CCTV Policy

Sept 2021

Version 1

1. Scope

This policy applies to all staff at Expanse Learning Wigan College (Hereafter referred to as the college).

2. Introduction

The purpose of this policy is to regulate the management, operation and use of the closed-circuit television (CCTV) system at the College. The system comprises a number of fixed and dome cameras located around the college site. All cameras are monitored from within the Comms office and are only available to selected senior staff. Any access to the CCTV must be recorded in the CCTV log situated in the CCTV cabinet and within the event function on DatabridgeMIS. This policy follows Data Protection Act guidelines and will be subject to review annually to include consultation as appropriate with interested parties. The CCTV system is owned by the college.

3. Objectives of the CCTV scheme

- To protect the college buildings and their assets.
- To increase personal safety and reduce the fear of crime.
- To support the police in a bid to deter and detect crime.
- To assist in identifying, apprehending and prosecuting offenders.
- The purpose of Safeguarding
- The purpose of public safety.
- To assist in managing the college.

4. Statement of intent

The CCTV Scheme will be registered with the Information Commissioner under the terms of the Data Protection Act 2018 and will seek to comply with the requirements of the Data Protection Act, the inauguration of the General Data Protection Regulations and the Commissioner's Code of Practice. The college will treat the system and all information, documents and recordings obtained and used as data which are protected by the Act. Cameras will be used to monitor activities within the college, its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of the college, together with its visitors.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Footage will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Footage will never be released to the media for purposes of entertainment. The planning and design have endeavoured to ensure that the scheme will give maximum effectiveness and efficiency, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage. Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at all access routes to areas covered by the college CCTV.

5. Data Controller

The Data controller for the college is the Shared Services Team.

6. Operation of the system

The scheme will be administered and managed by Shared Services, in accordance with the principles and objectives expressed in the code. The day-to-day management will be the responsibility of both the Senior Leadership Team (SLT) and the Head of College. The CCTV system will be operated 24 hours each day, every day of the year, and is monitored remotely via Hik-Connect App. CCTV recordings are currently held on the system for 30 days before automatic deletion.

7. Comms Office

The Shared Services Team will check and confirm the efficiency of the system on a regular basis and in particular that the equipment is properly recording and that cameras are functional. This will be via monthly checks. Access to the CCTV system will be strictly limited to the SLT and the Head of College. Unless an immediate response to events is required.

Visitors and other contractors wishing to enter the CCTV System will be subject to particular arrangement as outlined below:

- The Health, Safety and Facilities Manager must satisfy themselves over the identity of any other visitors to the main SLT office and the purpose of the visit
- Where any doubt exists, access will be refused
- Details of all visits and visitors will be endorsed in the CCTV System logbook.

The system may generate a certain amount of interest. It is vital that operations are managed with the minimum of disruption. Casual visits will not be permitted. Visitors must first obtain permission from the Health, Safety and Facilities Manager, or his nominated deputy and must be accompanied by him throughout the visit. Any visit may be immediately curtailed if prevailing operational requirements make this necessary.

8. Monitoring procedures

Camera surveillance may be maintained at all times. A monitor is installed in a secure cupboard within the main SLT office to which pictures will be continuously recorded. If covert surveillance is planned, it can only be undertaken by the police or the Council using the appropriate authorisation forms.

9. Video disc/USB procedures

In order to maintain and preserve the integrity of the discs/USB's used to record events from the hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:

- Each disc/USB must be identified by a unique mark
- Before using, each disc/USB must be cleaned of any previous recording
- The controller must register the date and time of disc insert, including disc reference.
- A disc/USB (recording) required for evidential purposes must be sealed, witnessed, signed by the controller dated and stored in the main safe. If a disc is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the controller, dated and returned to the evidence store
- If the disc/USB is archived the reference must be noted.

Recordings may be viewed by the police for the prevention and detection of crime and authorised officers of the Council. A record will be maintained of the release of recordings to the police or other authorised applicants. A register will be available for this purpose.

Viewing of recordings by the police must be recorded in writing and in the logbook. Requests by the police can only be actioned under section 29 of the Data Protection Act 1998. Should a recording be required as evidence, a copy may be released to the police under the procedures described in the above bullet points of section 7 of this Code. Recordings will only be released to the police on the clear understanding that the recording remains the property of the college, and both the recording and information contained on it are to be treated in accordance with this code. The college also retains the right to refuse permission for the police to pass to any other person the recording or any part of the information contained thereon. On occasions when a Court requires the release of an original recording, this will be produced from the secure evidence store, complete in its sealed bag.

The police may require the college to retain the stored discs for possible use as evidence in the future. Such discs /USB will be properly indexed and properly and securely stored until they are needed by the police.

Applications received from outside bodies (for example solicitors) to view or release recordings will be referred to the Facilities and Health and Safety Director and brought to the Board for approval. In these circumstances discs/USB will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a court order. A fee can be charged in such circumstances: £10 for subject access requests; a sum not exceeding the cost of materials in other cases.

10. Breaches of the code (including breaches of security)

Any breach of the Code of Practice by college staff will be initially investigated by the Assistant Head of College, in order for them to take the appropriate disciplinary action. Any serious breach of the Code of Practice will be immediately investigated, and an independent investigation carried out to make recommendations on how to remedy the breach.

This will be completed within 72 hours of notification of a serious breach.

11. Assessment of the scheme and code of practice

Performance monitoring, including random operating checks, may be carried out by the Shared Services Team.

12. Complaints

Any complaints about the college's CCTV system should follow the college's complaint policy *(ELCO-ORG-007(v2) – Complaint Policy).* Complaints will be investigated in accordance with this policy.

13. Access by the data subject

The Data Protection Act provides data subjects (individuals to whom 'personal data' relate) with a right to data held about themselves, including those obtained by CCTV. Requests for data subject access should be made on an application form available from the Head of College.

14. Public information

Copies of this Code of Practice will be available to the public from the College Office and the Head of College.

Summary of Key Points:

- This Policy will be reviewed annually
- The CCTV system is owned and operated by the college
- The Main SLT Office is not open to visitors except by prior arrangement and good reason
- Liaison meetings may be held with the police and other bodies
- Recordings will be properly indexed, stored and destroyed after appropriate use
- Recordings may only be viewed by authorised Council and college officers, SLT and the police
- Recordings required as evidence will be properly recorded witnessed and packaged before copies are released to the police
- Recordings will not be made available to the media for commercial or entertainment
- Discs /USB will be disposed of securely by incineration or approved disposal
- Any breaches of this code will be investigated by the Head of College. An independent investigation will be carried out for serious breaches
- Breaches of the code and remedies will be reported to the Head of College.

15. Monitoring arrangements

This policy will be reviewed every 12 months but can be revised as needed.

Impact of non-compliance:

Staff:	Disciplinary action, prosecution
Student:	Not applicable
Legislation/organisational:	Reputational damage, litigation, statutory and non-regulated compliance. prosecution
Compliance lead:	Shared Services (Health and Safety)
Policy Reference:	ELCO—POL-HSE-002
Version:	1
Agreed policy location:	DatabridgeMIS and Company Website
Does the policy require Governor approval?	No

Approval

Prepared by	***Approved by***	***Counter Signatory***
Scott Roberts (Assoc. CIPD)	Tony Brown	Karl Wane
01/09/2021	01/09/2021	10/09/2021
		
Head of Shared Services	CEO	Director of Post 16 Education

Version Control

Version	***Date***	***Revision***	***Review Date***
1	01/09/2021	First Issue	31/08/2022
2			
3			
4			
5			