University Hospitals of Leicester NHS
NHS Trust

Digital Recording Policy

(Management, operation, and use of Closed Circuit Television (CCTV) and Body Worn Cameras (BWC))

Previously called
Closed Circuit Television (CCTV) Policy

Approved By:	Policy and Guideline Committee
Date of Original Approval:	**13 December 2005**
Trust Reference:	B44/2005
Version:	4
Supersedes:	3 – May 2018
Trust Lead:	Hannah Rose – Deputy Head of Privacy Saiful Choudhury – Head of Privacy
Board Director Lead:	Mr Andrew Furlong – Medical Director
Date of Latest Approval	7 February 2023 – Policy and Guideline Committee
Next Review Date:	March 2026

CONTENTS

REVIEW DATES AND DETAILS OF CHANGES MADE DURING THE REVIEW

1. **March 2023- Change of format to meet policy and guidelines format requirements**

2. **March 2023- Amendments to reflect change of organisation structure, roles and responsibilities.**

KEY WORDS

CCTV, Code of Practice, ICO, Crime, police, prosecution, apprehension of offenders, data protection act, privacy, RIPA, surveillance, digital recording devices, Body Worn Cameras, Body Worn Video, BWC, BWV

1. INTRODUCTION

University hospitals of Leicester NHS Trust (UHL) prioritises the safety and security of all patients, staff and visitors and aims to provide environments that are safe and secure.

The aim of this policy is to ensure (so far as is reasonably practicable) that any system installed and operated on its premises complies with regulatory requirements, national standards and codes of practice. The Trust's Digital Recording systems form part of the overall security management measures aimed at achieving compliance and delivering best practice in the interests of delivering safe services and providing a safe and secure environment.

UHL also works closely with partner organisations where the provision of safe services and a safe environment have shared ownership.

To assist in the provision of safe and secure environments the use of digital recording systems such as Closed Circuit Television (CCTV) and Body Worn Cameras (BWC) systems are used across its services.

The UHL Health and Safety policy sets out the roles and responsibilities of all staff. Additional responsibilities to enable the effective management and use of the Trust Digital Recording systems are detailed in this policy

2. POLICY SCOPE

- The Digital Recording policy standards apply to any digitally recorded information held, obtained, recorded, used or shared by the Trust that relates to personal information.
- This policy applies to all members of staff employed by UHL. It also applies to honorary contract holders, secondees, locum staff, bank staff, voluntary workers and agency staff using the resources of the Trust, as well as contractors and any others working on behalf of UHL.

3. DEFINITIONS

3.1 BWC – Body Worn Cameras:

Also known as body worn video, are devices that are typically utilized by law enforcement to record footage (audio and images) of their interactions with the public or to gather video evidence at crime scenes.

3.2 Data Controller:

The Privacy Unit is the Data controller, and is responsible for the oversight of the digital recording system where it affects the privacy of patients and staff.

3.3 CCTV – Closed Circuit Television:

Is a TV system in which signals are not publicly distributed but are monitored, primarily for surveillance and security purposes. This includes any standalone systems within the Trust.

3.4 Digital Recording System (The System):

A tool used for the prevention and detection of crime, the safety and security of public, patients, visitors and staff.

4. ROLES AND RESPONSIBILITIES

4.1 The Executive Lead for this policy is the Medical Director.

In line with the Secretary of State Directions and the NHS contract, UHL has a nominated the Medical Director as the Trust's Security Management Director (SMD). The role of the SMD includes:

- Promoting Security at Board level
- Agreeing the Local Security Management Specialist work plan and monitoring the delivery of the work plan by audit committee
- Ensuring compliance with the requirements of the directions issued by the Secretary of State, Department of Health and NHS Counter Fraud Authority

4.2 Trust Board

The Trust Board has overall accountability for the Trust's ability to meet the Digital Recording policy requirements. The Board is responsible for:

- Receiving, considering and approving regular Digital Recording policy reports and briefings;
- Signing off the Trust's Digital Recording policy and associated procedures and annual updates required in relation to compliance with relevant information security legal duties.
- The Trust is the identified Data Controller for all systems operating on its premises. The Trust is responsible for all cameras, monitors and data collection and retention processes. The Trust uses external companies (Data Processors) to control and maintain its system at some of its sites. All contracts with such companies will include adherence to this policy.

4.3 The Executive Information Management and Technology Board,

On behalf of the Trust Board, is responsible for ensuring adequate Digital Recording arrangements are in place.

4.4 Information Governance Steering Group (IGSG)

The IGSG is responsible on behalf of the Executive Information Management and Technology Board for:

- Developing, implementing and maintaining a Digital Recording policy, implementation strategy and Digital Recording work programme to provide assurance to the Trust that effective arrangements are in place: Agreeing Digital Recording relevant reports and recommendations and timely preparation of the annual Digital Recording assessment for Trust Board sign off: Working with Clinical, Corporate and Support Services to promote and embed Digital Recording into the organisational culture

4.5 Local Security Management Specialist

- Shall be responsible for ensuring that future development of Digital Recording Systems are approved in accordance with the requirements of Legislation
- Shall be responsible for seeking authorisation for covert surveillance from the relevant authority
- Will act as the link with the Counter Fraud and Security Management Service with respect to the Legislation covered by this Policy.
- Will be the first point of contact for those wishing to view or obtain a copy of digital footage captured by a Trust device.
- Will notify the Head of Privacy of any release of digitally recorded data to a third party.

4.6 Site Based Security Managers

Are responsible for the day to day management of Digital Recording Systems operated by their staff. They shall ensure that the use and management of the system is in keeping with this Policy, monitor compliance and report any breaches to the Security Management Director. Security Managers must ensure that operatives are suitably trained.

4.7 Security Officers

All Security Officers are required to undertake regular Trust mandatory training in Digital Recording to ensure that they are fully aware of their individual responsibilities and have the relevant knowledge to ensure compliance. Misuse of or a failure to properly safeguard information may be regarded as a disciplinary offence.

4.8 Privacy Unit

The Privacy Unit is the Data controller, and is responsible for the oversight of the digital recording system where it affects the privacy of patients and staff. The team advises on Data Protection issues and Subject Access Requests relating to surveillance footage. The Privacy Unit coordinates the Trust's response to requests from the Information Commissioner's Office for information on the Trust's use of digital recording.

4.9 Line Managers

Managers at all levels are responsible for ensuring that their staff are aware of this policy.

4.10 Trust Employees & staff working on behalf of the Trust

All Trust employees, whether permanent, temporary or contracted, students and contractors are responsible for ensuring that they are aware of the requirements of this policy and for ensuring that they comply with these on a day to day basis.

4.11 Senior Information Risk Owner (SIRO)

The SIRO is a nominated person (Executive or Senior Manager on the Board) who is familiar with information risk and the organisations response to risk. The SIRO takes ownership of the organisation's information governance policy including all information risk and acts as an advocate on the Board.

4.12 Information Commissioners Office (ICO)

The ICO regulates Data Protection in the UK. They offer advice and guidance, Monitor

breaches and conduct audits. The ICO monitor compliance and take enforcement action where appropriate.

5. POLICY STATEMENTS AND ASSOCIATED DOCUMENTS

5.1 Registered purpose of the Digital Recording system

In accordance with legislative requirements the registered purpose of the scheme is for the prevention and detection of crime, the safety and security of public**,** patients, visitors and staff.

5.2 Privacy of individuals – Recording of Images and Audio;

5.2.1 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. The static surveillance camera system is not installed for the purpose of recording conversations.

5.2.2 Body Worn Cameras will be operated in accordance with the Standard Operating Procedures 'Body Worn Cameras', available in Appendix 3 of this policy.

5.2.3 The Digital Recording System will also only be operated in accordance with the requirements and articles of the Human Rights Act 1998 and the General Data Protection Regulation 2016. The Digital Recording System will be operated fairly, within the law, and only for the purposes for which it was established and are identified within this Policy, or which are subsequently agreed in accordance with this Policy.

5.2.4 Article 8 of the Human Rights Act 1998 is the right to respect for private and family life, home and correspondence. Security Officers using BWC must consider Article 8 when recording and not record beyond what is necessary for the purposes set out in this policy.

5.2.5 The operation of the Digital Recording System will also recognise the need for formal authorisation of surveillance as required by the Regulation of Investigatory Powers Act 2000, in particular Part 2 of the Act.

5.2.6 Throughout this Policy it is intended, as far as reasonably practicable, to balance the objectives of the Digital Recording System with the need to safeguard the individual's rights. Every effort has been made throughout the Policy to indicate that a formal structure has been put in place, including a complaints procedure, by which it can be identified that the Digital Recording System is not only accountable, but is seen to be accountable.

5.2.7 Participation in the Digital Recording System by any organisation, individual or authority assumes an agreement by all such participants to comply fully with this Policy and to be accountable under the Office of the Information Commissioner's Code of Practice.

5.3 System Assessment and Administration

Before installing and using Digital Recording and similar surveillance equipment on any

Trust owned or occupied site the following assessment procedure must be carried out:

- Establish, and document, who is the person(s) or organisation(s) legally responsible for the proposed scheme and who are/is responsible for the day-to-day compliance with the requirements of the Code of Practice and this policy.
- The information asset administrators for the digital recording system will be the line manager(s).
- The Local Security Management Specialists will assess and document the appropriateness of and reasons for using Digital Recording or similar surveillance equipment, and any release to law enforcement or other third parties
- The Local Security Management Specialist will establish and document the purpose of the scheme.
- The Local Security Management Specialists will notify the Information Commissioner of the purpose(s) of the scheme. Registration with the Information Commissioners Office as a data controller (including the use of onsite recording equipment) is done by the Privacy Unit.

5.4 Siting of cameras and signage

5.4.1 The location of cameras will be carefully considered, so that the means by which, and the way in which, images are captured will comply with GDPR principles including processing and management requirements.

5.4.2 The Trust will ensure that there is sufficient signage or other means of communication to inform people that they are in an area where Digital Recording is being carried out.

5.4.3 The most effective way of doing this is by using prominently placed signs at the entrance to the Digital Recording zone.

5.4.4 The following standards must be met:

- Cameras must be sited in such a way that they only monitor those spaces, which are intended to be covered by the equipment.

- If private domestic areas such as gardens or areas not covered by the scheme, border those spaces which are intended to be covered by the equipment then the user must consult with the owners of such spaces. If images from those spaces might be recorded, these areas may need to be blanked out, either manually or digitally.

- Operators must be aware of the purpose(s) for which the scheme has been established.

5.5 Use of Body Worn Cameras

Security Officers must be aware of their specific responsibilities when using a Body Worn Camera. These are set out in Appendix 3 – Standard Operating Procedures.

5.6 Processing images

Footage that is not required for the purpose for which the equipment is being used must not be retained in an identifiable form for longer than necessary, in compliance with GDPR Principle 5 (Article 5(e)). Footage marked 'evidential' will be retained securely for 18 months and then reviewed and if not needed, destroyed securely.

While images are retained it is essential that their integrity be maintained, whether it is to ensure their evidential value or to protect the rights of people whose images may have been recorded. It is therefore important that access to and security of the images is controlled in accordance with the requirements of the GDPR and for law enforcement purposes the Data Protection Act 2018 – and Law Enforcement Directive 2017.

So that data protection principles are complied with, the data controller and system operators will ensure that footage is not retained for longer than 30 days unless it is required for evidential purposes in legal or other investigation proceedings. Once the image 18 month retention period has expired, the footage itself is removed or erased.

Footage retained for evidential purposes will be removed from the system and retained in a secure place to which access is controlled.

5.7 Disclosure of images to third parties

It is important that access to and disclosure of the footage recorded by surveillance systems is restricted or carefully controlled not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.

Where disclosure is requested the data controller must satisfy themselves that:

5.7.1 The reason(s) or purpose(s) for the disclosure is compatible with the reason(s) or purpose(s) for which the footage was originally obtained.

5.7.2 Access is restricted to authorised persons who need to have access in order to achieve the purpose(s) of using the equipment.

5.7.3 All access to images must be documented.

5.7.4 Access to images must only be allowed for a lawful purpose and prescribed circumstances and must be authorised by the Local Security Management Specialist, with a notification to the Head of Privacy within the IM&T Department.

5.8 Access to images as part of a Subject Access Request (SAR)

Access to personal data held in the form of surveillance footage must be granted in accordance with the General Data Protection Regulation 2016 and Applied UK Data Protection Act. SARs will be handled by the Privacy Unit and the footage will be provided by the Security team.

5.8.1 If the requester has asked for a copy of the footage, arrangements for the redaction of any third party data must be made with an external editing company.

5.8.2 If redaction is not possible due to the cost implication of the editing involved, the requester must be informed of this in good time within the 30 day time limit. A viewing of the footage will be made available instead. This viewing must be completed at an agreed time that is convenient for the requester, in an area that has

been made private for the purposes of viewing footage, such as a secured office.

5.8.3 If the requester refuses an offer to view the footage and insists on a copy of it, the Trust may produce a report or transcript of the recording. This method must only be used as a last resort to comply with the SAR, and must not be used as an alternative to offering a viewing.

6. EDUCATION AND TRAINING REQUIREMENTS

Full training will be provided to all Security Officers in how to use BWC. This will be given to all new officers and refresher training will be given every 12 months.

Full training will be provided to all Security Officers in how to use the non-BWC surveillance equipment. This will be provided by the Security team.

7. POLICY MONITORING TABLE

Element to be monitored	Lead	Tool	Frequency	Reporting arrangements
Regular checks on data protection law and assessments to be completed on surveillance system when used in a new area or for new purpose	Privacy Team	Data Protection Impact Assessment Tool and contact with ICO as appropriate	Annually/ in line with legal changes	IGSG
Regular checks on the system take place to ensure that it is working properly	Security team/LSMS	Security standards	Quarterly	IGSG

8. EQUALITY IMPACT ASSESSMENT

The Trust recognises the diversity of the local community it serves. Our aim therefore is to provide a safe environment free from discrimination and treat all individuals fairly with dignity and appropriately according to their needs.

As part of its development, this policy and its impact on equality have been reviewed and no detriment was identified.

9. SUPPORTING REFERENCES, EVIDENCE BASE AND RELATED POLICIES

The following documents are supporting policies that provide advice and guidance to managers and staff, to enable the safe management of services:

- Trust Health and Safety Policy A17/2002
- General Data Protection Regulation 2016
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality;
- The NHS Confidentiality Code of Practice.
- Information Commissioners Office – CCTV Code of Practice
- Security Policy- A14/2002
- NHS Protect Security Manual Guidance Note 3.5 – CCTV

10. PROCESS FOR VERSION CONTROL, DOCUMENT ARCHIVING AND REVIEW

The UHL Information Governance Steering Group is responsible for keeping this policy up to date.

The policy will be reviewed every three years or sooner if there is any significant change in legislation or if a technology that has not been used at UHL is to be employed.

The updated version of the Policy will then be uploaded and available through INsite Documents and the Trust's externally-accessible Freedom of Information publication scheme. It will be archived through the Trusts PAGL system.

1. Management of Digital Recording Schemes

No Digital Recording scheme must be initiated, installed, moved or replaced without prior approval by the Local Security Management Specialist to approve such schemes. The Privacy Unit must also be informed.

All schemes are required to meet the following standards and must be formally approved (as above) prior to any installation:

- Establish who are the person(s) legally responsible for the proposed scheme within the Trust.

Assess the appropriateness of, and reasons for, using digital recording or similar surveillance equipment.

- Document this assessment process and the reasons for the installation of the scheme.
- Establish and document in accordance with current legislation the purpose of the Scheme.
- Ensure that the notification lodged with the Office of the Information Commissioner covers the purposes for which this equipment will be used.
- Establish and document the person(s) or organisation(s) that are responsible for ensuring the day-to-day compliance with the operational requirements of such schemes and this policy.

Any new digital recording equipment must be purchased in conjunction with appropriate procurement arrangements. If a member of staff wants to implement a new digital recording system they must contact the Local Security Management Specialist.

2. Digital Recording

- All Digital Recording systems installed onto Trust premises must have the storage capacity to hold a minimum of 30-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.
- There are no prescribed minimum or maximum retention periods which apply to all systems or footage. Rather, retention must reflect the organisation's purposes for recording information. The retention period must be informed by the purpose for which the information is collected and how long it is needed to achieve this purpose. It must not be kept for longer than is necessary, and must be the shortest period necessary to serve your own purpose. This must not be determined simply by the storage capacity of a system. UHL standard is 30 days unless the footage is justifiably marked and retained as 'evidence'.
- Where a Digital Recording system is installed all sites must have local access to a DVD recorder that is compatible with the system in use.
- All sites must hold a stock of blank, write once DVDs.

Where there is access to recorded footage via the network, controls must be put into place so only authorised users are able to access it.

- If police require access to recorded footage, an area must be made available for viewing.

- If the police require a copy of the footage on DVD, two copies must be made. One copy to be retained by the Trust and the other given to the police. The event will be noted in the log and the details and signature of the recipient obtained.

3. Positioning of cameras and signs

The location of the equipment must be carefully considered, the following points must be taken into consideration before installing either a new camera or a full Digital Recording system.

- Equipment must be situated so they can only monitor the area that is intended to be monitored.

- Equipment must be situated so they can only monitor for the predefined purpose.

- Cameras must not be positioned in areas where it would be considered private e.g. toilet, changing room, private office.

- If the area covered by a camera borders private property every effort must be made to ensure the private area cannot be viewed

Signs must be placed so that the public and staff are aware that they are entering a zone covered by surveillance equipment. The size of the sign will vary according to the location, a large A3 sign may be used in a parking area, where as an A4 sign be placed on a door.
They must be clearly visible and legible, the sign must contain the identity of the organisation responsible for the scheme, the purposes of the scheme and contact detail for the organisation.

4. Site Administration and Procedures

An incident log will be maintained at each site and kept secure. Brief details of incidents will be noted together with any consequential action taken.
It is recognised that the images obtained are sensitive and subject to the law on data protection. All , DVDs, digital images and copies will be handled in accordance with working procedures, which are designed to ensure the integrity of the system. A DVD log will be kept at each site for the purposes of recording the use of DVDs, their use and retention for evidential purposes.
Other than by authorised staff investigating untoward incidents, digital images will only be viewed at the request of the police or through subject access procedures. Copies of DVDs will only be made for the purposes of crime detection, evidence for prosecutions or where required by law.

5. Digital Recording Staff

All staff involved in the handling of the Digital Recording equipment, both directly employed and contracted, will be made aware of the sensitivity of the footage being handled.

Staff will be fully briefed and trained in respect of all functions, both operational and administrative, relating to camera operation. Training by camera installers will also be provided as appropriate.

Training in the requirements of the law on Data Protection and further training in accordance with Trust requirements will be given to staff who are required to manage and to work the Digital Recording systems.

6. Recording

Systems are supported by recording facilities which will function as appropriate. In addition incidents can be recorded in 'real time' where necessary.

A DVD log will be maintained at each site. Each DVD will be uniquely identified and all activities relating to each DVD. E.g. date and hours of recording, viewing for specific purpose, copies taken, DVDs retained for evidence, DVDs destroyed etc. will be recorded in the log.

In the event of the DVD being required for evidence, it will be retained for a period recommended by the Trust's legal advisors and/or the police.

7. Monitoring procedures

The responsibility for monitoring the Digital Recording system and the log lies with the Security Manager.

8. Camera Control

On each occasion an incident is recorded a report setting out the time, date and detail of the incident will be submitted by the relevant operator to the relevant Security manager.

Adjustment and alteration to siting or use of cameras must be made by staff that has the appropriate authority. Data protection principles must be considered during this process. All footage belongs to and remains the property of the Trust. Footage handling procedures are in place to ensure the integrity of the image information held.

9. The viewing areas/rooms

Images captured by the systems will be monitored on each site, in a secure environment. Unauthorised personnel or visitors must not be able to see the monitors.

Access to view monitors DVDs and digital recordings will only be granted to persons with a legitimate reason or those who have followed the subject access procedures. Identity and authorisation will have been presented and validated to the responsible officer. Visitors will be required to complete and sign an access log. Details recorded will include name, department or organisation, the person who granted access, time of entry and exit, and DVD or digital image referenced and extracts viewed.

Retention and Disposal

1. At the end of their useful life all footage will be overwritten and DVDs will be destroyed and disposed of as confidential waste. Spot checked for erasure prior to being destroyed or disposed of.

2. It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose(s) for which they are intended. Upon installation an initial check must be undertaken to ensure that the equipment performs properly.

3. If the system records features such as the location of the camera and/or date and time reference, these must be accurate. When installing cameras, consideration must be given to the physical conditions where the camera is located e.g. infrared equipment may need to be installed in poorly lit areas.

4. It is important that access to and disclosure of the footage recorded by digital systems is restricted or carefully controlled not only to ensure that the rights of individuals are preserved, but also to ensure that the continuity of evidence remains intact, should the images be required for evidential purposes.

5. Access to recorded images must be restricted to that staffs that need to have access in order to achieve the purpose(s) of using the equipment.

6. All access to images must be documented.

7. Access to images by third parties must only be allowed in limited and prescribed circumstances and permission for footage to be burned onto DVD must be authorised by the Local Security Management Specialist.

8. If the purpose of the system is the prevention and detection of crime, then disclosure to third parties should be limited to the following:

    - Law enforcement agencies where the images recorded would assist in a specific criminal enquiry, or where the images are to be used to assist law enforcement agencies in the return of patients who take unauthorised absence under section of the Mental Health Act 1983, or relevant criminal justice legislation.

    - Prosecution agencies.

    - Relevant legal representatives.

9. The media, where it is decided that the public's assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. As part of that assessment, the wishes of the victim of an incident must be taken into account.

10. People whose images have been recorded and retained (unless disclosure to and individual would prejudice the criminal enquiries or criminal proceedings).

11. All requests for subject access should be recorded and reported to the Audit Committee. If access or disclosure is denied, the reason should be documented and also reported to the Security Management and Police Liaison Group, for onward reporting to the Audit Committee. A log of requests is to be maintained by the Privacy Unit.

12. If access to or disclosure of the images is allowed, then the following must be documented.

    - The date and time at which access was allowed or the date on which disclosure was made.
    - The identification of the third party who was allowed access or to whom disclosure was made.
    - The reason for allowing access or disclosure.
    - The extent of the information to which access was allowed or which was disclosed.

13. Recorded images must not be made more widely available – for example they must not be routinely made available to the media or placed on the Internet. If it is intended that images will be made more widely available authorisation is required from the Privacy Unit. The reason for that decision must be documented.

14. If it is decided that images will be disclosed to the media (other than in the circumstances outlined above) the images of individuals will need to be disguised or blurred so that they are not readily identifiable.

15. If the system does not have the facilities to carry out the type of editing required an editing company may be hired to carry out that editing.

16. If and editing company is hired, then the manager or designated member of staff needs to ensure that:

17. There is contractual relationship between the data controller and the editing company.

18. That the editing company has given appropriate guarantees regarding the security measures they take in relation to the images.

19. The manager has checked to ensure that those guarantees are met.

20. The written contract makes it explicit that the editing company can only use the images in accordance with the instructions of the manager or designated member of staff.

21. The written contract makes the security guarantees provided by the editing company explicit.

22. There is a non-disclosure agreement signed by the editing party. This is available from the Privacy Unit.

University Hospitals of Leicester NHS
NHS Trust

Application for Access to Digitally Recorded Footage (Law Enforcement form)

Name of person making request:	
Organisation:	
Address:	
Telephone Number:	

STORAGE OF FOOTAGE TO BE VIEWED

Date:	
Reason: (For police only)	

Signed:		Dated:	
Request Granted:		Request Denied (Reason):	

TO BE COMPLETED IF IMAGES ARE FOR DISCLOSURE

Disc No.	
Issued To:	
Crime No: (For police only) UHL Reference No: Other Reference No:	
Date Issued:	
Issued By:	
Return Date:	

I acknowledge receipt of the above Disc:		Organisation and Title	
Signed:			
Print Name			

Application for Access to Digitally Recorded Footage (Civilian form Page 1 of 2)

In addition to this form we will need proof of your identity and the correct fee (if applicable) before we can process your request.

Details of person making request for footage	
Title:	
Forename:	
Surname:	
Current Address:	
Contact Telephone Number:	

Details of Footage Requested		
Date that the footage was recorded:		
Approximate time:	**Start Time:** 00:00	**Finish Time:** 00:00
Location:		
Additional Details which will assist in locating exact CCTV required:		
"I would like to come in and view the footage" (please indicate as appropriate)	Yes/No	Yes/No
"I would like a copy of the footage" (please indicate as appropriate)	Yes/No	Yes/No

Application for Access to Digitally Recorded Footage (Civilian form Page 2 of 2)

Declaration:

I declare that the information given to me is correct to the best of my knowledge and that I am entitled to apply for this footage.

Signed

(By the applicant)

Date:

You are advised that the making of false or misleading statements in order to obtain personal information to which you are not entitled is a criminal offence which could lead to prosecution.

Please return this form along with appropriate documentation and fee (if applicable) to:

Privacy Unit
University Hospitals of Leicester NHS Trust
C/O Glenfield County Hall
Leicester
LE3 8RA

Telephone No: 0116 258 8537

1. BWC is used within UHL in accordance with current data protection legislation and Article 8 of the Human Rights Act. Security Officers must be aware of their specific responsibilities when using a Body Worn Camera. These are under the control of the officer wearing the camera, and can be set to record at the discretion of the officer.

2. If the circumstances arise where it is appropriate, BWC can be used on wards and other areas where a fixed camera would not be an appropriate option in a healthcare situation.

3. All of the security officers who use BWC will be appropriately trained in the use of the camera and in how to recognise a situation in which it would be appropriate to begin recording.

Common Law and Use of BWC

4. Common Law provides the Security Officers with the authority to use BWC in the lawful execution of their duties, for the purposes of the prevention and detection of crime and for the protection and health and safety of patients and staff.

5. These cameras are able to record both images and audio, however these will only be set to record when the Security Officer wearing the camera decides that the situation meets at least one of the criteria prescribed below:
   - Any Use of Force or Anticipated Use of Force
   - Where a Security Officer is directed to record all or part of a particular incident by a Supervising Officer.
   - The situation involves violence or aggression (verbal or physical) against any members of staff employed by UHL including honorary contract holders, secondees, locum staff, bank staff, voluntary workers and agency staff, as well as contractors, visitors, patients or any other people on Trust sites.

6. The officer wearing the camera must make every effort to announce the intention that it will be set to record audio and images to those who may be included in the recording.

7. BWC is to be used in an overt manner only; no covert use is to be employed.

8. Once recording has commenced, the Security Officer must, if practicable, make an announcement (captured on the recording) with regards to the time, date, location and the rationale for the recording.

9. Recordings must commence at the start of any deployment to an incident and should continue uninterrupted until the incident is concluded, either because of resumption of normal duties or because recording has commenced through another video system.

10. An announcement must, if practicable, be made (captured on the recording) to indicate the ending of the recording.

11. Recordings must not be made of general duties / patrolling duties unless this is part of a specific operation.

12. Security Officers must remember their Duty of Care to patients and use sound judgment when using BWC in areas such as hospital wards or areas of religious worship, to avoid causing harm and distress to patients.

13. If requested to stop recording, the benefits and safeguards provided should be highlighted to those present. These include:

    - That the Security Officer's continued presence might be required to prevent a breach of the peace or injury to any person;
    - That continuing to record would safeguard all parties, with a true and accurate recording of any significant statement made by those party to the incident and of the surroundings
    - That continuing to record will safeguard the Security Officer against any potential allegations.

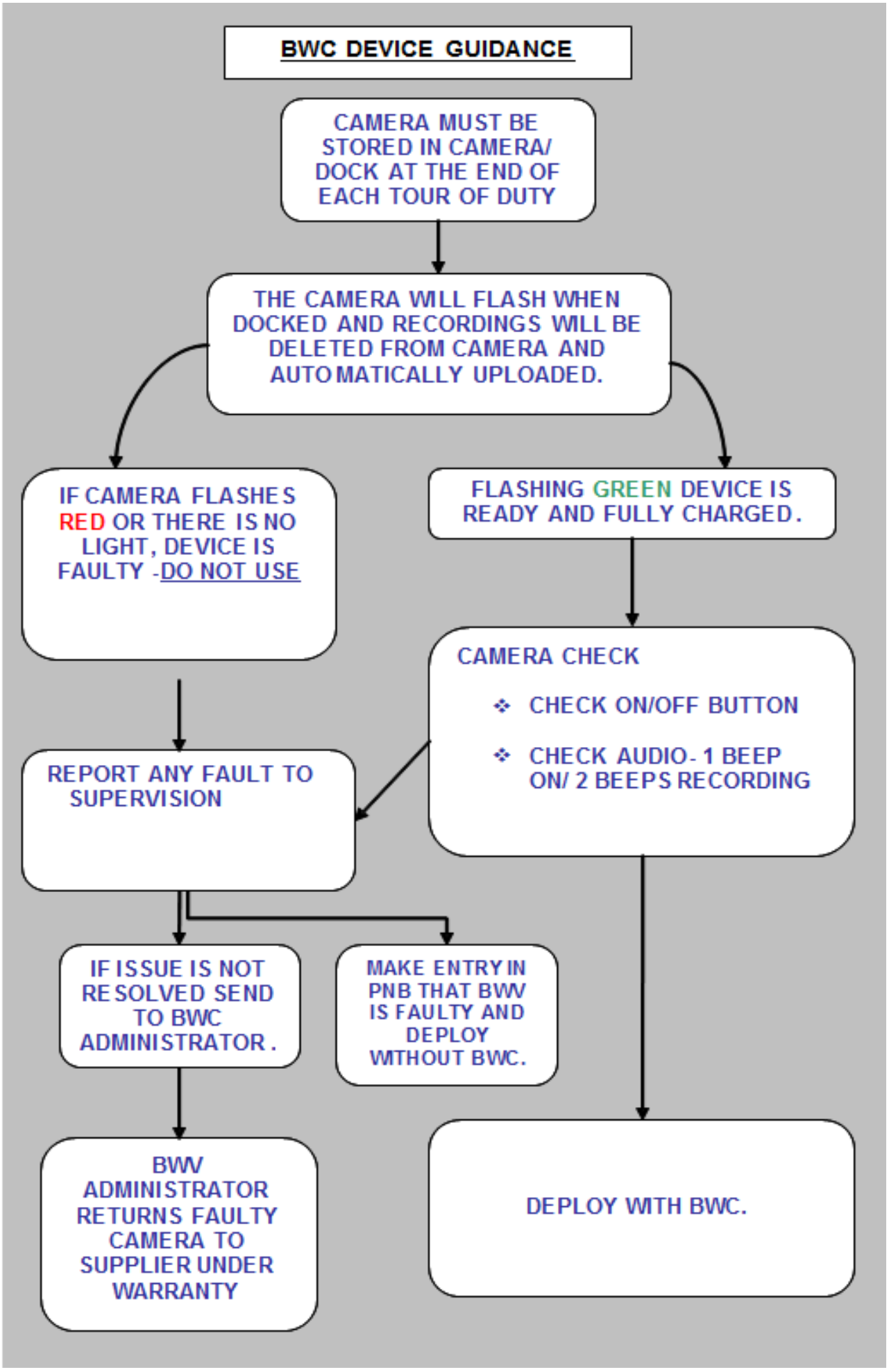
    The recording must CEASE under certain conditions:

    - If it becomes clear that the use of BWC is causing an escalation of the incident and/or is obstructing or delaying the peaceful resolution of the incident.
    - If it becomes clear that the use of BWC is causing high levels of offence and distress by recording images of a sensitive nature on the hospital wards.

14. Body Worn Cameras will be issued at handover (and checked for faults) to each public facing Security Officer, who **MUST** carry their BWC (unless their device is faulty) when being deployed on operational duties. Supervisors are required to ensure compliance.
15. Security Officers must always use their own issued cameras to record footage when possible, as the BWC system automatically assigns this footage to that personal account for audit and access purposes.
16. In the event another camera is used, the Supervisor must be informed as soon as possible so that the footage can be reassigned to the right account, so that the audit trail remains accurate and footage that has been recorded is not showing as recorded by a different Security Officer.
17. The microphone on the BWC device is sensitive so as to capture all speech relative to the images in view. Unfortunately this also means that Security radio traffic will be captured. BWC operators should where practicable use earpieces to their own radios to minimise any such intrusions and be mindful of colleagues nearby who may not be using earpieces.
18. There may be occasions where an incident is only partially recorded, such as through technical failure, the equipment being knocked, covered or dislodged during a struggle or through the nature of the incident where the BWC view is restricted. There may also be occasions where the sound recording is unclear or verbal responses are difficult to hear because of other more prominent sounds such as Security radio traffic or noise created by strong winds. Security Officers must therefore ensure that they gather and retain evidence through normal (non-video) means and must not become reliant on video recording for the sole provision of their evidence.

<u>Viewing the Footage</u>

19. Footage captured on a BWC will not be available for instant viewing by the officer wearing the camera, but will be held on a separate server, operated from the control room. This will be subject to the same retention period as the footage from the fixed cameras, 30 days unless marked as 'evidential'.
20. Subject access for footage from Digital Recording systems will be available until such time as it is deleted. Security Officers are responsible for marking each recording as evidential.
21. Recordings marked as evidential at any time during the 30 day period will prevent deletion and will be subject to the same retention period as that of the footage from non-BWC source


BWC DEVICE GUIDANCE
CAMERA MUST BE STORED IN CAMERA/ DOCK AT THE END OF EACH TOUR OF DUTY
THE CAMERA WILL FLASH WHEN DOCKED AND RECORDINGS WILL BE DELETED FROM CAMERA AND AUTOMATICALLY UPLOADED.
IF CAMERA FLASHES RED OR THERE IS NO LIGHT, DEVICE IS FAULTY -DO NOT USE
FLASHING GREEN DEVICE IS READY AND FULLY CHARGED.
CAMERA CHECK
CHECK ON/OFF BUTTON
CHECK AUDIO- 1 BEEP ON/ 2 BEEPS RECORDING
REPORT ANY FAULT TO SUPERVISION
IF ISSUE IS NOT RESOLVED SEND TO BWC ADMINISTRATOR.
MAKE ENTRY IN PNB THAT BWV IS FAULTY AND DEPLOY WITHOUT BWC.
BWV ADMINISTRATOR RETURNS FAULTY CAMERA TO SUPPLIER UNDER WARRANTY
DEPLOY WITH BWC.