SWC

POLICIES & PROCEDURES

CCTV Policy

Policy Owner:	Director of Corporate Services
Date Approved:	04 November 2026
Version:	V3.0
Equality Screening Date:	3 November 2022
Date of First Issue:	11 January 2023
Date of Next Review:	October 2028
Location:	Gateway

Contents

1. Introduction 2
2. Policy Purpose 2
3. Policy Aim 2
4. Policy Scope 3
5. Compliance with the Data Protection Act 2018 3
6. Recordings, storage and access 6
7. Applications for disclosure of CCTV images / footage 6
8. Retention of images 8
9. Monitoring and Review 9

Appendix 1 – Request to View CCTV Footage 10

Related Documentation 11

Change Log 11

Communication 11

Communication Plan 11

Document Development 11

Approval Dates 11

Document History 12

1. Introduction

1.1 The College has installed image only (no audio) CCTV surveillance systems on all College owned premises. The College will have due regard to the Data Protection Act, incorporating the General Data Protection Regulation (GDPR), the Freedom of Information Act, the Protection of Freedoms Act and the Human Rights Act.

1.2 Each Campus system comprises of a number of fixed cameras located around each campus site. All CCTV monitors are located in a secure control room and are only accessible to designated staff within that campus.

1.3 The CCTV systems in Erne, Skills Centre, Cookstown, Gortin Road and Kilcronagh campuses are owned and controlled by the College. These cameras are operated by the Estates department. The College is the Data Controller for all CCTV images.

1.4 The CCTV systems in the Omagh and Dungannon campuses are owned by Belfast Educational Services (BES) and operated by Mitie FM as “Appointed Agents” of the College. Where Mitie operate CCTV they do so on behalf of the College as Data Processors.

2. Policy Purpose

2.1 The purpose of this Policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at South West College. The policy details the procedures to be followed in order to ensure that the College complies with relevant legislation and the current Information Commissioner’s Office Code of Practice.

3. Policy Aim

3.1 The aim of the policy is to ensure that the use of CCTV surveillance is proportionate, in compliance with GDPR, and will achieve its stated purpose.

4. Policy Scope

4.1 This Policy applies to all fixed and mobile CCTV and other video-surveillance systems operated by or on behalf of the College at any College premises or location. It applies to all staff, contractors and appointed agents who design, manage, operate, maintain, access, view, extract, disclose or otherwise process CCTV images. Any proposed use of audio recording, automatic number plate recognition, facial recognition, analytics or other enhanced surveillance capability must not be introduced until its necessity, proportionality, lawful basis, security and privacy impacts have been assessed and formally approved following consultation with the Data Protection Officer.

5. Compliance with the Data Protection Act 2018

5.1 Registration and Ownership

The College is the Data Controller for personal data captured by CCTV systems operated by or on its behalf and is registered with the Information Commissioner's Office under registration number Z1124639. Mitie Facilities Management acts as a Data Processor where it operates CCTV on the College's behalf and must process images only on documented College instructions and in accordance with applicable contractual and data protection requirements. The College will identify and document the applicable lawful basis under Article 6 of the UK GDPR, normally the performance of a task carried out in the public interest, and will meet any additional legal conditions where special category or criminal offence data is processed.

5.2 Stated Purpose

5.2.1 The purposes of the CCTV systems are as follows:

- Deterring, prevention and deterrence of a crime including misuse or abuse of College equipment, reduce the fear of crime and increase personal safety.
- Identification, apprehension and prosecution of offenders.
- Security and protection of campus buildings and grounds and College assets internally and externally and identifications of incidents that require a response.
- Safeguarding and health and safety.
- In exceptional circumstances the images may be viewed for investigatory

purposes.

5.2.2 The purpose of the CCTV systems will be reviewed in line with the review cycle of this policy i.e. biennially.

5.3 Privacy

5.3.1 The College will operate CCTV lawfully, fairly and transparently and will ensure that surveillance is necessary and proportionate to a documented purpose. A Data Protection Impact Assessment (DPIA) will be completed before a new system or materially different use is introduced and will be reviewed whenever the purpose, technology, coverage, risk or processing arrangements change. Camera locations and fields of view will be periodically reviewed to minimise unnecessary capture and intrusion.

5.3.2 Cameras will be used to monitor activities within the college buildings, including exterior areas, 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 wellbeing of the college, together with its staff, students and visitors.

5.3.3 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Data, photographic or digital material will only be released to the media for use in the investigation of a specific crime and with the written authority of the police and will never be released to the media for the purposes of entertainment.

5.3.4 Covert surveillance will be considered only in exceptional circumstances where it is necessary and proportionate for a specific investigation and where less intrusive measures would be ineffective. No covert surveillance may begin without consultation with the Data Protection Officer, completion of a DPIA and written authorisation by the Chief Executive. Before authorisation, the College must also determine whether the proposed activity falls within the Regulation of Investigatory Powers Act 2000 or any applicable code of practice and obtain any further authorisation or approval required. The written authority must define the purpose, scope, location, duration, review arrangements, handling of collateral intrusion and arrangements for retention and destruction. Covert surveillance must cease when

the authorised purpose has been achieved or the authority expires.

5.3.5 Wherever practicable cameras will be sited so as to avoid focusing on private residential property.

5.4 Signage

5.4.1 Signs will be placed at pedestrian and vehicular entrances, and prominent internal spaces in order to inform staff, students, visitors and members of the public that CCTV is in operation. The signage indicates that the system is managed by South West College or by Mitie where relevant and a contact number is provided.

5.4.2 The Estates and Sustainability Manager, or Mitie representative, is the designated person responsible for ensuring that adequate signage is erected.

5.5 Responsibility

5.5.1 The person with overall responsibility for the management of the CCTV surveillance systems in College ownership is the Estates and Sustainability Manager. The overall responsibility for the management of the CCTV surveillance systems operated by Mitie is the Operations Manager (Mitie).

5.6 Complaints

5.6.1 Complaints about the CCTV surveillance system can be made through the College's Customer Complaints and Compliments Policy which is available on the College's website and staff and student intranets.

5.7 Monitoring

5.7.1 CCTV monitoring equipment will be located in secure and restricted areas on all sites. Access to these areas will be limited to:

- Senior Caretakers
- Campus Managers
- IT Services Staff
- Data Protection Officer
- Police Officers
- Estates Officers
- Mitie Facilities Manager

- Estates and Sustainability Manager

5.7.2 Unless an immediate response is required, CCTV systems are NOT manned or actively monitored on a regular basis and are NOT located where they can be viewed by any member of staff in that location. Recordings are only viewed as a result of an event or incident or a formal request in line with the College's Procedure for requesting Access to CCTV Images.

6. Recordings, storage and access

6.1 In its administration of its CCTV system, the College complies with the Data Protection Act. Due regard is given to the data protection principles embodied in the Data Protection Act. These principles require that personal data shall be:

a) Processed lawfully, fairly and in a transparent manner;
b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) Accurate and where necessary, kept up to date;
e) Kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed;
f) And processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7. Applications for disclosure of CCTV images / footage

7.1 Applications by individual data subjects for own data

7.1.1 Reviewing or releasing CCTV footage will only be permitted in limited circumstances. Requests by individual data subjects for images relating to themselves (Subject Access Request) should be submitted using the form in Appendix 1 to the relevant Campus Manager or Estates Officer who will consult the

Data Protection Officer.

7.1.2 In order to locate the images on the College's CCTV system, sufficient detail must be provided by the data subject in order to allow the relevant images (if any) to be located and the data subject to be identified.

7.1.3 Where the College is unable to comply with a Subject Access Request without disclosing the personal data of another individual who is identified or identifiable from that information, it is not obliged to comply with the request unless satisfied that the other individual(s) have provided their express consent to the disclosure, or if it is reasonable, having regard to the circumstances, to comply without the consent of the individual.

7.2 Access to and disclosure of images to third parties

7.2.1 A request for images made by a third party should be submitted using the form in Appendix 1 to the Campus Manager or Estates Officer who will consult the Data Protection Officer.

7.2.2 In limited circumstances it may be appropriate to disclose images to a third party, such as when a disclosure is required by law, in relation to the prevention or detection of crime or in other circumstances where an exemption applies under relevant legislation.

7.2.3 Any disclosure will be limited to what is necessary and proportionate and must be authorised by the Data Protection Officer, or by a formally designated nominee in consultation with the Data Protection Officer. The reason, lawful basis, recipient, images disclosed, date, authorising officer and method of secure transfer must be recorded. Where other identifiable individuals appear, appropriate redaction or other safeguards will be applied unless an exemption permits disclosure without them.

7.2.4 If a request is received to view CCTV footage by PSNI, a Form 81 will be requested. However, if a Form 81 is not available, the PSNI officer will be requested to complete the form in Appendix 1.

7.2.5 Where a suspicion of misconduct arises and at the formal request of the Campus

Manager, the Estates Officer or the Appointed Agents may provide access to CCTV images for use in staff or student disciplinary cases.

8. Retention of images

8.1 Unless required for evidential purposes, the investigation of an offence/disciplinary matter or as required by law, CCTV images will be retained for no longer than necessary.

8.2 Where footage is required for an investigation, complaint, claim or legal process, it will be securely exported to an approved encrypted College storage location or encrypted device; access will be restricted to authorised persons and a clear audit trail and chain-of-custody record will be maintained. The footage must not be copied to personal devices or transmitted using unapproved methods. It will be retained only for as long as required for the relevant process and any appeal or legal hold, after which all working and retained copies will be securely deleted or destroyed by the responsible officer in accordance with the FE Sector Retention and Disposal Schedule.

8.3 Images may be held for a longer period where there has been an accident or incident which may have legal repercussions for the College and may be required for evidential purposes. In these circumstances, the footage will be retained by the Health & Safety Officer or the Risk & Compliance Officer and retained until the completion of any legal proceedings in line with the FE Sector Retention and Disposal Schedule. After this period, the footage will be destroyed. [1]

[1] CCTV footage is normally retained for 30 days ie the capacity of the system to store images. Downloaded images required for an investigation or claim will be held until the completion of the investigation or claim in line with the FE Sector Retention and Disposal Schedule.

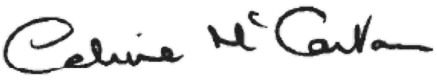
9. Monitoring and Review

9.1 All staff involved in the operation of the College's CCTV System will be made aware of this policy and will only be authorised to use the CCTV System in a way that is consistent with the purposes and procedures contained herein.

9.2 All staff with responsibility for accessing, recording, disclosing or otherwise processing CCTV images will be required to undertake data protection training.

9.3 The Estates and Sustainability Manager, supported by the Data Protection Officer and relevant Campus Managers, will undertake and document periodic compliance checks. These will include camera purpose and positioning, signage, user access permissions, access and disclosure logs, retention and deletion arrangements, processor compliance, security controls, staff training and any complaints or incidents. Identified actions will be assigned, monitored and escalated through the College's governance arrangements as appropriate.

9.4 This Policy will be reviewed on a biennial basis or sooner in the light of legislative changes.

Signed Principal and Chief Executive: 

Date: 04 November 2026

Signed Chair of the Governing Body: 

Date: 04 November 2026

Appendix 1 – Request to View CCTV Footage

Requester's name:	**Date:**
Date of incident requested:	Location of incident:
Approx. time of incident:	Approx. time of incident end:
Nature of incident	
Print name:	Sign:
Please forward this request to the Campus Manager for approval	
I hereby approve the above request to view CCTV footage for the dates and times indicated above. This approval only extends to the written request above and does not extend to any further dates or times. In the first instance, the requested footage should be viewed directly on the CCTV system and should not be copied or extracted. It must be viewed by a minimum of two authorised persons together; no individual is permitted to access or view CCTV footage alone. The names of both viewers, the date and time of viewing and the purpose of access must be recorded. A copy or extract may only be created where this is subsequently demonstrated to be necessary for an authorised investigation, disclosure or legal process, and the reason and approval must be recorded. Following viewing, the footage must remain securely held on, or be returned to, the approved CCTV system or secure College storage, as applicable.	
Signature:	**Date:**
This form will be retained by the CCTV controller as a record of control	

Related Documentation

Title	Location	Owner
Data Protection Policy	Gateway and SWC Website	Risk and Compliance Officer
Customer Complaints and Compliments Policy	Gateway and SWC Website	Risk and Compliance Officer

Change Log

Location	Change from deletion/addition	Change to
Sections 4–9	Expanded scope and strengthened provisions on lawful basis, DPIAs, covert surveillance, access, disclosure, secure extraction, retention, oversight and audit trails.	Updated controls aligned with current data protection and covert-surveillance requirements; issued as V3.0.
	Appendix 1	Update to approval request.

Communication

Who needs to know (for action)	Campus Managers, SWC Estates Staff, Mitie Staff
Who needs to be aware	All Staff, Students, Stakeholders, Visitors All Governing Body Members

Communication Plan

Action	By Whom	By When
Upload to Gateway	Executive Support Officer	On Approval
Circulate to Staff	Director of Corporate Services	On Approval

Document Development

Details of staff who were involved in the development of this policy:

Name	Role
Martin Devlin	Estates Officer
Joanne Lucas	Data Protection Officer

Details of staff, external groups or external organisations who were consulted in the development of this policy:

Name	Organisation	Date
Sharon McGrath	Director of Corporate Services	28/09/26
Rachel Elliott	Estates and Sustainability Manager	28/09/26
Paul Wade	Head of IT Services	28/10/22
Pamela Corrigan	Information Security Officer	28/10/22

Approval Dates

Approved by	Date
Governing Body	04 November 2026

Document History

Issue no. under review	Date of review:	Persons involved in review	Changes made after review? Yes/No If Yes refer to change log	New Issue No.	If changes made was consultation required?	If changes made was Equality Screening required?
V1.0	January 2025		Yes	V2.0		
V2.0	September 2026	Sharon McGrath Rachel Elliott	Yes	V3.0	No	No