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

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 [redacted]t or the VAPR team on [redacted]

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 –** [redacted]
- **Complaints –** [redacted]t
- **Inquests –** [redacted]
- **HR –** [redacted]

6.3.4 All External requests for BWV footage must be sent to [redacted] 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 [redacted]

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 a n d 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 [redacted] or [redacted] 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;

[redacted]

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*

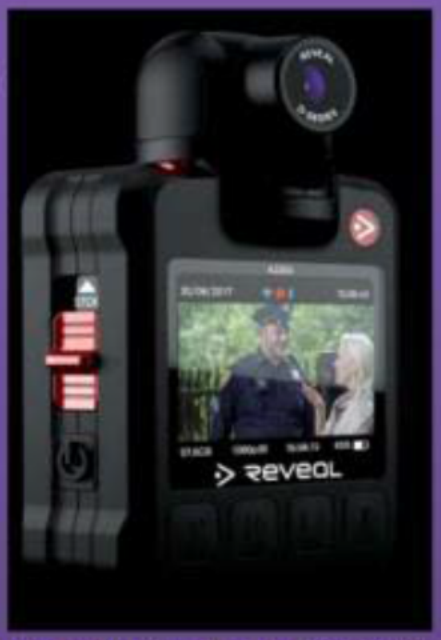
Annex 2

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: [redacted]

Information Governance Team: [redacted]

Data Protection Officer: [redacted]

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"

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 – [redacted]
Complaints – [redacted]
Inquests – [redacted]
HR – [redacted]

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

[redacted]

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

[redacted] [redacted]

(Within 21 days of the incident)

Internal Requests

CCTV will be processed by EPUT CCTV Team

BWC will be processed by EPUT BWC Team

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

External Requests

Will be sent to EPUT Legal Team to review and authorise

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

Data Protection (Privacy) Impact Assessment (DPIA) Form

The Essex Partnership University NHS Foundation Trust's (EPUT) data processing activity MUST comply with the (UK) General Data Protection Regulation/Data Protection Act (2018).

This (Stage 1) Section of the Data Protection Impact Assessment will provide guidance for evaluating whether a full scale DPIA should be conducted. This form will assist Information Asset Owners in identifying how the collection of people's personal information may affect their privacy.
In this evaluation process you are required to answer the following set of screening questions relating to the key characteristics of the project and the system that the project will deliver. Answers to the questions need to be considered as a whole, in order to determine whether the overall impact and related risk warrant a full scale DPIA (Stage 2).

***DPIA Ref Number:**	**DPIA148**
Name of Project:	**Body-Cameras Roll Out**
Proposed Implementation Date:	01.12.2021
Name of Person Completing DPIA:	[redacted]
Contact Details:	[redacted]
Date of Completion:	**October 2021**

**This will be entered by the IG Team*

If you have any questions or would like any help in completing this document please contact the IG Team at epunft.info.gov@nhs.net

Stage 1 – Screening Questions

Screening Question	Response (Yes/No)	Rationale
Will the project involve the collection of new information about data subjects?	☒ Yes ☐ No	The project will be used to collect data via the means of video footage, which will be stored for one month on a cloud storage system. The recording can then be used

		for evidential or trust employment purposes.
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	☒ Yes ☐ No	**The below organisations will only receive data under a legal obligation:** Essex Police (and any other police forces that the Trust may incidentally interact with, such as Suffolk or Metropolitan) Essex Acute Hospital Trusts (Mid-Essex Hospitals, Basildon & Thurrock University Hospital, Southend Hospital, Princess Alexandra Hospital, Colchester Hospital (ESNEFT) Neighbouring Mental Health Trusts (Norfolk & Suffolk, ELFT, NELFT, Herts) NHS England Crown Prosecution Service Court service On rare occasions footage may be released via the Communications Team (with appropriate Legal /IG permissions) to the media in order to reduce the risk of harm to members of the public.
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	☐ Yes ☒ No	The information will be used for evidential purposes both internally (EPUT) and externally (Police, Criminal Justice and those with legal obligations).
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	☒ Yes ☐ No	The footage recorded will be used for evidence if required. This could lead to disciplinary actions by EPUT or alternate care arrangements.
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.	☐ Yes ☒ No	No. The information will be confidential and in accordance with EPUT privacy/confidentiality policies

Does the project involve you using new technology which might be perceived as being privacy intrusive i.e. the use of cookies (a software application) to download personal information whilst using the software / mobile devices to record conversations?	☒ Yes ☐ No	The project includes the roll-out and use of body worn cameras in EPUT wards. The cameras will only be activated when there is a requirement for their use. Audio and visual footage will be recorded, with the only intrusive consideration coming from service users.
Has consent been gained from the individual and appropriately recorded for future reference?	☒ Yes ☐ No	Service users will be advised that body-worn camera imagery and audio may be captured when users deem it appropriate to do so in ward meetings, MDTs, and via posters displayed on the wards. Body-worn cameras should also be referenced in ward welcome packs. Service users will be advised that a body-worn camera will be activated prior to activation in order to record an incident and will be informed again once recording is active. It is important to note that in principle there is no requirement to obtain the express consent of the person or persons being filmed since the actions of the camera operator are deemed to be lawful. The Operations staff will make the decision on a case-by-case basis whether to switch on the device to record. The individual(s) on scene will be shown the device and informed verbally that recording is in progress – there will be no covert recording. The BWV SOP details what should be done if people object to be recorded or if they ask for an event to be recorded and when they

		should stop recording. Equally, staff may have to justify not recording in any particular circumstance.
Is it essential the data remains identifiable?	☒ Yes ☐ No	All images and audio will be time-stamped and non-modifiable following capture, other than flagging for retention for either evidential or safety purposes. All footage is encrypted and cannot be edited prior to upload. All images and audio will be securely stored on the Microsoft Azure cloud. Access will be restricted, and changes tracked
Will the data be used for research?	☒ Yes ☐ No	Data could be used for research purposes, for studies of behavioural patterns and trends.

If you have answered "Yes" to any of the above, please continue on to Stage 2.
If you have answered "No" to all of the above questions, then please sign the Sign-off and Approval page and send to the IG team.

Stage 2 – Full Data Privacy Impact Assessment

This stage should be completed if you answered "Yes" to any of the questions above or if it is clear that a Full DPIA is required from the outset.

2.1 Project Aim & Objective?

The project scoping document can be used here, it's a good idea to link/ embed the document.
You should explain the project objectives/purpose, benefits to organisation, and any other parties, such as the data subjects (those individuals who you will be collecting information about).
You should be able to summarise the reason for the DPIA here.

Objectives of using BWV:

- To protect staff, patients and visitors
- To protect staff premises and Trust assets
- To increase personal safety and reduce the fear of crime
- To reduce incidents of violence and aggression to staff members
- To support the Police in reducing and detecting crime
- To assist in identifying, apprehending and prosecuting offenders
- To provide a deterrent effect and reduce criminal activity
- To assist in quality patient care
- To assist service level research to ensure delivery of quality patient care and safety in line with Trust policy and procedures and professional regulations

Operational staff will only deploy BWV technology against the defined operational requirements (where there is risk of violence, aggression or assault potential criminal acts against staff and or the Trust) and ensure that the use is proportionate, legitimate, necessary and justifiable. In addition, it will ensure that the use satisfies the requirement of addressing a pressing staff and patient safety need described in the Trust Surveillance Camera Policy, the assignment instructions and NHS England and NHS improvement advice and guidance.

At all stages it will comply with the Data Protection Act, Health & Safety at Work Act (Duty of Care) and PACE legislation. In the case of the Human Rights Act 1998, there will be adherence to the requirements of Article 6 (Right to a fair trial) and in respect of Article 8 (Right to respect for private and family life, home and correspondence) since this is a qualified right, information will only be captured and processed to achieve a legitimate aim as detailed earlier. It is important to note that in principle there is no requirement to obtain the express consent of the person or persons being filmed since the actions of the Operations staff are deemed to be lawful.

The Trust has established the need for the use of cameras that are capable of capturing both moving images and audio information which are worn by uniformed Operational staff for the purposes described above.
Further use of BWV will require separate DPIAs to be carried out.

BWV acts as a deterrent and encourages compliance through self-awareness.
- Supports de-escalation of violence.
- Safety of staff by reducing verbal and physical attacks.
- Contribute to the transparency of security procedures.
- Provision of verifiable recordings with timestamp & support statements.
- Saving lengthy descriptive reports having to be provided.
- Footage is readily acceptable by courts and CPS.

- Acceleration of judicial process by encouraging early guilty pleas.
- A reduction in complaints against staff.
- BWV should reduce absenteeism by supporting with all the above.
- A tangible contribution to efficient workflow and cost savings.

Prior to any activation subjects and persons in the immediate vicinity will be informed of the activation by the Operations staff.
Immediately on the unit being turned on they will again be informed of its activation.
Any non-evidential material is retained for 30 days.
This material is restricted and cannot be disclosed to third parties without the express authority of the subject of the recording unless prescribed by law.
Recorded material is Trust information and it can be accessed on request in writing in accordance with the Data Protection Act, unless an exemption applies in the circumstances.
The BWV operator will decide on a case-by-case basis when and when not to switch the BWV on or off. There should always be a presumption to record if the 'need to address a pressing staff/patient safety need' has been achieved unless the circumstances dictate otherwise.

Based on the above, the following categories of members of the public are likely to have their contact recorded:

- Witnesses of lawful activities.
- Witnesses of crimes, or those who witness other parties verbally or physically abusing Trust staff as they discharge their duties.
- Persons suspected of committing offences.

In addition, persons, unrelated to any specific interaction between Trust staff and any of the categories of persons above, might find their activities captured on a BWV device. To some degree, this is inevitable since a camera lens or microphone is non-discriminatory and captures whatever is within its vicinity. They will adopt a number of safeguards to firstly avoid this occurrence where possible and to ensure that the data is held securely until it is no longer required.
As previously mentioned, BWV is capable of capturing primary evidence in such a way that it is able to bring a compelling and an indisputable account of an incident. It will considerably reduce ambiguity. It will not replace the need to capture other types of evidence but should be considered as an additional tool.
BWV will not be routinely recording and monitoring all activity, the always on approach.
To do so would fundamentally breach the privacy of large numbers of members of the public, who are going about their private business, as well as to a degree the privacy of Trust staff going about their work. This cannot be justified from the perspective of proportionality and legitimacy.
Added to this, is that current technology is incapable of operating in such a way principally due to a lack of suitable and sustainable battery life. In addition, such a practice would require the storing, reviewing and then disposal of large quantities of data.

In every case where the BWV is activated, the staff member involved must be prepared to justify its use.

All images from BWV have the potential for use in court proceedings whether they provide information that is beneficial to the prosecution or defence.
The information will be safeguarded by an audit trail in the same way as other evidence that is retained for court. It must be emphasised that BWV can collect valuable evidence for use in criminal prosecutions, ensure the Trust acts with integrity and transparency and potentially provides objective evidence of controversial events. It offers protection for both citizens and the Trust.
However, this justification may be closely scrutinised by a court and it is essential that BWV recordings will not retained where there is no clear evidence of an offence, unless some other good reason exists for their retention.

EPUT Privacy Policy covers the use of body worn devices - Privacy Policy | EPUT

2.2 Information Flows/Processing of Information

Any suggested collection, purpose and volume of Person Identifiable Information (PII) should be recorded here.
If a Data Flow Mapping exercise has been completed this should be linked here and the information below should provide a summary of those maps:

Whom is the Information processed about? (please tick √ all the related options)	x	**Employees**	
	x	**Patients**	
	x	**Students**	
	x	**Agency Staff/Volunteers**	
	x	**Partner Businesses or Organisations**	
	x	**Other**	**Parent of Child plus details of any other proxy access granted by parent.**
What are the Data Classes that will be held or processed as part of the implementation or change? (please tick √ all the related options) (When data is processed,interpreted, organised, structured or presented so as to make them meaningful or useful, it is called information.)	x	**Person sensitive details** (name, address, postcode, date of birth, NHS number, Gender, GP Practice, Consultant, Third Party Relationships, Email Address, IP address – *please delete as appropriate*)	
		Family, lifestyle and social circumstances (marital status, housing, travel, leisure activities, membership of charities – *please delete as appropriate*)	
		Education and training details (qualifications or certifications, training records)	
		Employment details (career history, recruitment and termination details, attendance	

		details, appraisals, other – *please delete as appropriate*)
		Financial details (income, salary, assets, investments, payments, other – *please delete as appropriate*)
	x	**Criminal proceedings, outcomes and sentences**
		Goods or services (contracts, licenses, agreements etc.)
		Goods or services (contracts, licenses, agreements etc.)
		Religious or other beliefs of a similar nature
		Political opinions
	x	**Physical or mental health conditions**
	x	**Offences including alleged offences**
		Sexual health
		Trade Union membership
		Other
How will the information be collected and transferred to the organisation?	**Collection**: Body Worn Video (BVW) equipment consists of a small camera attached to the uniform of Operations staff which record visual and sound data. The purpose of the recording is to safeguard staff, patients and the public during violent and aggressive or anti-social behaviour incidents. The footage will be in an encrypted format, securely stored and only viewed by authorised persons. **Use**: The devices will only be activated during an incident and continuous recording is strictly not permitted. **Store and deletion**: Visual and sound recordings will reside on the device until it is 'docked'. Once docked, the RFID card must be used to access the recording and enable it to be sent to the server. They will remove the recording from the device. Once the recording is on the server, it will automatically be deleted after 30 days unless transferred from the server.	

	Stored online in secure Microsoft Azure cloud account. Data is regularly backed up Access controlled through permissions and user roles with only authorized users able to view or share videos
Who will have access the information?	Authorised EPUT staff will have access to the data. Access to the system is controlled via the LSMS team. All user activity (viewing, deleting of videos) is recorded and logged within the application.
Where will the information be held?	☐ On paper ☒ On a database saved on a network folder/drive ☒ external Website / system ☐ On a dedicated system saved to NHS network ☐ Other – please state below:
What will the information be used for?	To protect staff, patients and visitors To increase personal safety and reduce the fear of crime
What are the retention periods for this data? (please refer to the NHS Code of Practice Records Management) **How will it be destroyed/deleted?**	30 days for Body-Worn Camera footage 3 years for footage deemed of evidential value (footage has to be flagged for retention) 10 years for footage deemed of safety value (footage has to be flagged for retention) Data that is deemed suitable for deletion will be confirmed by the EPUT LSMS and I.T Departments and erased from the server (see below).
Will the Information be shared with anyone else? If so Who?	☒ Yes ☐ No Please provide details: Any external agency requesting copy of the data will have to apply through the EPUT legal team via a data protection SAR's process (The same process for CCTV)
Does this Project/ Initiative involve the use of a System Supplier? If so please provide	☒ Yes ☐ No Please provide details:

details.	Reveal Media Ltd products and services [redacted]
How will the data be kept up to date and checked for accuracy and completeness?	The software will receive updates from the System Supplier – Reveal Media Ltd. Accuracy and completeness checks will be conducted by senior ward personnel, LSMS and I.T Departments (when required).
Will any data be transferred outside the organisation premises or systems	☐ Yes ☒ No Please provide details: Held by the Trust for 30 days then deleted unless identified incident occurs. ☐ Yes –Within the European Economic Area (EEA) ☐ Yes –Outside the European Economic Area (international) Please name the country:
Does this include back-up or server arrangements?	☒ Yes ☐ No Stored online in secure Microsoft Azure cloud account. Data is regularly backed up as part of the hosted service. This is not managed by EPUT IT.
Is there a contingency plan / backup policy in place to manage the effect of an unforeseen event?	☐ Yes ☒ No Please provide details: N/A if Cameras do not work.
If personal, sensitive or business sensitive data is being processed by the system, has this been added to the relevant Data Flow Mapping document?	☐ Yes ☒ No Please provide details: To be added to the next DFM request from the team once project is approved.
Attach Data Flow Mapping Spreadsheet here if you have completed this	

2.0 Legal Basis (see Appendix 1 for detail)	
2.1 What is the lawful basis for processing Personal Data under General Data Protection Regulation. DPA 2018 **NB –DO NOT select 6) (1) a) if processing is for the purpose of direct health or social care**	☐ 6) (1) a) Consent - (all article 7 conditions must be met ☐ 6) (1) b) Delivery of a Contract ☐ 6) (1) c) Legal Obligation ☐ 6) (1) d) Vital interests ☒ 6) (1) e) A public / official function / Interest
2.2 Does the processing involve special categories of data A) racial or ethnic origin of the individual B) the political opinions of the individual C) the religious or philosophical beliefs of the individual D) whether the individual is a member of a trade union E) processing of genetic or biometric data for uniquely identifying an individual F) physical or mental health of the individual G) sex life or sexual orientation of the individual	☐ Yes ☒ No Please provide details:
2.3 If Yes What is the lawful basis for processing Personal Data under General Data Protection Regulation Article 9. **NB –DO NOT select 6) (1) a) if processing is for the purpose of direct health or social care**	☐ 9) (2) a) Consent – (all article 7 conditions must be met) ☐ 9) (2) b) Employment, social security etc. ☐ 9) (2) c) Vital interests ☐ 9) (2) d) Legitimate activities (not to be used for public authorities) ☐ 9) (2) e) Data already been made public by subject ☐ 9) (2) f) Legal obligation ☐ 9) (2) g) Public interest ☐ 9) (2) h) Provision of Health or Social Care ☐ 9) (2) i) Public health

	☐ 9) (2) j) Historical or scientific research
2.4 Where consent is applied, Please provide details of the consent process and embed any consent forms **Note: Consent must follow Article 7 requirements**	☐ Explicit consent Provide details below:
2.5 Please indicate other legislation which provides a legal basis for processing **(Please tick relevant legislation or add details as necessary)**	☐ Children Act 1989 as amended 2004 ☐ Mental Capacity Act 2005 ☐ Health & Social Care Act 2012 ☐ Care Act 2014 ☐ H&SC (Safe and Quality) Act 2015 ☐ NHS Act 2006 ☒ Human rights Act 1998 ☐ Data Protection Act 2018 Sch 1 para 2 ☐ Other (Please specify)

3.0 Risk Assessment (see Appendix 2 for examples)

	Consequence				
Likelihood	1 Negligible	2 Low	3 Medium	4 High	5 Extreme
1 Rare	L1	L2	L3	M4	M5
2 Unlikely	L2	L4	M6	M8	S10
3 Possible	L3	M6	M9	S12	H15
4 Likely	L4	M8	S12	H16	H20
5 Almost Certain	M5	M10	S15	H20	H25

3.1 Highlight Risks and Identify Controls

All key risks should be highlighted here with any controls that have been identified. All risks to the project should be held on a formal risk register							
No	**Summary of Risk**	**Risk to Individuals**	**Risk to the organisation**	**Compliance Risk**	**Identified Risk L/M/S/H**	**Proposed Controls**	**Residual Risk L/M/S/H**
1	Inappropriate or continuous recording on scene	L4	L3	M6	Med	Training. Audit appropriateness of device use per user	Low
2	Inability to switch off visual or audio recording	L2	L3	M6	Med	Training. Audit appropriateness of device use per user. Provide guidance to BWV users on appropriateness of use of the device. Ensure users are trained in appropriate use.	Low
3	Loss/theft of camera	L1	M5	M5	High	Ensure movement of devices is monitored and there is a checking in/out process. A device may become detach and fall into unauthorised possession with the possibility of the data being accessed by an unauthorised individual. Where a device is lost, all possible attempts will be made to identify and notify persons who are subjects of information on the device. In addition, the captured information is stored on the	Med

						device's internal memory.	
4	Footage may show victims, potential witnesses, suspects or other third parties in a state of distress and/or undress	L3	L4	S12	High	Edit or obscure sections of the recording if they identify individuals who are not the subjects of concern. It is inevitable that in some circumstances this will occur, and users will be trained to ensure that wherever possible the focus of their activity is on the person subject of the incident. It is widely recognised that citizens are likely to have a strong expectation of privacy in their own homes (article 8 of the Human Rights Act) and under normal circumstance BWV should not be used in private dwellings. However, if when attending for the primary purpose of delivering medical care and a violent and aggressive or anti-social behaviour situation arises the BWV may be activated after announcing to the individuals on scene.	Med
	The proximity and vantage point of cameras may	L3	L4	S12	High	Edit or obscure sections of the recording if they identify individuals who	Med

	also increase the level of privacy intrusion when recording footage from within someone's home					are not the subjects of concern. It is inevitable that in some circumstances this will occur, and users will be trained to ensure that wherever possible the focus of their activity is on the person subject of the incident. It is widely recognised that citizens are likely to have a strong expectation of privacy in their own homes (article 8 of the Human Rights Act) and under normal circumstance BWV should not be used in private dwellings. However, if when attending for the primary purpose of delivering medical care and a violent and aggressive or anti-social behaviour situation arises the BWV may be activated after announcing to the individuals on scene.	

* IG Team Use Only

DPIA reviewed by Data Protection Officer for Approval	Yes Comment:
DPIA reviewed by Cyber :	Yes Comment:
Does the Trust have a compliant Privacy Notice for this process	☐ Yes ☐ No Comment:
Stage 1 Agreed	☐ Yes ☐ No
Stage 2 Required	☐ Yes ☐ No Comment:

Sign Off and Approval – Stage 1

Once this document has been completed and the solutions agreed it should be signed off by the DPO, Project Lead and the Information Governance Manager within the organisation

	Name	Date	Signed
Project Lead	[redacted]		
Information Governance Manager			

Sign Off and Approval – Stage 2

Once this document has been completed and the solutions agreed it should be signed off by the DPO and SIRO within the organisation

	Name	Date	Signed
SIRO	[redacted]		
Data Protection Officer			

Appendix 1 – Glossary of Terms

Item	Definition
Personal Data	This means data which relates to a living individual (data subject) who can be identified, directly or indirectly, by reference to an identifier such as name, an identification number, location data, and online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person: A) from those data, or B) from those data and any other information which is in the possession of, or is likely to come into the possession of, the data controller. It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual
Special Categories of Data	This means personal data consisting of information as to the: H) racial or ethnic origin of the individual I) the political opinions of the individual J) the religious or philosophical beliefs of the individual K) whether the individual is a member of a trade union L) processing of genetic or biometric data for uniquely identifying an individual M) physical or mental health of the individual N) sex life or sexual orientation of the individual
Direct Marketing	This is "junk mail" which is directed to particular individuals. The mail which are addressed to "the occupier" is not directed to an individual and is therefore not direct marketing. Direct marketing also includes all other means by which an individual may be contacted directly such as emails and text messages which you have asked to be sent to you. Direct marketing does not just refer to selling products or services to individuals, it also includes promoting particular views or campaigns such as those of a political party or charity.
Automated Decision Making	Automated decisions only arise if 2 requirements are met. First, the decision has to be taken using personal information solely by automatic means including profiling, which produces legal effects concerning the data subject or similarly affects them. For example, if an individual applies for a personal loan online, the website uses algorithms and auto credit searching to provide an immediate yes / no decision. The second

	requirement is that the decision has to have a significant effect on the individual concerned.
International organisation	Means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.
Information Assets	Information assets are records, information of any kind, data of any kind and any format which we use to support our roles and responsibilities. Examples of Information Assets are databases, systems, manual and electronic records, archived data, libraries, operations and support procedures, manual and training materials, contracts and agreements, business continuity plans, software and hardware.
SIRO (Senior Information Risk Owner)	This person is an executive who takes ownership of the organisation's information risk policy and acts as advocate for information risk on the Board
IAO (Information Asset Owner)	These are senior individuals involved in running the relevant service/department. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets. They are responsible for providing regular reports regarding information risks and incidents pertaining to the assets under their control/area.
IAA (Information Asset Administrator)	There are individuals who ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management and ensure that information asset registers are accurate and up to date. These roles tend to be system managers
Explicit Consent	Express or explicit consent is given by the data subject freely given, specific, informed and unambiguous indication of the data subjects wishes, usually orally (which must be documented in the patients casenotes) or in writing, to a particular use of disclosure of information.
Anonymity	Information may be used more freely if the subject of the information is not identifiable in any way – this is anonymised data. However, even where such obvious identifiers are missing, rare diseases, drug treatments or statistical analyses which may have very small numbers within a small population may allow individuals to be identified. A combination of items increases the chances of patient identification. When anonymised data will serve the purpose, health professionals must anonymise data and whilst it is not necessary to seek

	consent, general information about when anonymised data will be used should be made available to patients.
Pseudonymisation	Means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person Patient identifiers such as name, address, date of birth are substituted with a pseudonym, code or other unique reference so that the data will only be identifiable to those who have the code or reference.
Information Risk	An identified risk to any information asset that the Trust holds. Please see the Information Risk Policy for further information.
Privacy Invasive Technologies	Examples of such technologies include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining and logging of electronic traffic. Technologies that are inherently intrusive, new and sound threatening are a concern and hence represent a risk
Authentication Requirements	An identifier enables organisations to collate data about an individual. There are increasingly onerous registration processes and document production requirements imposed to ensure the correct person can have, for example, the correct access to a system or have a smartcard. These are warning signs of potential privacy risks.
Retention Periods	Records are required to be kept for a certain period either because of statutory requirement or because they may be needed for administrative purposes during this time. If an organisation decides that it needs to keep records longer than the recommended minimum period, it can very the period accordingly and record the decision and the reasons behind. The retention period should be calculated from the beginning of the year after the last date on the record. Any decision to keep records longer than 30 years must obtain approval from The National Archives.
Information Governance Alliance (IGA) Records	Is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice. The

Management NHS Code of Practice	code of practice contains an annex with a health records retention schedule and a Business and Corporate (non-health) records retention schedule.
(UK) General Data Protection Regulation (EU) 2016/679 (GDPR)	European legislation (applied in UK law by the Data Protection Act 2018) on the protection of natural persons with regard to the processing of personal data. The Regulation defines the ways in which information about living people may be legally used and handled. The 6 principles of the Regulation state the fundamental principles relating to processing personal data must: • be processed fairly and lawfully. • Collected for specified, explicit and legitimate purposes • be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. • be accurate and, where necessary, jept up to date. • Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal dta are processed. • be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage. The Regulation also requires that the Data Controller and Data Processor are both able to demonstrate compliance with these principles.
Privacy and Electronic Communications Regulations 2003	These regulations apply to sending unsolicited marketing messages electronically such as telephone, fax, email and text. Unsolicited marketing material should only be sent if the requester has opted in to receive this information.
Article 6 Conditions of Processing	1) (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes - only lawful if ALL article 7 conditions for consent are met 1) (b) A contract with the individual: for example, to supply goods or services they have requested, or to fulfil your obligations under an employment contract. This also includes steps taken at their request before entering into a contract. 1) (c) Compliance with a legal obligation: if you are required by UK or EU law to process the data for a particular purpose, you can. 1) (d) Vital interests: you can process personal data if it's necessary to protect someone's life. This could be the life of the data subject or someone else.

	1) (e) A public task: if you need to process personal data to carry out your official functions or a task in the public interest – and you have a legal basis for the processing under UK law – you can. If you are a UK public authority, our view is that this is likely to give you a lawful basis for many if not all of your activities. 1) (f) Legitimate Interest: If you need to process personal data in the legitimate interests of the Data Controller or 3rd Party or Data Subjects Rights in particular where data subject is a child. NB 1) (f) does not apply to processing carried out by Public authorities in the performance of their tasks.
Article 9 Conditions of Processing special categories of data	(1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. (2) Paragraph 1 shall not apply if one of the following applies: 2) (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject only lawful if ALL article 7 conditions for consent are met (see column D)" 2) (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; 2) (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; 2) (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact

	with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects; 2) (e) processing relates to personal data which are manifestly made public by the data subject; 2) (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; 2) (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; 2) (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3; 2) (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; 2) (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
Article 7 (Recital 32) Conditions for Consent	Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website,

	choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

Appendix 2 – Examples of Risk

EXAMPLES OF PRIVACY AND RELATED RISKS
RISKS TO INDIVIDUALS
Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
New surveillance methods may be an unjustified intrusion on their privacy.
Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
The sharing and merging of datasets can allow organisations to collect a much wider set of information that individuals may expect.
Identifiers might be collected and linked, which prevents people from using a service anonymously.
Vulnerable people may be particularly concerned about the risks of identification of the disclosure of information.
Collecting information and linking identifiers may mean that an organisation is no longer using information which is safely anonymised.
Information, which is collected and stored unnecessarily, or is not properly managed, so that duplicate records are created, presents a greater security risk.
If a retention period is not established, information might be used for longer than is necessary.
CORPORATE RISKS
Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
Problems, which are only identified after the project has launched, are more likely to require expensive fines.
The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engagement with the organisation.
Information, which is collected and stored unnecessarily, or is not properly managed, so that duplicate records are created, is less useful to the business.

Public distrust about how information is used can damage an organisations reputation and lead to loss of business.
Data losses (which damage individuals) could lead to claims for compensation.
COMPLIANCE RISKS
Non-compliance with the DPA.
Non-compliance with the Privacy and Electronic Communications Regulations (PECR)
Non-compliance with sector specific legislation or standards
Non-compliance with Human Rights legislation

Essex Partnership University NHS Foundation Trust

CP24 - Appendix 1

Equality Impact Assessment (EIA)

Date (DD/MM/YYYY)	08/08/2023	
Directorate / Locality / Department	Risk and Compliance/ VAPR Advisor & Estates & Compliance/ Estates Compliance Manager	
Name of New Policy / Service / Function	Surveillance Policy (BWC & CCTV)	
Is this a New Policy / Service / Function or a change / review to an existing one?	Existing Function	
Name of Person(s) completing this EIA and their Role(s) within the Trust *(begin with the lead completing this assessment)*	[redacted]	VAPR Advisor
	[redacted]tt	Estates Compliance Manager
Name of Service Director	[redacted]	
Contact Email address of Assessor	[redacted]	
Has this been previously assessed? *(If yes, please provide details of the last assessment and attach a copy)*	No	

Guidance on Completing this Document

The Equality Impact Assessment (EIA) is made up of two parts, an Initial Screening Tool and a Full Equality Impact Assessment. These are designed to make sure that our policies, services and functions do what they are intended to do in a way that does not discriminate against any protected characteristic groups in line with the Equality Act (2010).

Authors of new Policies, Services or Functions must gauge their impact on the nine Protected Characteristic Groups under the Equality Act. This is done using the Initial Screening Tool (Pages 2, 3 and 4)

If a positive or negative impact is identified, you will also need to complete the Full Equality Impact Assessment (Pages 4, 5, 6 and the action plan on Page 7). Please note that the lead assessor is responsible for ensuring these actions are incorporated into the departmental plan, and it is the responsibility of the assessor to notify their Director and any nominated staff members of these actions.

This document is designed to help us consider the following:

- What is this Policy / Service / Function aiming to achieve?
- Who will this benefit?
- Could this lead to negative impact or discrimination against different groups?
- Does this activity have a positive impact on Equality and Inclusion?

Glossary:

Service: your department / service area and its employees
Functions: your department / service area's activities
Projects: your department / service area's work programmes
Strategy: a plan of action intended to accomplish a specific goal
Policy: a plan of action to influence and determine decisions, actions and other matters
Procedure: a series of steps taken to implement a policy
Protected Characteristic: Any characteristic protected under the Equality Act 2010

Initial EIA Screening Tool

Does this Policy/Service/Function effect one group less or more favourably than another on the basis of:	Yes / No	What / where is the evidence / reasoning to suggest this?
Race, Ethnic Origins, Nationality (including traveling communities)	No	BWC/CCTV is a system used to assist inpatient clinical staff provide care and safety for patients and staff. The system has no methodology or faculty for bias. BWC/CCTV does not use facial recognition software and records without bias
Sex (Based on Biological Sex; Male, Female or Intersex)	No	BWC/CCTV cannot distinguish patients based on biological such as male, female or intersex. BWC/CCTV does not use facial recognition software and records without bias
Age	No	BWC/CCTV cannot distinguish patients based on age. BWC/CCTV does not use facial recognition software and records without bias
Sexual Orientation Including the LGBTQ+ Community	No	BWC/CCTV cannot distinguish patients based on their sexual orientation including the LGBTQ+ Community. BWC/CCTV does not use facial recognition software and records without bias
People who are Married or are in a Civil Partnership	No	BWC/CCTV cannot distinguish patients based on whether they are married or are in a civil partnership. BWC/CCTV does not use facial recognition software and records without bias
People who are Pregnant or are on Maternity / Paternity Leave	No	BWC/CCTV cannot distinguish patients based on whether they are pregnant or are on maternity / paternity leave. BWC/CCTV does not use facial recognition software and records without bias.

Does this Policy/Service/Function effect one group less or more favourably than another on the basis of:	Yes / No	What / where is the evidence / reasoning to suggest this?
People who are Transgender / who have had gender reassignment treatments As well as gender minority groups	No	BWC/CCTV cannot distinguish patients based on whether a patient is transgender, has had gender reassignment treatments, or identifies with other gender minority groups. BWC/CCTV does not use facial recognition software and records without bias
Religion, Belief or Culture Including an absence of belief	No	BWC/CCTV cannot distinguish patients based on a patient's religion, belief or culture including an absence of belief. BWC/CCTV does not use facial recognition software and records without bias
Disability / Mental, Neurological or Physical health conditions Including Learning Disabilities	No	BWC/CCTV cannot interpret a patient's disability / mental, neurological or physical health conditions including learning disabilities. BWC/CCTV does not use facial recognition software and records without bias. The body worn cameras although small have an easily accessible record button, the cameras are easy to attach to the uniform and would not cause difficulty in using.
Other Marginalised or Minority Groups Carers, Low Income Families, people without a fixed abode or currently living in sheltered accommodation.	No	BWC/CCTV is used in an inpatient environment and cannot distinguish whether a patient is identified as a member of a marginalised or minority group, carers, low-income families, people without a fixed abode or currently living in sheltered accommodation. BWC/CCTV does not use facial recognition software and records without bias

Guidance on Completing this Document

This screening tool asks for evidence to ensure that these considerations are done in collaboration with groups that may be affected. Listed below are the ways that this evidence can be gathered to support this decision:

- Reviews with Staff who may be impacted by these changes
- Service User / Carer feedback or focus groups
- Guidance from national organisations (CQC / NHS Employers)
- The Equality and Inclusion Hub (on the Staff Intranet)
- Input from Staff Equality Networks or the Equality Advisor
- Reviewing this against good practice in other NHS Trust

Initial Screening Question	Response
If you have identified no negative impacts, then please explain how you reached that decision. please provide / attach reference to any reasoning or evidence that supports this: (Nature of policy, service or function, reviews, surveys, feedback, service user or staff data)	BWC/CCTV is a system used to assist inpatient clinical staff provide care for patients. The system has no methodology or faculty for bias (CP28- Surveillance systems Policy)
Is there a need for additional consultation? (Such as with external organisations, operational leads, patients, carers or voluntary sector)	N/A
Can we reduce any negative impacts by taking different actions or by making accommodations to this proposed Policy / Service / Function?	N/A
Is there any way any positive impacts to certain communities could be built upon or improved to benefit all protected characteristic groups?	N/A
If you have identified any negative impacts, are there reasons why these are valid, legal and/or justifiable?	N/A

Please complete this document and send a copy to EPUT's Compliance, Assurance & Risk Assistant / Trust Policy Controller) at [redacted] as part of the Approval Process, if this proposal / policy etc. has no positive or negative impacts on protected characteristic groups, a Full Equality Impact Assessment will not need to be completed

To be completed by the Trust Policy Controller				
Is a Full Equality Impact Assessment Required for this Policy, Service or Function?	Yes		No	X
Name:	[redacted]			
Date:	08/08/2023			