

## Closed Circuit Television (CCTV) Policy

### Review

Formal Review Cycle	3 years (or earlier should regulatory requirements change)		
Latest Formal Review (date)	07 July 2025	Next Formal Review Due (date)	06 July 2028
Policy Owner	S Brown, Executive Director of Capital Projects and Estates		
Policy Author	S Brown, Executive Director of Capital Projects and Estates		

### Approvals

Board of Corp Y/N	N	Committee		Date Board approved	
ELT Y/N	Y	ELT date approved		Additional committee	

### Publication

Website Y/N	Y	Intranet Y/N	Y	Student VLE Y/N	Y	Other	
-------------	---	--------------	---	-----------------	---	-------	--

### Change History

Version	Date Reviewed/ Revised	Description of Change	Reviewed by	Approved by
1	08 May 2017	New Policy	S Brown	
2	11 <sup>th</sup> April 2021	Policy amended to incorporate Northumberland College and Body Worn Camera's (BWC's)	S Brown	
3	16 <sup>th</sup> March 2025	Policy reviewed and updated	S Brown	

# EPNE Closed Circuit Television (C.C.T.V.) Policy

## 1. Policy Statement

### 1.1. Introduction

Education Partnership North-East (EPNE) has deployed a combination of internal and external CCTV surveillance cameras across a selection of its sites to assist in the safeguarding of staff, students and visitors together with the ongoing security of its real estate. None of the current systems are continually monitored, however, recorded images are securely stored for a short period, normally 30 days but system dependent. Images will be kept no longer than necessary to fulfil the purposes for which they were collected. Access to recorded images can be obtained, but only with the authority of a senior member of staff as defined later in this document.

EPNE believes surveillance systems have a legitimate role to play in helping to promote and maintain a safe and secure environment, however, EPNE recognises that this may raise concerns about the effect on individuals and their privacy. This policy is intended to outline how the employed CCTV systems will be utilised to address these concerns whilst creating the correct conditions in which staff can operate and students can study.

### 1.2. Purpose

This Policy has been prepared to comply with the standards set out in the **“Amended Surveillance Camera Code of Practice, March 2022”** and the Information Commissioner’s Office **“Video surveillance (including guidance for organisations using CCTV)”**. Its purpose is to ensure the EPNE CCTV systems are used to create a safer environment for staff, students and visitors and to ensure its operation is consistent with the Data Protection Act 2018.

Specifically, within EPNE CCTV systems will be employed to:

- Protect the health, safety and welfare of staff, students and visitors attending any site equipped with CCTV.
- Monitor the security of the sites and property contained within.
- Protect staff, students and visitors from harassment or intimidation.
- Assist in the maintenance of good order and behaviour across the college estate.
- Assist in the prevention, investigation and detection of disciplinary offences in accordance with EPNE disciplinary procedures.
- Help identify individuals who breach EPNE policies.
- Support the Police in deterring and detecting crime.

## 2. Scope

This policy applies to the surveillance camera systems installed across EPNE sites which includes systems referred to as CCTV and body worn cameras. All are employed for the purposes of promoting safeguarding,

security and to identify criminal activity whether occurring, anticipated or perceived in order to enhance the safety and wellbeing of staff, students, and visitors. It also applies to information relating to individuals for the purposes of monitoring activities on EPNE premises, car parks and other public areas.

The use of conventional cameras, surveillance cameras and CCTV for other purposes including for artistic, administrative, educational or research purposes is not covered by this policy.

### **3. Aims of the Policy/Underpinning Principles**

The underlying principles of this policy align with the guiding principles outlined within "[The Home Office Surveillance Code of Practice](#)". These include:

1. Ensure the use of the system is always employed for a specified legitimate aim and capable of meeting an identified pressing need.
2. Take into account the effect on individuals and their privacy.
3. Provide as much transparency in the use of the system as possible, providing contact details for information and complaints.
4. Detail clear responsibility and accountability for all surveillance activities including images and information collected, held and used.
5. Provide clear rules, policies and procedures, ensuring they are communicated to all who need to comply.
6. Ensure no more images or information is stored than that which is strictly required.
7. Restrict access to recorded/retained images and information with clear rules defining who can gain access.
8. Consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Ensure images will be subject to appropriate security measures to safeguard against unauthorized access and use.
10. Provide effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with.
11. Ensure the use of the system in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value, when used in the pursuit of a legitimate aim.
12. Ensure that when any information is used to support a surveillance camera system and comparisons are made against a reference database, information should be checked and verified for accuracy.

### **4. Responsibilities**

#### **4.1. The Head of Corporate Governance and Policy**

- Ensure EPNE is registered with the Information Commissioner's Office

- Ensure subject access requests and Freedom of Information requests are responded to in a manner consistent with EPNE policy and procedure and legislation

#### **4.2. Director of Estates**

- Ensure the installation and operation of the CCTV system complies with the “Amended Surveillance Camera Code of Practice 2013, amended Nov 2021”.
- Ensure the operation and use of CCTV equipment and the recording and viewing of images complies with the “Data Protection Act 2018”.
- Ensure the system is maintained and repaired when necessary.
- Ensure staff operating the system are trained and equipped with the correct qualifications.
- Act as the first point of contact for any complaints received regarding the operation of the system.
- Ensure any images retained for evidential purposes are kept in a secure location where access is controlled.

#### **4.3. Security Staff**

- When required operate and monitor the camera surveillance systems located at EPNE sites.
- Will provide an immediate response to incidents observed where a “risk” is perceived.
- Ensure no unauthorised access to the system is allowed at any time. Normal access is strictly limited to authorised staff only.
- When in the receipt of authorisation to provide information, will only provide that which is relevant to the enquiry.
- In the event of an “emergency” and where it is not reasonably practicable to secure prior authorisation, may provide access to persons with a legitimate reason to access the CCTV system.
- Before allowing any person access to the CCTV system must satisfy themselves of the identity of any visitor and ensure that the visitor has the appropriate authorisation.
- Ensure all visitors complete and sign the Visitors Log, which shall include their name, department or the organisation they represent, the person who granted authorisation for their visit (if applicable) and the start and finish times of their access to the CCTV system.
- Will highlight any system failures to Estates as soon as reasonably practicable.

#### **4.4. Estates Admin Team**

- Will ensure the CCTV policy is maintained and is easily accessible via the EPNE College website.

## 5. Implementation

### 5.1. Explanation of Key Terms

- **Surveillance system** - Any electronic system or device that captures images of individuals or information relating to individuals.
- **CCTV** - Any surveillance system designed to capture and record images of individuals or information relating to individuals and/or property. The term includes CCTV as understood as a system of fixed cameras but also covers any such technology including automatic number plate recognition (ANPR), body worn cameras, unmanned aerial systems and any other systems that capture personal data.
- **System Operator** – Person or persons that take the decision to deploy a surveillance camera system, and are responsible for defining its purpose, and / or are responsible for the control of the use or processing of images or other information obtained by virtue of such system.
- **System User** – person or persons who may be employed or contracted by the systems operator who have access to live or recorded images or other information obtained by virtue of such system.
- **Data Subjects** – Persons whose images have been recorded by the CCTV systems.
- **Emergency** – A serious, unexpected, and often dangerous situation requiring immediate action.

## 6. Operation

### 6.1. Overview of EPNE CCTV Systems

- CCTV systems are installed within or externally fitted to the following locations:
  - Ashington
  - Bede
  - Berwick
  - City
  - Hartlepool 6<sup>th</sup> Form
  - Housing Innovation Construction Skills (HICSA)
  - Kirkley Hall
- The CCTV systems are owned by EPNE and include a combination of fixed cameras and / or body worn video devices.
- The CCTV systems will only be used in a manner which is fair to everyone and in accordance with this policy.
- CCTV signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that CCTV is in use. Students

will also be made aware of CCTV systems during their induction or commencement of their course.

- Fixed cameras will be configured to record images only whilst the use of body worn devices will allow both images and audio to be recorded.
- Remote access to cameras will only be employed sparingly and in exceptional circumstances.
- Where maintenance is required, staff in charge of the CCTV systems must be satisfied as to the identity of contractors prior to allowing access to the system.
- Although every effort has been made in the planning and design of the CCTV systems to provide maximum effectiveness, it is not possible to guarantee that the systems will detect every incident taking place within the area of coverage.

## **6.2. Monitoring and Recording**

- EPNE will be responsible for the management and processing of images.
- Authorised staff shall monitor live feeds from CCTV cameras where it is deemed reasonably necessary, for example to protect health and safety.

## **6.3. Compliance with Data Protection**

- It is recognised that the images obtained comprise personal data and are subject to the law on Data Protection. All copies will be handled in accordance with EPNE procedures.
- All staff involved in the operation of the camera surveillance system will, by training and access to this policy, be made aware of the sensitivity of handling CCTV images and recordings.
- Camera surveillance systems will be stored within secure locations and/or accessed by secure passwords. Unauthorised access to the CCTV screens will not be permitted at any time.

## **6.4. Disclosure of Images – See Appendix ‘A’**

Access to stored CCTV images will only be provided following approval by the relevant college authority. Requests will generally be received from an individual (staff, student, visitor, contractor or member of the public), third parties (police or other legal body) or by staff in relation to a college related incident.

Images can be supplied by a suitable medium, or arrangements can be made to view them on site.

### **6.4.1. Individual Access Rights**

Any individual whose personal data is held by EPNE in the form of a CCTV recording can request access to that recording. EPNE will respond in accordance with the Data Protection Act 2018.

Any person who wishes to access images must make their request in writing to the Head of Corporate Governance and Policy, attaching a completed Access Request Form. This form is included as appendix ‘B’.

#### **6.4.2. Access to Images by Third Parties external to the college**

Records may need to be disclosed to third parties for the following reasons:

- a. To the police, for the prevention and detection of crime.
- b. To a court for legal proceedings.
- c. To a solicitor for legal proceedings.

Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and the prevailing data protection legislation.

All third parties requesting access to images must make their request in writing to the Head of Corporate Governance and Policy, attaching a completed Access Request Form. This form is included as appendix 'B'.

#### **6.4.3. Access to Images by a member of college staff**

Staff members may request access to CCTV images for several reasons which includes:

- Investigation of an internal incident within the college e.g. theft.
- In support of a disciplinary investigation.
- To assist with health and safety related incidents.
- To support in the review of a safeguarding concern.

Any staff member who wishes to access images must obtain authorisation from a Senior Manager (see below) by submitting a completed Access Request Form as included within appendix 'B'.

Authorisation to view can only be granted by:

- Chief Executive Officer
- Deputy Chief Executive Officer
- Campus Principal
- Vice Principal – Corporate Services

#### **6.5. Record-keeping of data transferred or images viewed**

Where data/images have been disclosed, viewed or transferred to a portable storage device EPNE will retain a record as detailed in Appendix 'C' and will include:

- The date and time of removal.
- The name of the person removing the images.
- The name(s) of the person(s) viewing / or in receipt of the images.
- The reason for the request.
- The outcome, if any, of the viewing (if applicable).

- The date and time the images were returned to the system or secure place, or if they have been retained for evidential purposes (if applicable).
- Where access to data/images is refused, the reason(s) shall be documented and made available to the party requesting access.

## **6.6. Retention of Images**

The Service Desk will retain images for 30 days (system dependent), after which time they will be overwritten and any copies destroyed unless required as evidence in Police investigations, internal disciplinarys or there is a potential for future litigation claims.

- Data and images recorded by the CCTV system shall be permanently and securely deleted once the purpose for which they were collected has expired.
- Any physical matter such as tapes, discs, hard copy prints, still photographs shall be disposed of as confidential waste.

## **6.7. Body Worn Video Cameras**

### **6.7.4. Overview**

Body Worn Cameras (BWC's) are miniaturized video cameras and microphones which capture a user's interactions with other individuals. Normally attached to a user's clothing, they have the facility to be quickly turned on/off at key moments to gather evidential images. The presence and visibility of BWC's enhances the service provided by the current CCTV systems installed across EPNE sites and are designed to:

- Enhance the personal safety of students on site.
- Increase Staff/Student reassurance.
- Raise standards during confrontational incidents.
- Reduce incident escalation.
- Reduce complaints.
- Reduce the fear of crime on site.
- Assist with disciplinary and / or legal proceedings.
- Assist in the training of security staff.

### **6.7.5. General Principles**

- BWC's will be managed by the contracted security provider who has experience of their operation and the protocols which must be adopted in their deployment.
- Before being issued with a body worn video camera, security staff will undergo training in the use of the device together with data protection law and best practice.

- The security provider will ensure BWC's are clearly identifiable and any images or sound recorded are encrypted.
- BWC's will only be used in accordance with the stated purpose and objectives of this policy.
- Users of the BWC's will only initiate recordings in response to suspected criminal activity, anti-social behaviour or disturbance, incidents where violence, aggression or threatening behaviour is displayed or where video evidence of a situation may be reasonably required to meet the purposes and objectives for which surveillance systems are deployed.
- Prior to initiating any recording using a body worn video camera security staff will warn any persons being recorded (Data Subjects) that video and sound recording is being initiated. A record will be kept of the date, time, location and reason for any recording made.

#### **6.7.6. Protocols for using BWC's**

- BWC's will be operated within the protocols set out within this document.
- Each user will be issued with a copy of this document. They will be fully aware of its contents, which may be reviewed and updated from time to time and will be expected to comply with the protocols outlined.
- Having received the relevant training in the use of BWC's, security staff must ensure the use of a BWC is widely advertised prior to the start of the recording. The security member of staff must be wearing the "Video Recording in Progress Badge" prior to activating the unit.
- When a security officer decides to record an incident, they must:
  - Complete an incident report immediately providing details of the incident and the rationale for initiating the recording.
  - Inform a member of the Senior Team (Principal, Vice Principal, Associate Principal, 'Head of' or Director) ASAP to advise a recording has occurred.
  - Ensure any recording is stored safely and is not freely replayed within the public environment.

## **7. Associated Documents**

Legislation considered and applicable to the EPNE CCTV policy includes:

- Health and Safety at Work Act etc. 1974.
- Data Protection Act 2018.
- Human Rights Act 1998.
- The Regulation of Investigatory Powers Act 2000.
- The Private Security Industry Act 2001.

Standards considered and applicable to the EPNE CCTV policy includes:

- [Video surveillance \(including guidance for organisations using CCTV\) - ICO](#)
- [Home Office Surveillance Camera Code of Practice 2013 – amended 2021.](#)

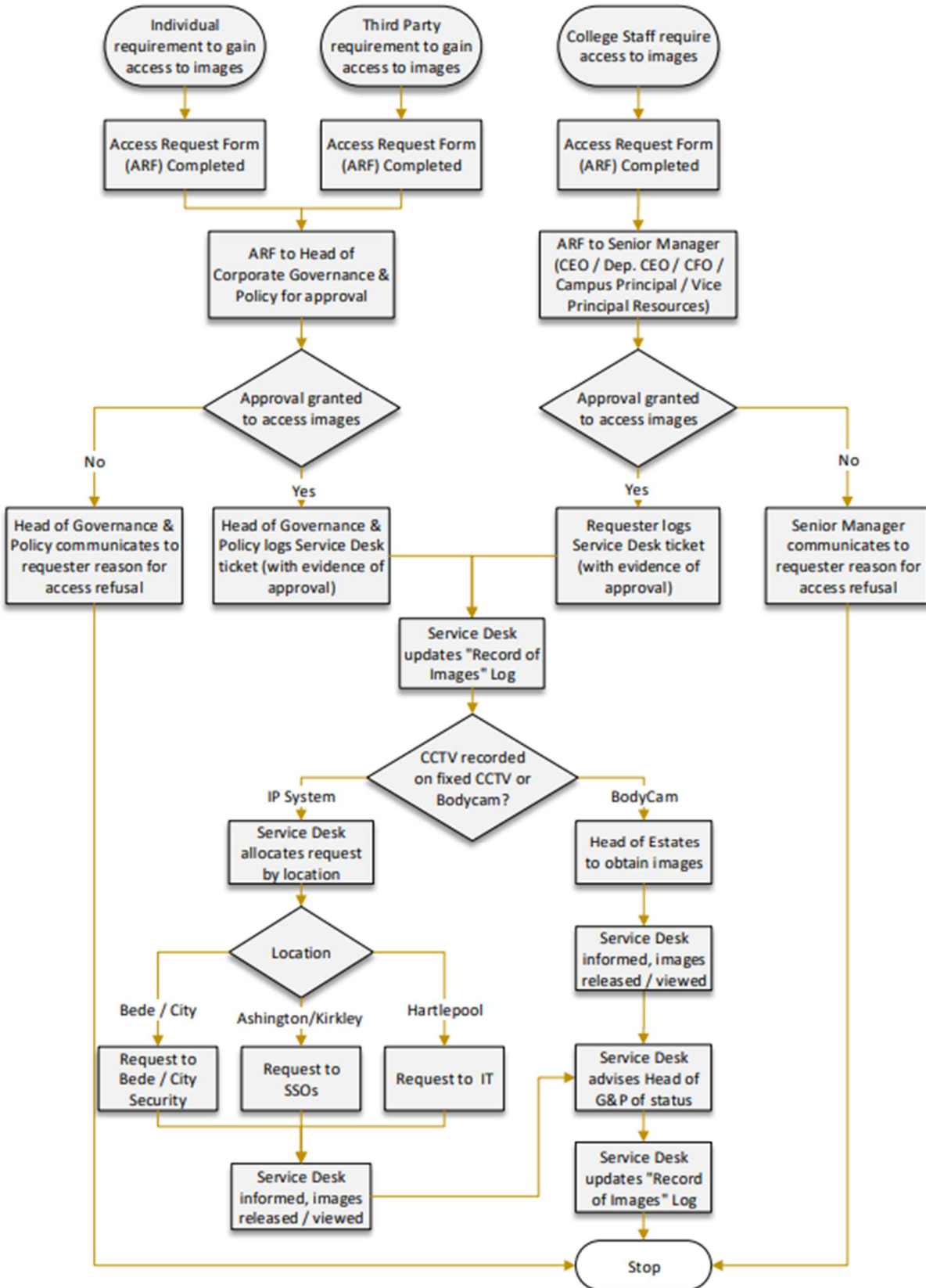
## 8. Policy Monitoring and Review

The policy shall be reviewed every three years, or as required, for example following amendments to applicable legislation.

## 9. Equality Impact Assessment

<b>Have you sought consultation on this policy?</b>		Consultation occurred with: Executive Director of Student Services Executive Director of IT Director of Health and Safety External Security Providers – Constant Security Services Vice Principal – Corporate Services		
<b>Details:</b>				
<b>Could a particular group be affected (negatively or positively)?</b>	<b>Impact Y/N</b>	<b>Description of Impact</b>	<b>Evidence</b>	<b>Mitigation/Justification</b>
Protected characteristics under the Equality Act 2010				
Age	N			
Disability	N			
Gender Reassignment	N			
Marriage and Civil Partnership	N			
Pregnancy and maternity	N			
Race	N			
Religion or belief	N			
Sex	N			
Sexual Orientation	N			
Additional characteristics to consider				
Young Persons in Care & Care Leavers	N			
Young Carers & Care Givers	N			
Young Parents	N			
Youth Offenders	N			
Those Receiving Free School Meals	N			
<b>If there is no impact, please explain:</b>	The Policy is aimed to safeguard and protect ‘all’ staff and students.			

## Appendix "A" - Disclosure of Images



## Appendix 'B' – Access Request Form

(Please use BLOCK CAPITALS to complete this form)

### 1. Details of Requester

Title.	First Name.	Surname
Organisation (where applicable)		
Address of Individual / Organisation		
Telephone No.		
Email address.		
Are you requesting images of yourself?	Yes	No
If not requesting images of yourself, please provide the reason for application and the authority to view these images.		

### 2. Information Required to Locate Images

Date	Time
Location(s) and Individual(s) Involved	

### 3. Access to Images

I would like to view the relevant images at the College	
I would like to be sent a copy of the relevant images	

I acknowledge that it may be necessary for EPNE to contact me to obtain further information to confirm my identity and / or requirements.

Name	Signature	Date
------	-----------	------

Appendix 'C' – Record of Images viewed or transferred to a portable storage device.

(Please use BLOCK CAPITALS to complete this form)

Date & Time	Name of Person removing images	Name of Person viewing / receiving the images (if applicable)	Reason	Outcome of viewing (if applicable)	Date & Time images returned if removed for evidential images (if applicable)