CCTV and IMAGE CAPTURE POLICY

Document Details			
Policy Number	MKC-Facilities-001	**No. of Appendices**	**0**
Document Title	**CCTV and Image capture Policy 2024 - 2026**		
Document Description			
Effective Date	**November 2023**	**Review Date**	**November 2027**
Version Number	**V1.0**	**Review Cycle**	**2 Years**
Document Status	**In review**	**New Policy**	**No**
Contact Details	Data.protection@midkent.ac.uk		

Document Authorisation				
	Authorisation Required	**Initial and Role**	**Digital Signature**	**Date**
Author	Yes	HF – Data Protection Officer	*Hazel Foreman*	5 Nov 23
Owner	Yes	MP – Executive Director for Finance and estates		
SLT Review	Yes	N/A		
Exec Approver	Yes			
GB Sub Committee	Yes – GR&A for major updates			
Full GB Committee	Yes – if required			

Policy Cross References - This policy should be read in conjunction with any other associated policies, with particular reference to	
Policy Name	**Policy Number**
Safeguarding Policy	
ICT Policies	
CCTV Policy	
Freedom of Information Policy	
Disciplinary Policy for students and staff	

Document Revision History		
Version Number	**Date**	**Summary of Revision**
V1.0	November 2023	• Update on CCTV numbers and locations. • Updates on job titles. • Addition of item 9 student disciplinary

Contents

1. Introduction

MidKent College "the College" maintains video image surveillance technology (CCTV) on both campuses. This policy details the purpose, use and management of the system at the College and identifies the procedures that must be followed to ensure the College complies with relevant legislation and codes of practice.

This policy is based on the Information Commissioners Office (ICO) code of practice covering surveillance by CCTV.

> "This code also reflects the wider regulatory environment. When using, or intending to use surveillance systems, many organisations also need to consider their obligations in relation to the Freedom of Information Act 2000 (FOIA), the POFA, the Human Rights Act 1998 (HRA) and the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act (POFA code)."

Amended Surveillance Camera Code of Practice (accessible version) - GOV.UK (www.gov.uk)

2. Scope and Aim of Policy

This policy and associated procedures applies to all CCTV systems including webcams and any other systems capturing images of identifiable individuals for the purpose of viewing or recording the activities of such individuals. These systems fall into two categories.

Category 1: The principle purposes of the CCTV and snow camera systems are as follows:

- To identify incidents requiring a response e.g. heavy snowfall, severe frost or flooding**.**

Category 2: From time-to-time, other camera systems e.g. time-lapse, drones, I-pads, GoPro's, 360 cameras, DLSR etc. may be in operation and the principle purposes of these are:

- To record staff and student activity in a teaching environment for educational and staff development purposes. In accordance with the relevant Privacy Notification;
- To record meetings as an accurate record or for training purposes. In accordance with the relevant Privacy Notification; and
- For marketing and promotional activity. In accordance with the relevant Privacy Notification and where informed consent has been obtained and recorded.

3. Operational Considerations

The operation of both categories of systems must be consistent with individuals' rights to privacy. Images are likely to be personal data as defined by current data protection legislation and must be processed in accordance with the law, kept secure and destroyed within the agreed retention period.

4. Procedures

a. Covert Monitoring

The College Principal is the only person that can authorise the use of covert monitoring. The request must be made in writing along with a DPIA. The decision must take into account the information contained in the DPIA, be recorded on the paperwork and then passed to the Data Protection Officer (DPO). The use of covert monitoring will be rare, only considered where all other options have been explored and time limited based on the stated purpose.

b. Third Party data requests

Request by third parties for access to or disclosure of images must be made in writing to the Information Governance Team.

c. Subject Access Requests

Staff, students and members of the public can access images relating to themselves but submitting and Data Subject Access Request. All requests are handled by the Information Governance Team.

This process is detailed in the Data Subject Access Request Procedure (GDPR DOC 2.2).

5. Signage for Category 1 operations

Signs are prominently displayed on the main inbound pedestrian and vehicular routes. The signage informs people that CCTV monitoring is in use, that MidKent College are responsible for the system, where further information can be found and provides a contact number.

6. Monitoring and Recording

Category 1 cameras can be monitored from computer equipment but access is limited to Authorised People and is controlled through username and password authentication. Authorised People are provided with Home Office licensed radio equipment to facilitate a response across each campus where an incident requires it.

Some category 2 cameras can be monitored from mobile devices and other computer devices but access is limited to Authorised People and is controlled through username and password authentication.

The Category 1 image recording equipment is situated in nominated secure rooms on each campus. System access is limited to Authorised People and is controlled through username and password authentication.

Category 1 and 2 recorded images are stored in accordance with the College's Data Retention Policy and will be subject to the college's standard back-up routines.

A list of Authorised People is in Appendix 1.

7. Viewing Images

The viewing of Category 1 images with identifiable living individuals can only be conducted by any of the Authorised Persons. This operation shall be conducted in a private area and with at least one other Authorised Person present. A log must be maintained of image viewing. The log should show why it was done, who was present, when and other relevant information.

The viewing of Category 2 images can only be conducted in accordance with the Privacy Notice and the lawful processing condition identified.

a. Copying Images for disclosure – Category 1

The Facilities Director or their nominated deputy is responsible for authorising this activity and for the security, storage and access to the copies of images.

The copying of images with identifiable living individuals can only be conducted by any of the Authorised Persons who hold a current SIA/CCTV endorsement license. This operation shall be conducted in a private area and with at least one other Authorised Person present. The copying of images is restricted to where they may be used at a later date as evidence, where the date will be beyond the stated retention period. A report should be produced showing why it was done, who was present, when and other relevant information, this should be passed to the DPO without delay.

An annual review will be conducted to cover compliance with legislation, effectiveness against stated objectives and that current safeguards are appropriate.

b. Copying Images for disclosure – Category 2

The copying of Category 2 images can only be conducted in accordance with the Privacy Notice and the lawful processing condition identified. Refer to the Data Protection policy.

8. Staff Disciplinary

Where a suspicion of misconduct arises and a formal request from the Director of People has been made, the Head of Facilities may provide access to images for the use in staff disciplinary cases. If needed, advice should be sought from the DPO.

9. Student Disciplinary

Where a suspicion of misconduct arises and a formal request from the Duty Manager or Principle or appropriate of teaching staff has been made, the Head of Facilities may provide access to images for the use in staff disciplinary cases. If needed, advice should be sought from the DPO.

10. Duties and Responsibilities

The College Principal is accountable for the CCTV operations.

The Executive Director of Finance and Estates is responsible for compliance with and implementation of this policy.

The Facilities Manager is responsible for the overall management and operation of the Category 1 CCTV systems, including activities relating to signage, installations, recording, reviewing, monitoring and data destruction in accordance with the documented data retention period. Retention of Records Procedure (GDPR DOC 2.3)

The Deputy Principal is responsible for the overall management and operation of the Category 2 systems, including activities relating to signage, installations, recording, reviewing, monitoring and data destruction in accordance with the documented data retention period. Retention of Records Procedure (GDPR DOC 2.3)

The DPO is responsible for advising on compliance with current Data Protection Legislation and other legislation in relation to surveillance technology.

Complaints or queries regarding the use of CCTV equipment at the College should be made in writing to the Data Protection Officer at data.protection@midkent.ac.uk These will be recorded and passed on to the Facilities Manager along with the DPO's advice. Any appeals following decisions made by the Facilities Manager will follow the College's usual appeals process.

The Director of People and Payroll is responsible for adequately training all staff monitored by and/or operating category 1 & 2 systems, and that staff have the required operator's license where needed under this policy. The minimum will be at induction and then at least annually. Should a data breach occur then staff from the area(s) concerned may be required to undertake further training.

11. Associated Policies and Procedures

- Examinations policy
- Data Protection policy
- Data Retention policy
- Health and Safety policy
- Data Subject Access Request procedure

12. Appendix 1 – Authorised People

A. Authorised People – Category 1

a. College Principal or their deputy
b. College Executive Directors
c. Student Liaison Behaviour Officer
d. Security Officers
e. Facilities Manager
f. Contracted Security assigned officers
g. Duty Managers
h. Senior Caretakers
i. Contracted CCTV maintenance and service engineers
j. College ICT team for the purposes of system security and maintenance

B. The following people may be authorised by the Facilities Manager, who are based at each campus, on a case to case basis to enable investigations to be undertaken

a. Police/PCSO
b. Staff who are not Authorised People
c. Data subject(s)
d. Insurance company
e. CITB for the purposes of ensuring compliance with CSCS Card examination procedures and rules
f. Awarding Organisations for the purposes of ensuring compliance with examination procedures and rules

C. Following people are authorised to produce copy files for the purpose of evidence

a. Any of the Authorised Persons who also hold a current SIA Public Space Surveillance (CCTV) license.

D. Authorised People – Category 2

a. Members of the teaching staff with their manager's approval.
b. Members of the Advanced Practitioners team.
c. Members of the Marketing team or their contracted agents.
d. Members of the Authorised People – Category 1

13. Appendix 2 – Camera Details/Locations

Medway Campus (30 days)

59 CCTV cameras
3 Snow cameras

Maidstone Campus (30 days)

Main Building Controlled

64 CCTV cameras
2 Snow cameras

UCM Building Controlled

119 CCTV cameras
1 Snow cameras

Skills factory

11 CCTV cameras

Car Park and roadway Controlled.

8 CCTV cameras