CLOSED CIRCUIT TELEVISION PROTOCOL

Protocols for installation, monitoring and management (CCTV)

1.0 INTRODUCTION AND AIMS

1.1 This protocol should be read in conjunction with the EPUT Surveillance Systems Policy (CP28).

1.2 The concept of Closed Circuit Television (CCTV) has been to be acceptable to patients, visitors and staff; the use remains under constant review.

1.3 The primary purpose of the use and activation of Closed Circuit Television (CCTV) in Essex Partnership University Trust (EPUT) is to improve the safety of patients and staff.

1.4 Evidence indicates that the use of video recording devices may reduce the incidences of aggression and violence, whilst also providing greater transparency and enabling increased scrutiny for any subsequent actions taken in response to such occurrences.

1.5 CCTV does not and cannot prevent incidents occurring; it is purely a means of ensuring that the Trust can record incidents, and the material can be used to support further action when necessary.

1.6 The Closed Circuit Television Protocol is intended to provide information and guidance to ensure that:

- Any CCTV systems are justified, appropriately managed and not open to abuse or misuse.
- Correct assessments are made in relation to the need for any CCTV requirement
- CCTV is appropriately installed, monitored, maintained and managed.
- Responsibility for the management of CCTV systems is identified at both local and Trust wide level.
- Access, storage and disclosure of images are in accordance with the principles of the General Data Protection Regulation 2016 and the Data Protection Act 2018 and with Trust policy on data protection.
- The identification and training of data managers where the Trust is the Data Controller of a CCTV system.

2.0 ASSESSMENT PROCESS FOR THE INSTALLATION OF CCTV SYSTEMS

2.1 Where consideration is being given to the installation of a new or replacement CCTV system this will be co-ordinated by the Compliance and Security Officer (CSO). No installation, maintenance or alteration will take place without the agreement of the CSO and Trust governance.

2.2 The CSO will liaise with Information Governance in carrying out a Data Privacy Impact Assessment, establishing the justification and requirement for new installations of CCTV.

2.3 In line with CP28 – Surveillance Systems Policy all installations must ensure quality footage to meet Information Commissioner's Office (ICO) guidance where possible.

3.0 SYSTEMS AND RECORDING

3.1 CCTV cannot and is not designed to replace clinical care or as a means to answer security concerns. It does not and cannot replace skilled employees as a method of observing patient behaviour.

3.2 There are three types of area that is defined for CCTV coverage.

- Public areas
- Communal areas
- Private areas

3.3 Public areas; these are areas to which the public have unrestricted access: grounds, corridors, car parks, etc.

3.4 Communal areas: Parts of wards shared by all patients; day rooms dining areas, corridors etc.

3.5 There are no special considerations required for Public or Communal areas beyond those required by the Information Commissioner on all CCTV cameras, such as signage, registration etc., and that a clear reason for installation is available.

3.6 Private areas: these are areas where any individual might reasonably expect privacy. These include bathrooms, bedrooms, toilets and seclusion rooms.

3.7 The use of monitoring CCTV (not recordable) within private areas is only routinely authorised for Seclusion Rooms and Health-Based Places of Safety

3.8 CCTV camera's when operational/without fault record 24/7 and Whilst a retention period of 31 days is often quoted, retention periods are not mandated in law, However the Trust attempts to fulfil a minimum of 31 days.

3.9 All faults with CCTV equipment – please report to Estates and Facilities helpdesk

HELP DESK - ESSEX (SOUTH) 01268 407814 - 8am to 4pm (Monday to Friday)

HELP DESK - ESSEX (NORTH & WEST) 01206 334500 - 8.30am to 5pm (Monday to Friday)

HELP DESK - BEDFORD 01234 310120 - 8am to 4pm (Monday to Friday)

4.0 DATA PROTECTION LEGISLATION

4.1 The Trust will identify, list and document all its CCTV schemes within the "Notification" ('registration of data systems'), which it is required to make to the Information Commissioner under the terms of the General Data Protection Regulations 2016 and the Data Protection Act 2018.

4.2 To comply with the current Data Protection Act legislation, all operational management of the Trust CCTV surveillance systems will conform to guidance within "Information Commissioner CCTV Code of Practice" published by the Information Commissioner (a copy of which is available from the Information Governance Manager). In order to conform to this code of practice the following guidelines must be adhered to:

- The data manager is responsible for CCTV systems Trust wide, maintaining compliance with relevant policies and procedures. The data manager will also be responsible for the management and control of all imagery that is downloaded in accordance with this policy including appropriate, back-up, retention, and destruction of all storage media.

- Cameras will not be hidden from view and appropriate steps must be taken, e.g. by signing and display posters, to inform employees, patients, visitors and the public of the presence of the CCTV surveillance system in use, Trust name and contact details, including a working telephone number, of who can provide further information if requested. To ensure privacy the cameras are fixed and focussed to observe Trust property, which can be demonstrated upon receiving a specific request.

- Images from the cameras are appropriately recorded, maintained and managed in accordance with this operational protocol and wider Policy.

- There is no audio recording undertaken from any part of the Trust CCTV surveillance systems.

4.3 In order to comply with the General Data Protection Regulation 2016 and the Data Protection Act 2018, the following standards must be met:

- All imagery must be fairly and lawfully processed.
- All imagery will only be maintained for specific purposes and all CCTV installations will be proportionate and not excessive.
- All CCTV imagery will be processed in accordance with individual's rights.
- CCTV imagery will not be transferred to countries outside of the EEA without adequate protection.
- All contractors with the capability of accessing CCTV data whether via periodic maintenance contracts or one-off tasks generated to undertake a download of footage regarding an incident must be in a signed contractual agreement with the Trust.

5.0 DISCLOSURE OF DATA/SUBJECT ACCESS REQUESTS (SAR)

5.1 Disclosure of images from the CCTV system must also be controlled and consistent with the purpose for which the system was established. For example, if the system is established to help prevent and detect crime it may be appropriate to disclose images to law enforcement agencies where a crime needs to be investigated. Even if a system was not established to prevent and detect crime, it may still be acceptable to disclose images to law enforcement agencies.

5.2 Any other requests for images should be approached with care, as a wide disclosure of these may be unfair to the individuals concerned. In some limited circumstances it may be appropriate to release images to a third party, where their needs outweigh those of the individuals whose images are recorded.

5.3 Failure to protect the data of subjects or the integrity of the system would likely result in disciplinary procedures being brought against not only the individual(s) undertaking the access but also those sharing it.

5.4 All Internal CCTV footage requests should be in relation to one of the below departmental investigations. Requests should be made via CP28 Appendix 3a and sent to:-

- **Safeguarding – epunft.safeguarding@nhs.net**
- **Complaints – epunft.complaints@nhs.net**
- **Inquests – epunft.floandinquests@nhs.net**
- **HR – epunft.employeerelations@nhs.net**

5.5 All External requests for CCTV footage must be sent to epunft.sar@nhs.net with a completed CCTV request form – (CP28 Appendix 3)

5.6 Guidance on making a request can be found on CP28 Appendix 4 CCTV/BWV Flowchart.

5.7 Requests for access to footage, if there is an associated Datix please provide reference within the application in line with the Trust incident reporting guidelines.

5.8 Following a SAR for CCTV footage, the Trusts Legal Team will request a copy of the CCTV from the Trust's CSO. The CSO will be responsible for obtaining the CCTV footage either in house or via contractors. The CSO will download a copy of the footage and drop into the internal shared drive (Legal) for legal to review. The Legal team will save a copy of the footage into the required SAR folder and delete the copy within the internal shared drive (Legal).

5.9 Disclosure of images to third parties should only be made in limited and prescribed circumstances. For example the prevention and detection of crime where disclosure to a third party (Police) would assist in a specific criminal enquiry, security issues or in pursuit of criminal activity.

5.10 If the data subject does not know the date and approximate time of the material being sought, the search for data will be at the discretion of the Trust's Legal Team/CCTV team on a case by case basis following an assessment of the basis of the severity of the case/requirements of request.

5.11 The Trust's Legal Team will have responsibility to determine whether to comply with a request for access to CCTV images and to determine whether the disclosure entails releasing images of third parties. If a third party identity cannot be removed then the request may be denied. Where access is denied the individual will receive a written response stating why within 1 (one) calendar month of receiving the completed "Subject Access Request form".

5.12 Where media is or may be required for evidential purposes in legal proceedings, or requested by legal representatives (solicitors, Crown Prosecution Services etc.), it will be kept and stored under designated secure environments until all legal proceedings are exhausted.

5.13 All staff who wish to request CCTV relating to damage to personal property are to submit a completed subject access request CCTV form directly to the Legal team for action. epunft.sar@nhs.net

5.14 All out of hours requests for CCTV footage will be supported in the event of a serious incident or to assist in identifying absconder, considered to be of high risk to self and/or members of the public. Out of hours CCTV footage requests that are supported will still need completed subject access request form sent to epunft.sar@nhs.net.

Out of hour's requests for CCTV footage - via the EPUT contact centre:
0300 123 0808
(Please also refer to CP28 Appendix 4 / CCTV - BWC Access Flowchart).

6.0 DESTRUCTION OF DATA

6.1 Destruction of CCTV data - Advice must be obtained for each individual case, for further information contact epunft.CCTV@nhs.net

6.2 Formatted data media i.e. memory sticks, hard drives and rewritable discs are not considered destroyed simply by reformatting/deleting due to software being available that allows the ability to reconstruct the data previously stored on such devices, therefore they will need to be destroyed and disposed of correctly. For further information contact epunft.CCTV@nhs.net

7.0 MONITORING COMPLIANCE

7.1 The Trust CSO is responsible for the review, assessment and installation of all CCTV systems, data collection and control of images.

7.2 This protocol is subject to the same monitoring / review arrangements as described in the CP28 – Surveillance Systems Policy incl. (CCTV) (BWV)

7.3 The protocol will be reviewed as required, with a minimum of 3 yearly review, unless required before.

8.0 GOVERNANCE REPORTING WITHIN THE TRUST

8.1 CCTV will be a standing item on the agendas of Corporate Health, Safety and Security Sub-Committee, thus ensuring that there is Trust-wide monitoring and assurance in relation to the use and effectiveness of CCTV.

8.2 The minutes of the Health, Safety and Security Sub-Committee will be reported to the Quality Committee, the minutes of which will be reported to the Trust Board of Directors. As such, there is a clear governance route for monitoring through to Board level.

9.0 ADVICE AND GUIDANCE

9.1 Any queries in terms of CCTV and Trust protocols should be emailed to the dedicated email address of epunft.cctv@nhs.net or alternately, you can call the Trust CSO via the Contact Centre.

END

BODY WORN VIDEO PROTOCOL

Protocols for the issue, use and usage of body worn video (BWV)

1.0 INTRODUCTION AND AIMS

1.1 This protocol should be read in conjunction with the EPUT Surveillance Systems Policy (CP28)

1.2 The concept of Body Worn Video (BWV) has been to be acceptable to patients, visitors and staff; their use remains under constant review.

1.3 The provider of the BWV is Reveal Media, the devices are robust cameras which fit to the user's clothing by a strong magnet and have an on/off button and a record/stop button.

1.4 The primary purpose of the use and activation of Body Worn Cameras (BWC) in Essex Partnership University Trust (EPUT) is to improve the safety of patients and staff.

1.5 Evidence indicates that the use of video recording devices may reduce the incidences of aggression and violence, whilst also providing greater transparency and enabling increased scrutiny for any subsequent actions taken in response to such occurrences.

1.6 The BWC and their associated accessories have undergone a rigorous testing process to endure that they are suitable and safe for use within the selected services.

1.7 BWV does not and cannot prevent incidents occurring; it is purely a means of ensuring that the Trust can record incidents, and the material can be used to support further action when necessary.

1.8 The Body Worn Video Protocol is intended to provide information and guidance to staff in terms of the issue, usage and storage of BWCs within the Trust. This outline the expectations of staff and managers in implementing safe working practices relating to BWV.

2.0 RESPONSIBILITIES AND TRAINING

2.1 This protocol applies to any person who is required to carry out duties on behalf of the Trust as a Body Worn Camera user.

2.2 This protocol applies to all staff working on wards where BWC's are deployed.

2.3 Training in the content of this protocol and the use of the BWC's will be provided by the Ward Managers, Matrons or the VAPR team. There is also a training video, and other supportive material, on the Trust intranet under the VAPR pages;

https://input.eput.nhs.uk/TeamCentre/risk/sec/Pages/Body-Worn-Cameras.aspx

2.4 The VAPR team and BWV administrator will regularly visit wards to ensure cameras are being used, in good working order and train any staff requiring additional support in using the devices.

2.5 Queries with the devices or their use can be directed to the BWV administrator on epunft.BWC@nhs.net or the VAPR team on epunft.VAPR@nhs.net

3.0 SYSTEMS AND RECORDING

3.1 The BWCs should be worn during each shift and be activated when and where an incident is taking place.

3.2 4 cameras per ward have been allocated, this allows 2 to be used whilst 2 are on charge for the following shift. It is suggested the Nurse in charge and the security nurse wear the cameras during the shift.

3.3 If the designated member of staff is unable to wear the unit due to sickness or injury, the NIC will allocate another suitable member of staff and keep a record of the change on the BWV booking form.

3.4 If the designated wearer leaves the hospital for any planned reason i.e. breaks or escorts, they should return their camera to the docking station, alerting the NIC so that another staff member can be allocated to wear the BWC. The new staff member will make a note of the change on the BWC booking form.

3.5 If staff are following a service user after absconding, the staff member can use the device to record the patient supported return to the ward.

3.6 The camera must be attached using the fitting provided. The magnets are extremely strong and care must be given to roll the parts apart using the finger holes.

3.7 Any footage recorded during the shift will be uploaded when the camera is returned to the docking station and stored on a secure cloud.

3.8 Footage should be recorded when it relates to an incident / potential incident and should also be supported by a DATIX entry.

3.9 The BWC (and associated fittings / harness) **must be** handed back at the end o f the shift and any faults or damage reported to the VAPR team via a DATIX.

4.0 FLOWCHART FOR USAGE

Staff Responders (users) are trained in PMVA and will have received further training in the use of BWV.

A member of staff from the designated wards will wear a BWC and they will be the designated 'staff responder' (users) to incidents.

Staff will sign the BWC log and collect the BWC from the designated area at the start of their shift. They will wear the BWC for the duration of the shift.

In the event of an incident occurring, member of staff feeling threatened or at the request of the patient, staff wearing the camera will immediately activate the BWC and notify the individual, that the incident is being recorded.

In the event that attack alarms have also been activated and other users attend the incident, users will activate their BWC on entrance to the unit in question. Wherever practical they will notify people that they are recording.

The users should continue to record for as long as necessary to gain best evidence before announcing the cessation of recording. Following the use of prone restraint and/or seclusion, users will continue to film after staff have disengaged from holding the patient to establish the patient's state of health (focus on their respiration rate and consciousness level).

When completing a DATIX for the incident, the use of BWCs should be noted by clicking the 'BWV used' button/ tab on the Datix submission. Without this tab being completed the footage is unlikely to be saved.

At the end of their shift the users will return their device to the docking station for uploading and recharging and sign the BWC log. They will report any faults o r damage to the cameras to the VAPR Team forthwith. Any faults/damages should be Datixed. If in the unlikely event of the camera running out of charge, it should be returned to the charging dock, where it will recharge and download footage. If required one of the 3 cameras can be used that have been charged for the following shift.

5.0 PROCEDURE

The following is guidance on the use of BWV when recording incidents;

5.1 How and when to use BWV

5.1.1 To connect the camera to the uniform, the magnet is pulled apart by placing fingers into the loops provided and rolled apart. Each part of the magnet is placed either side of the uniform, around the chest/shoulder area. The magnets snap together and are very secure. Please be careful when the magnets come together to prevent injury. If Cameras are fitted with clip attachment, Cameras can be secured on uniform using the crocodile clip where most comfortable.

5.1.2 The cameras are to be lifted from the docking stations turned upside down and the rear of the camera placed against the magnet connector. The camera is to be locked into place and rotated 180 degrees to secure the camera on the magnet.

5.1.3 The camera is ready to use but will be dormant until the side record button is turned on by the user. The user must clearly inform all persons present that they are recording for the safety of patients and staff.

5.1.4 The camera will remain recording until the user pushes the same side record button to turn the camera off. The user should inform all present that recording has stopped.

5.1.5 The camera can and should be used any time whereby the user feels unsafe, threatened, has or about to be assaulted. The cameras can also be used for incidents whereby the safety of patients are also at risk (i.e. a patient is threatening another patient, to protect a patient being searched by a staff member or an incident of self-harm.)

5.2 Recording an incident

5.2.1 The allocated member(s) of staff will wear a BWV device for the duration of their shift. The device will not be recording until activated.

5.2.2 The decision to record or not record any incident remains with the staff member wearing the device. The devices do not have to be used for violence and aggression only. They can be used at any time where the staff member or patient deems it necessary.

5.2.3 In cases where a patient requests that a member of staff records an interaction, staff should consider this request in the context of potentially being an indication of a developing incident.

5.2.4 Recording an interaction with a patient at their request may help to defuse the situation and provide some assurance to the patient that their concerns are being dealt with the patient's best interests in mind.

5.2.5 Start recording early: It is important to record as much of the incident as possible in order to secure the best possible overview; therefore recording should begin at the earliest opportunity.

5.3 Incident specific

5.3.1 Deployment of the BWC must be incident specific and therefore users should not indiscriminately record their day to day activities.

5.3.2 Inform: Patients will be informed about the use of BWCs via the Trust Web site, ward welcome packs, posters displayed on the wards and ward meetings. In addition to this at the commencement of any recording the users should, where practicable, make a verbal announcement to indicate why the recording has been activated.

5.3.3 If possible this should include: Date and Time; Location; Confirmation to those present that the incident is now being recorded using both video and audio.

5.3.4 If recording has commenced prior to arrival at the scene of an incident, the users should, as soon as is practicable, announce to those persons present at the incident that the recording is taking place and that actions and sounds are being recorded.

Users should use straightforward speech that can be easily understood by those present such as 'I am wearing a Body Worn Camera and recording this Incident'.

5.3.5 In so far as is practicable, users should restrict recording to areas and persons necessary in order to obtain evidence relating to the incident and should attempt to minimise collateral intrusion on those not involved. I.e. other service users not involved in the incident.

5.4 Privacy

5.4.1 During incidents in patient's rooms, bathrooms or toilets users may find that objections to recordings made with the BWC are voiced by the patient. In such circumstances, where the user feels that the recording is justified by the nature of the incident (for example an incident of serious self-harm or injury to others) they should continue to record and explain the reason(s) for this to the patient. Privacy and dignity should be taken into account as much as possible. Minimal use of BWC in such areas, or when patients are attending to personal care, to be used only when deemed necessary.

These may include:

- The BWC user's presence might be required to prevent further self-harm / injury to any person / property.
- Capturing the best evidence of incidents and the potential use of physical restraint in order to protect both staff and patients.
- Continuing to record would safeguard both parties with a true and accurate recording of any significant statement or action made by any party.

5.4.2 It is also acceptable for users to capture audio only footage in situations where staff consider this the most effective method to protect the privacy and dignity of the patient whilst maintaining safety for all (during the administration of intramuscular injection (IMI), searching or changing into anti-rip clothing). If audio only recordings are made, the users should clearly state the rationale for this.

5.5 Interruptions to Filming

Unless specific circumstances dictate otherwise recording must continue uninterrupted from the commencement of recording until the conclusion of the incident.

5.6 Concluding of filming

5.6.1 It is considered advisable that the users continues to record for a short period after the incident to clearly demonstrate to any subsequent viewer that the incident has concluded, the user has resumed other duties or activities and that the individual is in no physical distress. This is particularly important after the use of restraint, after administration of rapid tranquilisation and also if the patient has been secluded.

5.6.2 Users that have attended the incident from other areas will turn off their camera if instructed by the incident controller or when informed that their presence is no longer required at the incident.

Prior to concluding recording the user should make a verbal announcement to indicate the reason for ending the recording.

6.0 DATA

6.1 Uploading footage: At the end of the shift, the users will return the cameras to the designated station where the camera will be connected to the PC (or docking station) and signed back in by the user. Docking the camera will simultaneously charge the device and upload recorded footage to the secure site.

6.2 There is only one way that the camera can fit into the docking station so staff must ensure that they do not force the device into the docking station. Please ensure that the devices are fully pushed into the docking station, as if it is not the footage will not be downloaded.

6.3 Storing, reviewing and obtaining footage

6.3.1 All data captured will be stored on the providers secure system on the Trusts cloud storage. This has been reviewed by information governance for compliance with the GDPR and Information Governance requirements for the Trust. Data will not be linked to any specific patient record and will be stored in line with the following guidance

6.3.2 Footage will be marked for retention by either the VAPR Team as follows:

- Any footage linked to a Datix report will be retained and stored by the VAPR team for 99 years.

6.3.3 All Internal BWV footage requests should be in relation to one of the below departmental investigations. Requests should be made via CP28 Appendix 3a and sent to:-

- **Safeguarding – epunft.safeguarding@nhs.net**
- **Complaints – epunft.complaints@nhs.net**
- **Inquests – epunft.floandinquests@nhs.net**
- **HR – epunft.employeerelations@nhs.net**

6.3.4 All External requests for BWV footage must be sent to epunft.sar@nhs.net with a completed BWV request form – (CP28 Appendix 3)

6.3.5 Guidance on making a request can be found on CP28 Appendix 4 CCTV/BWV Flowchart.

6.3.6 Staff viewing footage should consider watching in pairs as material can be quite distressing.

6.4 Monitoring

This protocol is subject to the same monitoring / review arrangements as described in the CCTV policy (CP28)

The protocol will be reviewed as required, with a minimum of 3 yearly review, unless required before.

7.0 RETURN OF FAULTY OR BROKEN DEVICES

7.1 At all times, the body worn cameras remain the property of EPUT and are issued via the Trust VAPR team.

7.2 Each ward will have a docking station which contains and charges 4 cameras. Cameras should remain in the docking station unless being worn by a staff member. Two cameras are to be worn on a ward at a time; two should remain on charge and finalise downloading for the next shift.

7.3 Any breakages or damaged devices, should be reported via Datix and the VAPR team informed. The VAPR team will report and return the device to the provider for it to be repaired or replaced.

7.4 The VAPR Team will be able to provide a spare device whilst the ward device is replaced.

7.5 Staff are to ensure cameras are signed in and out on a booking form. Any losses of cameras could result in disciplinary action taken against staff members and the ward having to replace the device from their own budget.

8.0 MONITORING COMPLIANCE

8.1 It will be the VAPR Team's responsibility to monitor whether device usage is appropriate and in line with the usage requirements. The VAPR Team will liaise with staff and management to encourage regular usage.

8.2 The VAPR Team will also monitor and review material when required and share material with the legal team or staff as required.

8.3 If ward managers or Matrons require footage to be shared for training or investigation purposes they are to email the request with fully details to epunft.bwc@nhs.net

8.4 The VAPR Team will collate information and analyse data periodically.

9.0 GOVERNANCE REPORTING WITHIN THE TRUST

9.1 Body Worn Video will be a standing item on the agendas of Local Health and Safety Sub-Groups / Quality and Safety Sub-Groups. This will allow discussions and highlight any matters of concern or good practice.

9.2 The VAPR Team will report to the sub groups any good working practices as well as concerns to escalate regarding individual cases or areas of poor usage.

9.3 The minutes of the Health and Safety Sub-Groups / Quality and Safety Sub-Groups will be reported to the corporate Health, Safety and Security Sub-Committee, thus ensuring that there is Trust-wide monitoring and assurance in relation to the use and effectiveness of BWV as a health and safety measure, and as of an improved quality of care measure.

9.4 The minutes of the Health, Safety and Security Sub-Committee will be reported to the Quality Committee, the minutes of which will be reported to the Trust Board of Directors. As such, there is a clear governance route for monitoring through to Board level.

10.0 ADVICE AND GUIDANCE

10.1 Any queries in terms of use/issue of Body Worn Video and Trust protocols should be emailed to the dedicated email address of epunft.BWC@nhs.net or epunft.VAPR@nhs.net alternately, you can call the Trust VAPR Team via the Contact Centre.

10.2 Helpful documents and a training video can be found on the Intranet page;

https://input.eput.nhs.uk/TeamCentre/risk/sec/Pages/Body-Worn-Cameras.aspx

10.3 Should a query require more urgent advice, staff should contact the VAPR team or any member of the risk team by telephone who will direct them to the most appropriate point for advice.

Annex 1- BWC booking form (attached below)
Annex 2- BWC ward posters (attached below)

Annex 1

BODY WORN VIDEO BOOKING FORM				
Date	**Staff member/Role**	**Time Out**	**Time In**	**Camera recording/s made?**
21/8/2022	*Jane Doe/VAPR*	*08.05*	*18.20*	*Yes/No*

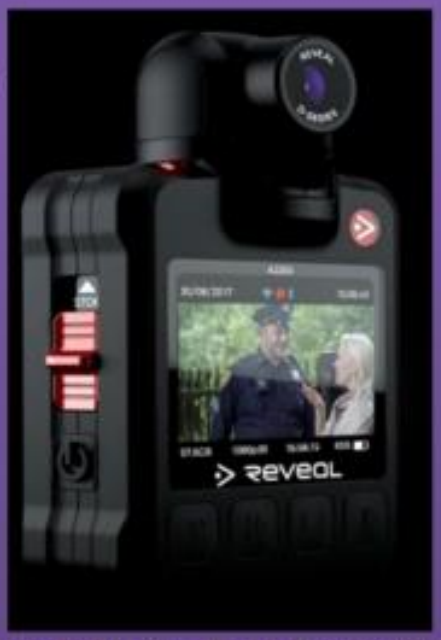
Annex 2

BODY WORN CAMERAS
EVERYBODY'S SAFETY MATTERS

NHS
Essex Partnership University
NHS Foundation Trust

We are now using Body Worn Cameras (BWC) in this ward location for the safety of patients and staff.

Staff who respond to incidents will be wearing small cameras which will be visible on their clothing.



These cameras record video and audio information, but only when activated by the wearer if staff believe that safety may be compromised when responding to incidents.

Staff wearing the cameras will clearly let people know when they begin any recording.

All recorded data will be processed in accordance with the Data Protection Act and General Data Protection Regulation.

Data will be stored for 60 days then securely deleted unless required for evidential purposes. This data will not be shared outside of the Trust without consent unless there is a lawful requirement.

For more information or to share your feedback please speak to the ward staff or contact the team below:

Local Security Management Specialist:
epunft.lsms@nhs.net

Information Governance Team:
epunft.info.gov@nhs.net

Data Protection Officer:
epunft.dpo@nhs.net

Further information can be found via
https://eput.nhs.uk/contact-us/your-health-records-information/

"I'm not just working, I'm working to improve lives"

SUBJECT ACCESS REQUEST FORM FOR CLOSED CIRCUIT TELEVISION (CCTV) AND BODY WORN VIDEO (BWV)
PLEASE USE BLOCK CAPITALS TO COMPLETE FORM

The General Data Protection Regulation 2016 and the Data Protection Act 2018 sets rules for processing personal information and allows you to find out what information about you is held. This includes images that are captured and recorded on CCTV or BWV. This is known as *the right of subject access.*

To enable the Essex Partnership University NHS Foundation Trust (the "Trust") to deal promptly with your request for access or obtain/receive copies of Closed Circuit Television or BWV media.

Please complete the form giving as much information as possible to support identification of the required information.

Under the terms of the Data Protection legislation, the Trust currently has 1 calendar month to comply with your request. The processing commences when your completed form is received by the Trust's Legal Dept., although the processing may be delayed if you have provided insufficient details.

Please complete below where applicable

DATA REQUESTOR DETAILS
Full Name:
Job Title:
PC Rank :
Collar No:
Station Details:
Crime Incident Number:
Contact Number/s:
Contact Email:

REASONS FOR ACCESS –Please give brief explanation below

I confirm that the data requested is needed for the above purposes and failure to provide the information will in my view be likely to prejudice those matters. ☐

POLICE REQUESTS ONLY
I am making enquiries which are concerned with: ☐ 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. ***"Check mark as* is *appropriate***

ADDITIONAL DETAILS	
In order for Essex Partnership University NHS Foundation Trust to locate the required information, all applicants must give a full and accurate description of the times, date and location of their presence on the CCTV/BWV system. If incomplete or inaccurate information is provided, the Trust may be entitled to refuse the Subject Access Request	
Location - Site name and Ward (please be as accurate as possible).	
Date and time at specified location (please specify within a 30 minute time band)	
Is this linked to a specific incident?	Yes / No
Description and colour of clothing worn	

.

Supply of Information

You have a right, subject to certain exceptions, to receive a copy of the CCTV/BWV images in a permanent form. However, viewing CCTV/BWV images at Trust premises will often be easier and quicker.

It should be noted that any CCTV/BWV images received **must not** be broadcast, replayed, copied or sold without the express permission of Essex Partnership University NHS Foundation Trust.

Do you wish to:

Only view the images **YES/NO** (please delete)

View and receive a permanent copy **YES/NO** (please delete)

Declaration – Data Subject declaration

In exercise of the right granted to me under the provisions of the General Data Protection Regulation 2016 and the Data Protection Act 2018 I request that you provide me with the information requested as indicated above.

I understand that it may be necessary for Essex Partnership University NHS Foundation Trust to obtain more detailed information in order to be satisfied as to my/the data subject's identify or locate my/the data subject's personal data.

Signed---------- **Dated**----------

Declaration by person(s) acting on behalf of the data subject.

I confirm that the information supplied in this application is correct and I am acting on behalf of the data subject and enclose proof of my authority to do so.

I understand that it may be necessary for Essex Partnership University NHS Foundation Trust to obtain more detailed information in order to be satisfied as to my/the data subject's identify or locate my/the data subject's personal data.

Name / Company ----------

Address----------

Post code ---------- Telephone No. ----------

Fax No. ---------- Email Address----------

Signed ---------- Dated----------

POLICE REQUESTS ONLY:

Countersignature: ……..
Name: ……..
Rank: ……..

Please note: a person who impersonates or attempts to impersonate another may be guilty of an offence.

Check box: Before returning this application form, please check:

1. **Have you completed all relevant sections in this form?**
2. **Have you signed and dated the declaration?**
3. **Have you enclosed proof of authority to act on behalf of the data subject, (if applicable)?**
4. **Please send all requests for CCTV/BWV to epunft.sar@nhs.net**

SUBJECT ACCESS REQUEST FORM FOR CLOSED CIRCUIT TELEVISION (CCTV) AND BODY WORN VIDEO (BWV)
PLEASE USE BLOCK CAPITALS TO COMPLETE FORM

The General Data Protection Regulation 2016 and the Data Protection Act 2018 sets rules for processing personal information and allows you to find out what information about you is held. This includes images that are captured and recorded on CCTV or BWV. This is known as *the right of subject access.*

To enable the Essex Partnership University NHS Foundation Trust (the "Trust") to deal promptly with your request for access or obtain/receive copies of Closed Circuit Television or BWV media.

Please complete the form giving as much information as possible to support identification of the required information.

Under the terms of the Data Protection legislation, the Trust currently has 1 calendar month to comply with your request. The processing commences when your completed form is received by the Trust's Legal Dept., although the processing may be delayed if you have provided insufficient details.

Please complete below where applicable

DATA REQUESTOR DETAILS
Full Name:
Job Title:
Datix Number:
Contact Number/s:
Contact Email:

REASONS FOR ACCESS – Please give brief explanation below

I confirm that the data requested is needed for the above purposes and failure to provide the information will in my view be likely to prejudice those matters. ☐

ADDITIONAL DETAILS	
In order for Essex Partnership University NHS Foundation Trust to locate the required information, all applicants must give a full and accurate description of the times, date and location of their presence on the CCTV/BWV system. If incomplete or inaccurate information is provided, the Trust may be entitled to refuse the Subject Access Request	
Location - Site name and Ward (please be as accurate as possible).	
Date and time at specified location (please specify within a 30 minute time band)	
Is this linked to a specific incident?	Yes / No
Description and colour of clothing worn	

.

Supply of Information

You have a right, subject to certain exceptions, to receive a copy of the CCTV/BWV images in a permanent form. However, viewing CCTV/BWV images at Trust premises will often be easier and quicker.

It should be noted that any CCTV/BWV images received **must not** be broadcast, replayed, copied or sold without the express permission of Essex Partnership University NHS Foundation Trust.

Upon request with complete information - Footage will be placed into secured shared files with limited access.

Declaration – Data Subject declaration
In exercise of the right granted to me under the provisions of the General Data Protection Regulation 2016 and the Data Protection Act 2018 I request that you provide me with the information requested as indicated above. I understand that it may be necessary for Essex Partnership University NHS Foundation Trust to obtain more detailed information in order to be satisfied as to my/the data subject's identify or locate my/the data subject's personal data. **Signed----------** **Dated----------**

Check box: Before returning this application form, please check:

1. **Have you completed all relevant sections in this form?**
2. **Have you signed and dated the declaration?**
3. **Please send all Internal staff requests for CCTV/BWV to the relevant investigating department addresses below:-**

    - **Safeguarding – epunft.safeguarding@nhs.net**
    - **Complaints – epunft.complaints@nhs.net**
    - **Inquests – epunft.floandinquests@nhs.net**
    - **HR – epunft.employeerelations@nhs.net**

Essex Partnership University NHS Foundation Trust

Access to CCTV / BWV flowchart

Access to footage required for **Internal Staff investigation e.g. (HR / Safeguarding / Complaints / Inquests)**

Access to footage required for Non-Staff Request (Police / Insurers / 3rd Parties) to view or obtain copies of images / footage

CCTV and BWC requests should be made on a data protection form to be sent to

Safeguarding – epunft.safeguarding@nhs.net
Complaints – epunft.complaints@nhs.net
Inquests – epunft.floandinquests@nhs.net
HR – epunft.employeerelations@nhs.net

CCTV and BWC requests should be made on a data protection form to be sent to:

epunft.sar@nhs.net

On receipt of request the CCTV/BWV request form (CP28 Appendix 1) will be sent to the requestor to complete where applicable

Completed form to be returned to epunft.CCTV@nhs.net or epunft.bwc@nhs.net

(Within 21 days of the incident)

Internal Requests

CCTV will be processed by EPUT CCTV Team

BWC will be processed by EPUT BWC Team

External Requests

Will be sent to EPUT Legal Team to review and authorise

Compliance & Security Officer or the BWC co-ordinator will liaise with requestor on sharing method

Appropriate release or refusal of request will be facilitated by EPUT Legal Team. Communication sent to requestor

CCTV/ BWC emergency out of hours contact numbers

Contact via Contact Centre 0300 123 0808

Essex Partnership University
NHS Foundation Trust

CP28 – Surveillance Systems Policy incl. (CCTV) (BWV)

POLICY REFERENCE NUMBER:	CP28
VERSION NUMBER:	3.1
KEY CHANGES FROM PREVIOUS VERSION	Additional bullet point under s6.1; Appendix 3 split into Appendix 3 & 3a to provide forms for External and Internal requests
AUTHOR:	Compliance and Security Officer / Violence/Abuse Prevention and Reduction Advisor
CONSULTATION GROUPS:	HSSC/DPO/Information Governance
IMPLEMENTATION DATE:	June 2018
AMENDMENT DATE(S):	May 2020; August 2021; August 2022; April 2023
LAST REVIEW DATE:	August 2022
NEXT REVIEW DATE:	August 2025
APPROVAL BY HEALTH, SAFETY & SECURITY SUB-COMMITTEE:	July 2022
RATIFICATION BY QUALITY COMMITTEE:	August 2022
COPYRIGHT	2018-2023

POLICY SUMMARY
The purpose of this policy is to ensure employees of Essex Partnership University NHS Foundation Trust are provided with clear guidance on the regulation, management and use of Surveillance Systems throughout its premises

The Trust monitors the implementation of and compliance with this policy in the following ways:
This Policy is monitored through the Trust Health, Safety and Security Committee.

SERVICES	**APPLICABLE**	**COMMENTS**
TRUSTWIDE	✓	

THE DIRECTOR RESPONSIBLE FOR MONITORING AND REVIEWING THIS POLICY IS EXECUTIVE CHIEF FINANCE OFFICER

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

SURVEILLANCE SYSTEMS POLICY

CONTENTS

THIS IS AN INTERACTIVE CONTENTS LIST – PLEASE CLICK ON THE SECTION HEADINGS TO GO TO THE SECTIONS

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

SURVEILLANCE SYSTEMS POLICY

1.0 INTRODUCTION

1.1 This policy and associated protocol guidance sets out the responsibilities and processes to be followed in relation to the installation and management of all surveillance systems at Essex Partnership University NHS Foundation Trust sites.

1.2 This document has been written in accordance with and adheres to the principles of the General Data Protection Regulation 2016 and the Data Protection Act 2018, Human Rights Act (1998) and follows guidance from - A data protection code of practice for surveillance cameras and personal information (2017)

Essex Partnership University NHS Foundation Trust is registered with the ICO – Ref: **ZA242481**.

1.3 The purpose of this policy is to ensure that:

- Any Surveillance systems installed are justified, appropriately managed and not open to abuse or misuse.
- Correct data privacy impact assessments are made in relation to the need for any Surveillance system.
- Standards are applied to ensure schemes are valid.
- Surveillance is appropriately installed, maintained and managed.
- Responsibility for the management of Surveillance systems is identified at both local and Trust wide level.
- Access, storage and disclosure of images are in accordance with the principles of the General Data Protection Regulations 2016 and the Data Protection Act 2018 and with Trust policy on data sharing.

2.0 SCOPE

2.1 This policy and its procedural guidance is binding on all employees of the Trust and applies also to other persons who may, from time to time, and for whatever purpose, be present on Trust premises.

2.2 This policy is also intended to cover service areas of the Trust where activities are carried out, including those properties not owned but used by the Trust.

2.3 Any data stored on removable drives, including CD's, DVD's, Memory sticks or hard drives are also deemed to be part of the CCTV system and will therefore be covered by the content of this policy.

2.4 This policy refers only to overt surveillance only.

2.5 "Covert Surveillance" is where surveillance systems may be hidden or placed discreetly and may be used in sensitive investigations where on going problems occur within specific areas. If it is thought that covert surveillance is required the CSO and or VAPR Advisor must be consulted who will seek guidance from the Police on an appropriate course of action. Covert surveillance is not permitted within the Trust without legal RIPA (Regulation of Investigating Powers Act 2000) authorisation from the Police and the consent of the Trust Chief Executive.

2.6 Exclusions to this Policy include equipment incorporating Oxehealth Systems.

3.0 DEFINITIONS

3.1 The following definitions will apply to this policy:

- The "Trust" - Essex Partnership University NHS Foundation Trust.
- Surveillance systems refer to closed circuit television (CCTV) (BWV) body worn video.
- 'Scheme/System' - Any of the Trust's surveillance systems schemes (a systematic plan for a course of action)
- VAPR Advisor – Violence/Abuse Prevention and Reduction Advisor with managerial responsibility for all BWV and knowledge of relevant procedures.
- CSO – Compliance & Security Officer who has managerial responsibility for all Trust CCTV systems and knowledge of installations/functionality and relevant procedures.
- Data Protection Officer- is the Associate Director of Electronic Systems and Information Governance.
- Data Controller – Decides what is to be recorded, how the information should be used and to whom it may be disclosed.
- Data Managers - Individuals with responsibility for localised system management i.e. Access to reviewing of, efficient reporting of failure/outages, informing data Controller of site changes affecting any surveillance system via DPIA (Data privacy impact assessment).

3.2 The systems may capture images, where individuals (subjects) or their vehicle registrations can be identified. Under the General Data Protection Regulations 2016 this is deemed personal data.

4.0 RESPONSIBILITIES

4.1 The Trust Board of Directors has overall responsibility for ensuring the principles of this policy and procedures and other associated policies are implemented across the organisation. The duty of ensuring all measures needed to implement this policy and associated procedural guidelines is delegated to Directors within their areas of responsibility.

4.2 The Trust Board of Directors is fully committed to a culture of providing high quality healthcare and improving patient/staff and all relevant people's safety.

4.3 The Director of ITT will ensure:

- Network availability for the use of surveillance systems across the Trust
- Where possible to accommodate storage systems within Comm's cabinets utilising the UPS.
- The provision and support of obtaining IP address details (subnet mask/Default gateway) to enable surveillance systems to be connected to the Trust network.
- CSO/VAPR Advisor are included in discussions relating to reconfigurations of communication rooms at sites where surveillance systems are in operation to allow for safer storage and resilience of hardware.
- Provide ad-hoc technical support.

4.4 Directors and Senior Management will have responsibility within their own service area for;

- Monitoring the implementation of this policy via supervision.
- Be able to evidence that EPUT policies and procedures have been followed during any level of investigation.

4.5 Capital development and all site refurbishment project design must incorporate the appropriateness of surveillance systems installation by involving the CSO at the earliest stage.

4.6 CSO and VAPR Advisor have designated responsibilities in the assessment of any surveillance system scheme implemented and on-going responsibilities in relation to the operation and management of any scheme. These are detailed in the procedural guidance. This is to include the completion of a data privacy impact assessment (DPIA); an evaluation of proportionality and necessity. DPIA's must be reviewed by the Information Governance team and the views and advice of the Data Protection Officer sought.

4.7 The CSO/VAPR Advisor are identified as the data managers with authority for the following:

- Security and storage of data.
- Security clearance of persons (staff/contractors and all relevant people's) who have experience/competence to use the system appropriately for immediate review of time sensitive footage.
- Retrieval where appropriate of data in line with section 6.1
- Destruction of data specifically relating to internal systems within their own responsibility in line with retention guidelines.
- Overarching design and control of installations and directing competent contractors to provide maintenance and remedial actions.
- Liaison with ITT to resolve conversion and codec issues with playback of recorded footage for investigation.
- Liaison with law enforcement agencies and other requesting parties; relating coverage and potential/likelihood of capturing requested incident.
- In conjunction with respective Information Governance team or DPO, responsible for identifying non-compliance with the British Standard

and/or legislation, operational procedures and breaches of confidentiality including unauthorised sharing of data.

4.8 Where any surveillance system impacts on service users, staff and members of the public - Data Managers, where identified as the nominated contact point, will:

- Ensure the procedures and principles detailed within this policy and associated procedural guidance are followed and monitored to meet all relevant guidance.

4.9 Individuals working with or utilising any surveillance system:-

- Have an understanding of the **Surveillance Systems Policy**, procedures and local protocols.
- Implement those areas of this policy and procedural guidance that falls within their work remit.
- Identify any use of surveillance systems that may result in a breach of this policy

4.10 All faults identified for **CCTV** Camera's must be reported to the Estates Helpdesk or via 3i online portal. All faults for Body worn camera's to be reported to VAPR Advisor team (Refer to relevant protocols).

4.11 A Datix must be raised if there are any learning or safety concerns identified from the footage. If a staff member reviews any footage in which the content raises concerns about practice or safety etc. then this requires immediate escalation to the Trust Safeguarding team and/or the Director of Service; this must be done immediately.

5.0 OWNERSHIP AND OPERATION OF SURVEILLANCE SYSTEM SCHEMES

5.1 The majority of Surveillance Systems are owned and operated by the Trust. Equipment and processes are managed via the Estates and Facilities/Legal/VAPR Advisor /Information Governance teams. Maintenance is carried out by approved 3rd party contractors in line with current standards.

5.2 Where the Trust occupation is under a lease arrangement and the CCTV system is owned/controlled by a landlord, incorporating Private Finance Initiative (PFI). The compliance with statutory duties is their responsibility and the Trust is required to ensure information sharing agreements are in place between both organisations. If the system owner has not taken steps to inform visitors that the system is in place, we retain a duty to inform our visitors and staff that CCTV is in place.

5.3 Responsibility for the review, assessment and installation of all relevant surveillance systems, data collection and control of images is delegated to the CSO/VAPR Advisor.

5.4 All Surveillance systems must offer the capability for efficient reviewing of footage to support incident investigation. All Trust owned systems must be part of the Trust IT network for remote access by the CSO/VAPR Advisor or other trained persons.

5.5 To support the retention of valuable data and the ability to provide observation of high risk environments, the recordable Surveillance systems must be attached to a UPS (uninterrupted power supply) whether by a standalone unit or as part of a sites IT infrastructure.

5.6 Signage must be displayed on all sites with recordable Surveillance systems. The standardised signage identifying the contact point to request access to footage and the reasons for installation must be located on the approach to enter a building (potentially multiple access points). It is also good practice to have Surveillance signage within areas of a site where service user capacity had not been assessed when initially entering the site e.g. via 136.

5.7 Whilst a retention period of 31 days is often quoted, retention periods are not mandated in law. The legal definition is for as long as necessary for the purpose. The Trusts' portfolio of Surveillance systems is diverse and retention periods vary dependent upon the capacity of the technology. However the Trust attempts to fulfil a minimum of 31 days.

5.8 Under section 19 of the Police and Criminal Evidence Act 1984 the Police have the power to seize hardware where information/data is stored in support of their investigations.

6.0 PURPOSES

6.1 Surveillance systems across the Trust property portfolio are in place for the below purposes:-

- Quality patient care/safety.
- Protection of patient's staff and visitors.
- Protection of Trust property and assets.
- To support Police in identifying, apprehending and prosecuting offenders.
- To reduce incidents of violence and aggression.
- To increase personal safety and reduction of fear.
- Internal and External investigations.

For these reasons the information processed may include visual images of people and their behaviours. This information may be about staff, service users and general public including offenders and suspected offenders. Where necessary or required this information is shared with the data subjects themselves, employees, services providers, police forces, security organisations and persons making an enquiry.

6.2 Data Protection issues:

- All schemes will be operated fairly and lawfully in accordance with the principles of the General Data Protection Regulation 2016; Data Protection Act 2018; Human Rights Act (1998); Protection of Freedoms Act 2012 and only for the defined purpose set out in Section 6.1.
- All schemes will be operated with due consideration for the privacy of individuals.
- All Trust Surveillance systems are to be registered with the Information Governance Manager via Data privacy impact assessments.
- Any change to the purpose for which any scheme is operated (Section 6.1) will require the prior approval of the CSO/VAPR Advisor and consultation with the Trusts Data Protection Officer and Information Governance team.

6.3 Effective records of installations should exist, including locations of cameras and hardware along with installation date, projected lifespan of internal hard drives and basic system specification maintained by CSO.

7.0 BREACHES OF THIS POLICY

7.1 The Trust reserves the right to take appropriate disciplinary action against any employee who breaches this policy in accordance with the Trust's disciplinary procedures.

7.2 As a major purpose of these schemes is in assisting to safeguard the health and safety of staff, patients, and visitors, it should be noted that intentional or reckless damage of any Trust Surveillance Systems may be a criminal offence and will be regarded as a serious breach of Trust policy and subject to disciplinary procedures.

8.0 COMPLAINTS PROCEDURE

8.1 Data subjects who feel they may have grievances and complaints concerning the operation of the Trust's Surveillance systems management can contact the Information Governance Team or the Data Protection Officer via EPUT Intranet.

8.2 If the data subject is not satisfied with the response, he/she may contact the Information Commissioner's Office.

9.0 IMPLEMENTATION OF POLICY

9.1 This policy will be disseminated across the organisation through the Trust Intranet site.

10.0 REFERENCES

10.1 Other related policies include:

- Data Protection & Confidentiality Policy / Procedures
- Security Policy RM09
- Restrictive Practice Policy RM05
- In-Patient Observation Policy CLP8
- Missing Patient Policy CLP34
- Freedom of Information Policy / Procedures CP25
- Information Governance & Security Policy / Procedures CP50
- Information Sharing & Consent Policy /Procedures CP60
- Criminal Behaviour within a Health Environment (Zero Tolerance) Policy CP22

(This list is not exhaustive)

10.2 Related Legislation and Publications:

- Data Protection Act 2018
- Protection of Freedoms Act 2012
- The CCTV Code of Practice produced by the Information Commissioner
- The CCTV Code of Practice revised edition 2016
- General Data Protection Regulation
- The Human Rights Act 1998
- The Regulation of Investigatory Powers Act 2000
- Caldicott Report 1997
- Health and Safety at Work Act 1974
- Police and Criminal Evidence Act 1984

(This list is not exhaustive)

11.0 REVIEW OF THIS POLICY

11.1 This policy and associated protocol's, its implementation and the operation of the Trust's Surveillance systems schemes, will be reviewed by the CSO and or VAPR Advisor in conjunction with the Information Governance Manager, Legal team every three years or as required during that period before review.

END