Information and Surveillance Commissioners are displayed in all public areas covered by the hospital surveillance cameras.

4.1 Operation of the systems

The Trust surveillance camera systems are strategically administered and managed by the Business Security Unit, in accordance with the principles and objectives expressed in the Data Protection Act 2018, GDPR, Home Office Surveillance Code of Practice, CAA guidance and the Surveillance Commissioner's Codes of Practice.

The day-to-day management of surveillance cameras located at all hospital sites will be the responsibility of the uniform security team. Surveillence systems in other areas are to be managed by the department/organisation/business in which the systems are located and the Business Security Unit takes no responsibility for these systems even if located within the hospital surveillance camera footprint.

The Control Room will only be staffed by authorised and SIA licensed security personnel.

The CCTV system will be operated 24 hours a day, 365/6 days a year.

The BWV cameras will be activated by the individual staff member when required to record an incident or offence. Their activation will be logged and if practical subject(s)

informed of their use.

The UAV will only be operated by a NQE qualified pilot, registered with the CAA with a current SIA CCTV licence and the appropriate insurance strictly as an aerial safety and response asset.

4.2 Security Control Room

The Duty Security Supervisor/Control room operator will check and confirm the efficiency of the system at each shift handover and ensure that equipment is in full working order with cameras correctly positioned.

Access to the CCTV Control Room will be restricted to authorised personnel only.

Contractors and other visitors requesting entry to the Control Room will be subject to specific arrangements as outlined below.

Control Room Operators must confirm the identity of any non-security personnel requesting entry to the Security Control Room, and the reason for entry, and if not clearly identified, access will be refused.

To ensure that the operation of camera systems is managed with the minimum of disruption, casual and non-essential visits by non-security personnel will not be permitted. All visitors must obtain permission to enter from the Site Security Manager/Supervisor or Business Security Unit, sign the log and must be accompanied throughout the visit.

Any visit may be immediately curtailed by the Security Manager/Supervisor if operational requirements deem this to be necessary (i.e. an incident occurring).

In the event of an out of hour's equipment failure requiring access to the CCTV Control Room, the security team must confirm the identity and purpose of contractors before allowing entry.

A visitor's book will be maintained within the Control Room. Full details of visitors including time/date of entry and exit, and purpose of visit will be logged.

At least one Security Officer should remain in the Control Room at all times.

4.3 Archiving procedure and release of data

In order to maintain and preserve the integrity of recordings for use in any future proceedings, the following procedures for use and retention must be strictly adhered to:

- The primary method of video capture transfer for all requests should be via the cloud server. In this case the file address and password must be forwarded under separate cover to recognised and verified individuals only.
- When unable to transfer data captures via the cloud server any data medium (i.e. DVD, stick or remote drive) & BWV data must be identified by a Name, Date, Time, Camera Location or Individual and recording equipment used.
- The data transfer medium must be sealed, signed by the controller, dated, witnessed and stored in a designated secure unit. A log will be maintained in the Control Room detailing the release of recorded media to the police or other authorised applicants, and a register will be available for this purpose.
- Viewing of data images within the Control Room by the Police must be recorded in writing and entered in the log book. Requests by the police to view images can only be actioned under section 29 of the Data Protection Act 1998 and the

Police and Criminal Evidence Act (PACE 1984). A written request will be required in all cases.

- If the data transfer medium, BWV or UAV data is required as evidence, a copy may be released to the Police. The medium will only be released to the Police on the clear understanding that the media remains the property of the Trust.
- The Police may require the Trust to retain stored data media for possible future evidence. Such media will be indexed and securely stored until they are required to be produced as evidence by the criminal justice system.
- Applications received from external agencies (e.g. solicitors or insurance companies) to view archives/recordings must in the first instance be made to the Head of Business Security. If appropriate and after liaison with the Trust Solicitor (or in their absence the Security Management Director). Camera data will only be released where satisfactory documentary evidence is produced confirming legal proceedings, a subject access request, or in response to a Court Order.
- Camera data can be viewed or released to Trust/BFS managers for the purpose of internal enquiries. This release must be authorised by a senior HR manager and a full log and audit trail established.

Still photographs of surveillance camera images should not be taken as a matter of routine. The taking of each photograph must be capable of justification (prevention or detection of crime), and only done so with permission from the immediate person in charge i.e. line manager. The retention of any such image(s) must be approved by the Business Security Unit.

All still photographs of camera images shall remain the property of Barnsley Hospital NHS Foundation Trust and shall be indexed in sequence. A record is to be kept of the reason for production of the photograph, date, and time, the particulars of production of a live photograph, and information identifying the security staff member responsible for producing the photograph. These images will not contain any security or verification watermark.

Still photographs of camera images released to the Police shall be dealt with by the police as an exhibit and shall at no time be used for anything other than the purpose specified and identified when released to the police.

Still photographs of camera images shall not be kept for longer than is necessary for the purpose of Police evidence. Once there is no need to keep the footage or stills, they must be destroyed as confidential waste or deleted from the system.

Any UAV footage or still photographs will be administered to the same standard and within the same procedures as CCTV or BWV information.

4.4 Guiding Principles

The Home Office Surveillance Camera Code of Practice 2013 outlines 12 guiding principles to be adopted by CCTV and BWV system operators. Although NHS hospitals are not included as ‘Relevant Authorities’, Barnsley Hospital NHS Foundation Trust will endeavour to uphold these principles at all times. They are included in Appendix A. The Trust continues to be accredited by the Surveillance Camera Commissioner for the legal, responsible and proportionate use of all its camera assets (CCTV and BWV). This accreditation is now subject of annual SSAIB audit.

4.5 Breaches of this policy

Any breach of the CCTV policy should be reported using the Trust's incident reporting system (Datix). It will be initially investigated by the Head of Business Security or other Accountable Officer, and may result in disciplinary action.

Investigations following breach of the Surveillance Camera Policy will result in recommendations and an action plan to remedy the breach where appropriate.

4.6 Complaints

Any complaints concerning the Trust's CCTV, BWV and UAV systems should be addressed to the Trust Complaints Manager. The complaints procedure can also be accessed visa the Trust website

4.7 Access by a data subject

The Data Protection Act and GDPR provides Data Subjects (individuals to whom "personal data" relates) with a right to access data concerning them, including data obtained by CCTV & BWV or in exceptional cases of use, a UAV. There may be occasions when data cannot be released and the reason(s) for refusal will be provided to the person requesting.

Requests for Data Subject Access should be made on the appropriate application form available from the Trust Head of Information Governance.

4.8 Centre for the Protection of National Infrastructure (CPNI)

The CPNI is the national technical authority in respect of protective security and the government authority for providing protective security advice to the UK national infrastructure. Health is a named sector within the UK national infrastructure and the role of CPNI is to protect security by helping reduce the vulnerability to all threats including terrorism. A number of key security strategies including surveillance measures adopted by the Trust are based on CPNI advice and guidance.

5 Roles & Responsibilities

Trust Board
The Trust Board has overall responsibility for ensuring that the Trust meets its statutory obligations that effective security arrangements are in place and are periodically reviewed.

Security Management Director (SMD)
The Chief Delivery Officer as strategic Trust lead for security management has delegated responsibility for security management. The SMD's remit also includes emphasising the security management needs of the Trust to the Board to ensure that responsibilities are taken seriously at the highest level. This officer will ensure the implementation of recommendations from previous and future security audits and for developing and reviewing the organisation-wide action planning following receipt of advice provided by the Business Security Unit.

Head of Business Security
The Head of Business Security as the Trust strategic Healthcare Security Manager is the designated lead for managing security, convergence and EPRR issues in line with other Trust policies and procedures and the uniform security team's Assignment Instructions (AI's). They are also responsible for providing specialist expertise in all anti-crime aspects and for working with the Trust to provide an environment that is safe and secure for all. The Business Security Unit staff manage the piloting of UAVs and are CAA qualified and operator registered.

Business Security Specialist
This specialist security manager as tactical lead will receive reports on any offences in connection with crime or misconduct on Trust premises and initially lead with any investigation that is required as a result of alleged unlawful, anti-social or criminal activities whilst ensuring the involvement of the police when necessary. In addition and in collaboration with the BFS Projects Officers, Counter-Terrorist Security Advisor (CTSA) and Environment Agency provide advice on the planning and commissioning elements of any future hospital development. This advice should be sought at the earliest possible stage to ensure the external and internal assets of the Trust are adequately safeguarded.

The Uniform Security Team Site Manager
The uniform security team site manager has responsibility for the operational and day-to-day implementation of this policy with the uniformed officers. This manager will ensure the initial safeguarding of all data (video & audio) obtained via the Trust surveillance systems. This will include retention and any onward transmission for evidential purposes.

Trust Managers and Supervisors
Managers are responsible for:

- The development and adaptation of Trust Security procedures to ensure that they are relevant to specific Directorate / Departmental needs.
- Overall supervision of the day to day security measures within their Service Unit, Ward or Department.
- Ensuring that any incident of crime or suspected crime is reported to the Security Team or Business Security Unit and/or local police. A Datix report is submitted by the member of staff concerned.
- Ensuring that appropriate education and training is provided for all staff.
- Staff are aware of the Trust and BFS privacy notices and the use of overt surveillance on site.

All Staff
All members of staff have a responsibility to ensure that they comply with relevant security policies and procedures (see Trust Policy Warehouse on the Intranet). It is also essential that all security incidents involving or observed by staff are reported in accordance with the Trust's incident reporting procedure (Datix) and they are aware of published privacy notices.

6 Associated Documentation and References.

Internal
Violence & Aggression Policy
Lone Worker Policy
Locker Policy
Security Policy
I/D Card Policy
Unacceptable Behaviour Procedures.
Security Department Assignment Instructions (AI's)
BFS UAV Operations Manual
Security Staff Toolbox Training
Patient Property Policy
Suspicious Packages & Bomb Hoax Procedures
Baby/Child Abduction Policy
Access Control Procedures
VIP Visitors Policy

External

Home Office – *Surveillance Camera Code of Conduct*
Home Office – *Surveillance and counter-terrorism*
Information Commissioners Office - *In the picture: A data protection code of practice for surveillance cameras and personal information*
Information Commissioners Office – *Conducting privacy impact assessments code of practice*
Information Commissioners Office – Privacy notices code of practice
Joint Commissioners – *Surveillance Road Map. A shared approach to the regulation of surveillance in the United Kingdom*
Ann Cavoukian, PhD – *Privacy by Design. The 7 Foundational Principles*
Information Commissioners Office – *Big data and data protection*
Information Commissioners Office – *The Guide to Data Protection*
Information Commissioners Office – *Data sharing code of practice*
Information Commissioners Office – *Subject access code of practice*
Information Commissioners Office – *The Guide to the Freedom of Information*
Surveillance Camera Commissioner – *Code of practice. A guide to the 12 principles*
Home Office Scientific Development Branch – *Is your CCTV system fit for purpose?*
Surveillance Camera Commissioner – *Self Assessment Tools for CCTV, BWV and UAVs*
Centre for the Protection of National Infrastructure (CPNI) – *Guide to Producing Operational Requirements for Security Measures*
Centre for the Protection of National Infrastructure (CPNI) – *Embedding Security Behaviours: using the 5Es*
Centre for the Protection of National Infrastructure (CPNI) – *Marauding Terrorist Attacks, Making your organisation ready.*
Centre for the Protection of National Infrastructure (CPNI) – *Passport to Good Security for Senior Executives*
Centre for the Protection of National Infrastructure (CPNI) – *Protective Security Management Systems (PSeMS). Guidance, Checklist and Case Studies.*
Centre for the Protection of National Infrastructure (CPNI) – *CCTV within the workplace. A guidance document.*
Centre for the Protection of National Infrastructure (CPNI) – *CCTV within the perimeter of a site. A guidance document*
Centre for the Protection of National Infrastructure (CPNI) – *Human Factors in CCTV control rooms: A best practice guide*
Centre for the Protection of National Infrastructure (CPNI) – *Storage of Recorded CCTV Images.*
CAP 722 – *Civil Aviation Publication 722 - Unmanned Aircraft System Operations in UK Airspace*
NACOSS Code of Practice NACP 20 – *Code of Practice for CCTV Systems.*
BS EN 50132 Series of Standards – *European Standards for CCTV Systems*
NSI Green Paper NAGR 16 – *Proposals for Second Edition of NACP 20*
Home Office – *UK Police Requirements for Digital CCTV Systems*
Data Protection, Information Commissioner's Office – *CCTV code of practice*

7 Training & Resources.

Surveillance camera operators will receive bespoke local training on using the systems. This will be refreshed annually and officers will maintain a CPD portfolio.

Operators of Trust surveillance and public open space cameras (CCTV & BWV) will hold a valid SIA CCTV licence.

UAV pilots will be NQE qualified and operate within current CAA pilot and operator regulations

A mandatory induction security awareness programme and information can be accessed via the Trust Intranet for all staff.

Let Us Know (LUK) confidential reporting line (1111)

General security awareness and crime reduction advice is available on the BFS Business Security Unit e-learning programme that is assessed and also accesses on the Trust induction programme

'Not on My Watch' and 'It's OK to Say' videos accessible by staff on the Trust Intranet.

Conflict Resolution and Customer Care training are available based on training needs.

The BFS Business Security Unit will provide bespoke security management training to all Trust departments and staff on request.

The 'Hospital Eyes' resource on the Trust internet site can be access by staff and members of the public and fully explains the Trust surveillance resources.

8 Monitoring and Audit

The Trust Health & Safety Group and Quality & Governance Committee will monitor the implementation and compliance of this policy and surveillance procedures.

Where monitoring has identified deficiencies, recommendations and action plans will be developed and changes implemented accordingly. Progress on these will be reported to the Quality & Governance Committee.

The Business Security Unit will carry out an annual audit by sending questionnaires to a number staff on a random basis, to encompass a wide range of staff groups. A number of semi-structured interviews will also take place with staff members along with a full audit of requested data and information.

Any subsequent actions required following the audit will be developed by the Business Security Unit.

Progress on the implementation of corrective actions required will be reported to the Health & Safety Group regularly until all corrective actions are completed.

9 Equality and Diversity

The Trust is committed to an environment that promotes equality and embraces diversity in its performance as an employer and service provider. It will adhere to legal and performance requirements and will mainstream equality and diversity principles through its policies, procedures and processes. This policy should be implemented with due regard to this commitment.

To ensure that the implementation of this policy does not have an adverse impact in response to the requirements of the Equality Act 2010 this policy has been screened for relevance during the policy development process and a full equality impact analysis conducted where necessary prior to consultation. The Trust will take remedial action when necessary to address any unexpected or unwarranted disparities and monitor practice to ensure that this policy is fairly implemented.

This policy and procedure can be made available in alternative formats on request including large print, Braille, moon, audio, and different languages. To arrange this please refer to the Trust translation and interpretation policy in the first instance.

The Trust will endeavor to make reasonable adjustments to accommodate any employee/patient with particular equality and diversity requirements in implementing this policy and procedure. This may include accessibility of meeting/appointment

venues, providing translation, arranging an interpreter to attend appointments/meetings, extending policy timeframes to enable translation to be undertaken, or assistance with formulating any written statements.

9.1 Recording and Monitoring of Equality and Diversity

The Trust understands the business case for equality and diversity and will make sure that this is translated into practice. Accordingly, all policies and procedures will be monitored to ensure their effectiveness.

Monitoring information will be collated, analysed and published on an annual basis as part Equality Delivery System. The monitoring will cover the nine protected characteristics and will meet statutory duties under the Equality Act 2010. Where adverse impact is identified through the monitoring process the Trust will investigate and take corrective action to mitigate and prevent any negative impact.

The information collected for monitoring and reporting purposes will be treated as confidential and it will not be used for any other purpose.

Barnsley Hospital NHS
NHS Foundation Trust

Appendix 1

Equality Impact Assessment

Surveillance Camera Policy

January 2023

INITIAL ASSESSMENT STAGE 1 (part 1)

<table>
<tr><td>Department:</td><td colspan="2">Business Security Unit</td><td>Division:</td><td>Barnsley Facilities Services</td></tr>
<tr><td>Title of Person(s) completing this form:</td><td colspan="2">Head of Business Security</td><td>New or Existing Policy/Service</td><td>Existing</td></tr>
<tr><td>Title of Policy/Service/Strategy being assessed:</td><td colspan="2">Surveillance Camera Policy</td><td>Implementation Date:</td><td>Review – January 2023</td></tr>
<tr><td>What is the main purpose (aims/objectives) of this policy/service?</td><td colspan="4">To combine legislation and guidance establishing a policy & procedures for CCTV, Body Worn Video (BWV) and Unmanned Aerial Vehicle (Drone) use within the Trust and where required provide survey and safety data or evidence for further investigation.</td></tr>
<tr><td rowspan="5">Will patients, carers, the public or staff be affected by this service?
Please tick as appropriate.</td><td></td><td>Yes</td><td>No</td><td rowspan="5">If staff, how many individuals/which groups of staff are likely to be affected?
Safer working environments for Estates, Facilities and Estates staff.</td></tr>
<tr><td>Patients</td><td>X</td><td></td></tr>
<tr><td>Carers</td><td>X</td><td></td></tr>
<tr><td>Public</td><td>X</td><td></td></tr>
<tr><td>Staff</td><td>X</td><td></td></tr>
<tr><td rowspan="5">Have patients, carers, the public or staff been involved in the development of this service?
Please tick as appropriate.</td><td>Patients</td><td>X</td><td></td><td rowspan="5">If yes, who did you engage with? Please state below:
Business Security Unit
Estates Management - BFS
Facilities Management - BFS
Trust Uniform Security Team
G4S Secure Solutions
All Trust staff including volunteers, non-executive directors and governing body
Trust Members
Trust Service Users (Patients, Visitors, Relatives)
All staff side organisations
Barnsley Hospital Charity
Contracted staff and service providers
South Yorkshire Integrated Care Service (ICS)
NHS England
South Yorkshire Police
Yorkshire Ambulance Service
Barnsley Metropolitan Borough Council including elected members
Partners and Community Together (PACT – CSG)
Ward Alliance Group
Pogmoor Residents Association
Old Town Residents Association</td></tr>
<tr><td>Carers</td><td>X</td><td></td></tr>
<tr><td>Public</td><td>X</td><td></td></tr>
<tr><td>Staff</td><td>X</td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

What consultation method(s) did you use?	Each section of the policy will be circulated internally and externally to appropriate partners and stakeholders to form part of our overall security policy. Consultation is part of the induction and awareness programmes to staff and the policy is available via the Trust internet and intranet sites. All security procedures are outlined during exercises and during Projects SCaN and ACT awareness programmes.

Equality Impact Assessment Stage 1 PART 2

Based on the data you have obtained during the consultation what does this data tell you about each of the above protected characteristics? Are there any trends/inequalities?

Barnsley Hospital NHS Foundation Trust has a duty to protect, secure and promote the health of the community at all times. The Trust strategy focuses on reducing health inequalities and the treatment of all members of the community including the most vulnerable and ensuring they are safe during this care. The purpose of the sections of the policy is to ensure appropriate, legal and necessary use of surveillance assets. Also, to combine legislation and guidance establishing a policy & procedures for CCTV, Body Worn Video (BWV) and Unmanned Aerial Vehicle (UAV) use within the Trust and where required provide evidence for further investigation thereby minimising any impact on the health of the Barnsley community irrespective of Race, Disability or Gender etc.

No trends or inequalities identified

What other evidence have you considered? Such as a 'Process Map' of your service (assessment of patient's journey through service) / analysis of complaints/ analysis of patient satisfaction surveys and feedback from focus groups/consultations/national & local statistics and audits etc.

Security Officers and clinical staff will only deploy surveillance camera technology against the defined operational requirements and Security Policy and ensure that the use is proportionate, legitimate, necessary and justifiable. In addition, it will ensure that the use satisfies the requirement of addressing a pressing staff and patient safety need described in Trust policy, the assignment instructions and NHS Protect advice and guidance. At all stages it will comply with the Data Protection Act and other legislation. In the case of the Human Rights Act 1998, there will be adherence to the requirements of Article 6 (Right to a fair trial) and in respect of Article 8 (Right to respect for private and family life, home and correspondence) since this is a qualified right, information will only be captured and processed to achieve a legitimate aim as detailed earlier. UAV assets will only be deployed strictly for aerial safety and survey purposes.

Surveillance camera signage is well displayed throughout the Trust site with a contact number in case of enquiry. Any staff or security team use of BWV cameras will be announced to the subject and persons in the immediate area prior to activation. Surveillance notices are to be displayed at all entrances to the Trust. The policy has been reviewed by the relevant Trust governance committees prior to being enacted and has undergone a rigorous privacy impact assessment. The Trust and BFS privacy notices are available on the public internet and can be provided on request.

The Trust ‘Hospital Eyes’ website fully explains surveillance asset use and translations can be freely provided if required. The policy outlines the full and comprehensive consultation process.

Equality Impact Assessment Stage 1 PART 3

ACCESS TO SERVICES

What are your standard methods of communication with service users?

Please tick as appropriate.

Communication Methods	Yes	No
Face to Face Verbal Communication	X	
Telephone	X	
Printed Information (E.g. leaflets/posters)	X	
Written Correspondence	X	
E-mail	X	
Other (Please specify) – Training and dedicated webpage	X	

If you provide written correspondence is a statement included at the bottom of the letter acknowledging that other formats can be made available on request?

Please tick as appropriate.

Yes	No
	X

But this service is provided on the Trust web links where the Framework is located.

Are your staff aware how to access Interpreter and translation services?

Interpreter & Translation Services	Yes	No
Telephone Interpreters (Other Languages)	X	
Face to Face Interpreters (Other Languages)	X	
British Sign Language Interpreters	X	
Information/Letters translated into audio/braille/larger print/other languages?	X	

EQUALITY IMPACT ASSESSMENT – STAGE 1 (PART 4)

Protected Characteristic	Positive Impact	Negative Impact	Neutral Impact	Reason/comments for positive or negative Impact Why it could benefit or disadvantage any of the protected characteristics
Men	Low	Low	Low	Not applicable
Women	Low	Low	Low	Not applicable
Younger People (17 – 25) and Children	Low	Low	Low	Not applicable
Older people (60+)	Low	Low	Low	Not applicable
Race or Ethnicity	Low	Low	Low	Not applicable
Learning Disabilities	Low	Low	Low	Not applicable
Hearing impairment	Low	Low	Low	Not applicable
Visual impairment	Low	Low	Low	Not applicable
Physical Disability	Low	Low	Low	Not applicable
Mental Health Need	Low	Low	Low	Not applicable
Gay/Lesbian/Bi sexual	Low	Low	Low	Not applicable
Trans	Low	Low	Low	Not applicable
Faith Groups (please specify)	Low	Low	Low	Not applicable
Marriage & Civil Partnership	Low	Low	Low	Not applicable
Pregnancy & Maternity	Low	Low	Low	Not applicable
Carer Status	Low	Low	Low	Not applicable
Other Group (please specify)	Low	Low	Low	Not applicable

INITIAL ASSESSMENT (PART 5)

Have you identified any issues that you consider could have an adverse (negative) impact on people from the following protected groups?

IF 'NO IMPACT' IS IDENTIFIED Action: No further documentation is required.

IF 'HIGH YES IMPACT' IS IDENTIFIED Action: Full Equality Impact Assessment Stage 2 Form must be completed.

(a) Following completion of the Stage 1 Assessment, is Stage 2 (a Full Assessment)
necessary? NO

Assessment Completed By: Mike Lees **Date Completed:** 16th January 2023

Line Manager: Sue Bonelle Date 17th January 2023

Head of Department : Mike Lees Date 17th January 2023

When is the next review? Please note review should be immediately on any amendments to your policy/procedure/strategy/service.

1 Year	**2 year**	**3Year X**

Title of Service/Policy being assessed:	Surveillance Camera Policy
Assessment Date:	10th January 2023
Is the service/policy aimed at a specific group of users?	No

STAGE 2 – FULL ASSESSMENT & IMPROVEMENT PLAN

MUST be completed if any negative issues have been identified at stage 1

Protected Characteristic	What adverse (negative) impacts were identified in Stage 1 and which groups were affected?	What changes or actions do you recommend to improve the service to eradicate or minimise the negative impacts on the specific groups identified?	Lead	Time-scale
Men Younger People (17-25) and Children Older People (50+) Race or Ethnicity Learning Disability Hearing Impairment Visual Impairment Physical Disability Mental Health Need Gay/Lesbian/Bisexual Transgender Faith Groups (please specify) Marriage & Civil Partnership Pregnancy & Maternity Carers Other Group (please specify) Applies to ALL Groups				

How will actions and proposals be monitored to ensure their success? Which Committee will you report to? (i.e. Divisional DQEC / Governance Meeting).	
Who will be responsible for monitoring these actions?	

Glossary of Terms used within the Policy

Closed-circuit television (CCTV) is the use of video cameras to transmit a signal to a specific, limited set of monitors. It differs from broadcast television in that the signal is not openly transmitted. Body worn video (BWV) are small individual cameras securely clipped or harnessed to an individual officer usually on the shoulder or chest. They are clearly identifiable and are capable of being activated by the officer at the scene of an incident and the footage stored for evidential purposes. Footage not required can be deleted immediately. BWV video and audio data is captured and stored in an encrypted format.

PTZ Pan, Tilt and Zoom

BFS Barnsley Facilities Services

BVW Body Worn Video

CAA Civil Aviation Authority

CCTV Closed Circuit Television

CPNI Centre for the Protection of National Infrastructure

GDPR General Data Protection Regulation

IP Internet Protocol (High Definition Digital Camera)

ICO Information Commissioners Office

ICS Integrated Care Board (or System)

PIA Privacy Impact Assessment

NQE National Qualified Entity – CAA accredited UAV training provider

SMD Security Management Director

RIPA Regulation of Investigative Powers Act 2000

SIA Security Industry Authority

UAV Unmanned Aerial Vehicle or ‘Drone’.

SCCO Surveillance Camera Commissioners Office

SSAIB Security Systems and Alarms Inspection Board

CTSA Police Counter Terrorist Security Advisor

Appendix 3

Home Office Surveillance Camera Code of Practice 2013

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 must take into account its effects 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 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 the 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 system which compares against a reference database for matching purposes should be accurate and up to date.

Appendix 4

Body Worn Video (BWV) Procedures

1. Staff using BWV must have received a briefing on its use and deployment. A full information pack containing details of how to operate the cameras, security of the equipment, GDPR, Caldicott principles and advice sources will be made available to all users.

2. Police Officers and accredited officers of the Local Authority must inform the Trust security management team of any operation of their BWV systems on Trust premises.

3. The terms of reference and objectives of the Trust CCTV system apply to the Trust BWV equipment

4. Person's subject of any operation of the system (when practical) will be informed and warned clearly that the system is to be deployed and this will be repeated upon activation. Any other persons (including staff and patients) in the immediate vicinity will also be informed even though they may not be the active subjects of surveillance.

5. The use of BWV for continuous recording will not be authorised although officers are encouraged to activate the screen when responding to an incident. The covert use of CCTV and BWV is strictly prohibited and it must be noted, an illegal act.

6. If BWV is activated on ward areas by clinical staff and/or security officers the privacy and dignity of patients must be maintained whenever possible. If there is a breach of patient privacy the accompanying datix report must be endorsed accordingly. Cameras will be activated in every case of restraint or the physical handling of patients or other service users.

7. BWV footage will only be handled and stored in strict accordance with the Data Protection Act, ICO & SCCO guidance, Trust and NHS retention schedules. All data will be encrypted and access limited to authorised persons only.

8. All Trust security systems including CCTV, BWV and access control are subject of Privacy Impact Assessments and Privacy Notices.

9. Operational guidance has been issued to security staff and specialists in the use of BWV. This will be strictly adhered to and regularly monitored.

10. All activations of BWV cameras must be subject of an accompanying datix report.

BWV records not only the actions and speech of an individual but can also record an individuals' associations with others within the recording range, including friends, family members, bystanders, victims and suspects. This policy recognises that the recording of individuals must be necessary, proportionate and effective and only when all other alternatives have been considered. There must be an operational need for its deployment. It raises a significant risk to individual privacy, and the Trust must be committed to only using the system to the degree and manner that respects and protects staff, patient and general public's right to personal privacy and dignity.

Appendix 5

Responsibility for Surveillance Camera Systems on Site

Business Security Unit (BSU)

- All car parks including Helensburgh Close (Summer Lane)
- All other exterior cameras excluding car parking automatic number plate recognition (ANPR) assets.
- All BWV cameras (Reveal & Calla)
- All wards and internal departments including Outpatients Department

W.H. Smith Ltd

- Hospital Shop (Ground Floor near to Main Entrance)

ISS

- Beckett's Restaurant & Vending Area

Materials Management Department (BFS)

- Cameras (x6) in loading bay and materials management area.

Appendix 6

Policy Version Control

Version	Date	Comments	Author
4	1/7/16	Major revision from CCTV Policy	Mike Lees
5	1/2/18	Revision to include BFS & UAVs	Mike Lees
6	1/2/2020	Update – See Document Control	Mike Lees
7	1/2/2023	Revision – Clinical BWV included	Mike Lees

Review Process Prior to Ratification:

Name of Group/Department/Committee	Date
Chief Delivery Officer as SMD	January 2023
Managing Director – Barnsley Facilities Services	January 2023
Director of Communications	January 2023
Head of Information Governance - DPIAs	January 2023
Security Site Manager	January 2023
Surveillance Camera Group	December 2022
Surveillance Camera Commissioner & SSAIB	December 2022
Security Contract Group	January 2023
Public Consultation (Pogmoor Residents Assn)	January 2023
Public Consultation (Ward Alliance Group)	Januaey 2023
Public Consultation (Barnsley Chronicle)	January 2023
Public Consultation (BBC Radio Sheffield)	N/A
Emergency Department Focus Group	January 2023
South Yorkshire Police	December 2022
Barnsley Metropolitan Borough Council	December 2022
Staff Side Representatives	January 2023
Equality & Diversity Manager (HR)	January 2023
Policy Review Committee	February 2023
Health & Safety Group	February 2023
Quality & Governance Committee	February 2023

Trust Approved Documents (policies, clinical guidelines and procedures)
Approval Form

Please complete the following information and attach to your document when submitting a policy, clinical guideline or procedure for approval.

Document type (policy, clinical guideline or procedure)	Trust Policy
Document title	Surveillance Camera Policy
Document author (Job title and team)	Head of Business Security BFS – Business Security Unit
New or reviewed document	Reviewed policy
List staff groups/departments consulted with during document development	See Appendix 3
Approval recommended by (meeting and dates):	Trust Health & Safety Group – February 2023
Date of next review (maximum 3 years)	February 2026
Key words for search criteria on intranet (max 10 words)	Security, BWV, Business, Unit, Recording, Control, Camera, System, Investigation, CCTV.
Key messages for staff (consider changes from previous versions and any impact on patient safety)	• Revision of objectives • Reference to Integrated Care Board • CCTV & BWV key responsibilities for systems • Responsibilities for systems on site.
I confirm that this is the <u>FINAL</u> version of this document	**Name: Mike Lees** **Designation: Head of Business Security**

FOR COMPLETION BY THE CLINICAL GOVERNANCE TEAM

Approved by (group/committee): Trust Health and Safety Group **Date approved: February 2023** **Date Clinical Governance Administrator informed of approval: 24/03/2023** **Date uploaded to Trust Approved Documents page: 29/03/2023**