



CCTV Policy

Key Information	
Policy Reference Number	CCSW-CCTV
ELT Post Responsible for Policy Update and Monitoring	Deputy Principal/Deputy CEO
Publish to College Website	Yes
Date Approved by ELT	02 March 2021
Date Approved by Committee)	09 March 2021
Date of Next Policy Review	04 March 2024

1. Purpose

- 1.1 The College uses closed-circuit television (CCTV) cameras to view and record individuals on and around its premises. This policy outlines the use of CCTV and the processing of data recorded by CCTV cameras to ensure that the College is compliant with data protection law and industry practice regarding CCTV.
- 1.2 The College recognises that images of individuals recorded by CCTV cameras in the workplace are personal data and therefore subject to the [Data Protection](#) Legislation. The College is the data controller.
- 1.3 The College is committed to providing a safe and secure learning environment. The purpose of this document is to regulate the use of CCTV to monitor and record public areas for the purposes of safety and security.
- 1.4 This policy applies to the CCTV monitoring of all learners enrolled at the College. They apply to staff, contractors, service providers, clients, customers and visitors at site locations where a CCTV system operates. These guidelines do not cover the use of CCTV to monitor staff activities.
- 1.5 This policy must also be adhered to by any external security contractors operating on site, for example, for security monitoring during weekends and holiday periods.

2. Responsibilities

- 2.1 The designated person responsible for the CCTV monitoring system in College is the Estates and Facilities Manager.
- 2.2 The Estates and Facilities Manager will carry out regular checks to ensure that College policy is being complied with and to review whether the system continues to be effective in meeting its purpose.
- 2.3 The designated senior manager is the Deputy Principal/Deputy CEO.
- 2.4 Information about who is responsible for the College CCTV system, how the CCTV system is being used and its purpose will be notified to the Information Commissioner within the College's Data Protection notification.
- 2.5 A [Data Protection Impact Assessment \(DPIA\)](#) shall be carried out prior to introducing a new surveillance camera system, using sound recording or placing a new CCTV camera in a workplace location.
- 2.6 All staff who operate, manage or process images from CCTV must comply with this policy.
- 2.7 Staff or agency camera control operators shall not use CCTV systems until they have completed appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data.
- 2.8 Camera control operators will not monitor individuals based on characteristics of race, gender, ethnicity, sexual orientation, disability, or other classifications protected by the College's Equality & Diversity Policy. Camera control operators will monitor based on suspicious behaviour and/or the need to view the movement of traffic and people, not individual characteristics.

3. CCTV Requirements

3.1 Purpose

- 3.1.1 The College uses CCTV around its site for the following legitimate business purposes:
 - 3.1.1.1 to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;
 - 3.1.1.2 for the personal safety of staff, learners, visitors and other members of the public and to act as a deterrent against crime;
 - 3.1.1.3 to support law enforcement bodies in the prevention, detection and prosecution of crime;
 - 3.1.1.4 to assist in day-to-day management, including ensuring the health and safety of staff and others;

- 3.1.1.5 to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings;
- 3.1.1.6 to assist in the defence of any civil litigation, including employment tribunal proceedings;
- 3.1.1.7 to assist with traffic management issues; and
- 3.1.1.8 to monitor the security of buildings.

3.2 CCTV Operation

- 3.2.1 CCTV systems may operate 24 hours a day.
- 3.2.2 CCTV camera locations shall be chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring. As far as practically possible, CCTV cameras shall not focus on private homes, gardens or other areas of private property. The College will limit camera positions and views of residential housing to what is absolutely necessary.
- 3.2.3 Camera control operators will not view private rooms or areas through windows.
- 3.2.4 Any camera location/data/time information that is recorded with the images must be regularly checked for accuracy and changes promptly made to accommodate summer/wintertime and leap year changes.
- 3.2.5 Ideally all cameras should be linked to the main recording system at a central point on the site. If this is not possible, other recording systems on the site should also adhere to these guidelines.
- 3.2.6 The cameras and the associated recording equipment must be properly maintained. The Estates and Facilities Manager is responsible for arranging ongoing checks and maintenance of the CCTV system and must keep a log of all equipment and media malfunction, repairs, and replacements, and of all complaints or enquiries or incidents about the system together with the action taken. An equivalent system must be operated by the Network Services Manager/team for equipment that comes under their control.
- 3.2.7 The College will post signage at appropriate locations, which includes the image of a CCTV camera. These must be placed in highly visible positions and make sure the public are aware that they are entering a zone that is covered by surveillance equipment.
- 3.2.8 Camera operators will only conduct video observation of public areas of the College, they will not record sound.
- 3.2.9 The CCTV monitors displaying images are sited so that the images cannot be routinely viewed by anyone other than the operators of the equipment.
- 3.2.10 Access to the recorded images is restricted to those who need access to achieve the purpose(s) of the CCTV system.
- 3.2.11 Duty managers may ask to see CCTV footage as it relates to specific incidents under investigation where they have approval to do so from the Data Protection Officer, Estates and Facilities Manager or a member of the Executive Leadership Team (ELT).

3.3 Storage and Use of Recorded Images.

- 3.3.1 Recorded material will be stored in a locked cupboard or safe, to maintain the integrity of any images, with access by authorised personnel only.
- 3.3.2 Recorded discs, digital images and derived photographs will be stored for a period not to exceed 30 days and will then be deleted or destroyed in a secure way.
- 3.3.3 The release of recorded footage or access shall be allowed to law enforcement in order to aid an investigation on the approval of the Data Protection Officer, Estates and Facilities Manager or a member of the Executive Leadership Team (ELT). Any such request must be valid and lawful and the College would normally have received a written request (*for example Schedule 2 Part 1 Paragraph 2 of the Data Protection Act 2018 "Crime and taxation"*).

- 3.3.4 Images from CCTV cameras shall not be routinely disclosed to other third parties, without express permission being given by the Data Protection Officer who shall ensure that the disclosure observes the Data Protection Legislation.
- 3.3.5 The Estates and Facilities Manager will maintain a log of all disclosures of CCTV images.
- 3.3.6 No images from the CCTV system or recordings in any format shall be passed to the media or placed on the internet.

3.4 Viewing of Images

- 3.4.1 The viewing of the recorded images, including still photographs taken from it, should take place in a restricted area, usually in the CCTV room. Individuals, other than those directly involved in the management and operation of the system, must not have access to the viewing without authority from the Estates and Facilities Manager, the duty manager (*in emergency cases only*) or the Data Protection Officer.
- 3.4.2 All viewings should be recorded into a CCTV register. This register will be available in the Estates and Facilities Office. The viewing operation must be logged as follows:
 - 3.4.2.1 date/time of the request;
 - 3.4.2.2 register reference number;
 - 3.4.2.3 the name of the person making the request;
 - 3.4.2.4 the reason for the request;
 - 3.4.2.5 date/time/location of the viewing session;
 - 3.4.2.6 the authoriser of the request;
 - 3.4.2.7 name of person managing the viewing session;
 - 3.4.2.8 who was present at the viewing;
 - 3.4.2.9 the name(s) and departments(s) of the viewer(s); and
 - 3.4.2.10 the outcome of the viewing session; and
 - 3.4.2.11 if appropriate, the date/time the images were moved to a secure location for later use for evidential purposes.
- 3.4.3 The rejection of a viewing request must be logged with details of the date/time of the request, the name of the requester, the reason for the request, the name of the authority rejecting the request, and the reason for the rejection.
- 3.4.4 The Estates and Facilities Manager or the duty manager must be consulted prior to any viewing if there is a likelihood of the stored images being used and/or retained for evidential purposes.

3.5 Subject Access Requests

- 3.5.1 Data subjects may make a request for disclosure of their personal information and this may include CCTV images (*data subject access request*). A data subject access request should be directed to the Data Protection Officer in accordance with College's Data Subject Rights Procedure.
- 3.5.2 Images of third parties shall be obscured when disclosing CCTV data as part of a subject access request, or, where it is considered necessary to do so.

4. Licences

- 4.1 The Private Security Industry Act 2001 requires that a Public Space Surveillance CCTV licence is required when CCTV operatives are supplied under a contract for services.
- 4.2 Contracts with any external security firms that operate within the College site must contain clearly defined responsibilities and should include guarantees about security, stipulate that such companies are responsible for the required Public Space Surveillance CCTV licences to cover their personnel, and that they have undertaken appropriate training by the company.

5. Training

- 5.1 Camera operators will be trained in the technical, legal and ethical parameters of appropriate camera use. This may include staff development on cultural awareness if appropriate.
- 5.2 Camera operators will be provided a link to a copy of this policy and provide an email response confirming that they have read and understood its contents.
- 5.3 Camera operators who use more free-hand/zoom features of the CCTV equipment (*i.e., to use it in any way other than the automated camera panning*) must have operator training that complies with current regulations. Applications for such training should be made via the College staff development procedures.
- 5.4 The Estates and Facilities Manager is responsible for providing an induction to the College CCTV system for newly appointed camera operators or security staff.

6. Using the Equipment

- 6.1 The Estates and Facilities Manager and Network Services Manager are responsible in ensuring that there is a regular check that the date and time stamp recorded on the images is accurate.
- 6.2 The Estates and Facilities Manager and Network Services Manager are responsible for a regular maintenance regime to ensure that the system continues to produce high quality images.

7. Complaints

- 7.1 Any complaints received with regard to the use of the CCTV system and/or associated images should be considered via the College complaints procedure.
- 7.2 Concerns about breaches of privacy should initially be directed to the Data Protection Officer. Following the conclusion of any internal investigation; Data Subjects also have the right to contact:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Telephone: 08456 306060 or 01625 545745
www.ico.gov.uk