Closed Circuit Television (CCTV) Policy

SAE UK and ICMP operate as trading names of ICMP Management Limited ("ICMP Management"). References to ICMP Management throughout this policy incorporate both SAE UK and/or ICMP, according to the context.

1. Statement of Intent

1.1. At ICMP Management CCTV is used to monitor any instances of aggression or physical damage to our building, our equipment and our staff, students and visitors. The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at campuses and ensure that:

1.1.1. We comply with data protection legislation, including the Data Protection Act 2018 and the General Data Protection Regulation (GDPR)

1.1.2. The images that are captured are useable for the purposes we require them for.

1.1.3. We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

1.2. This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

1.2.1. Observing what an individual is doing.

1.2.2. Taking action to prevent a crime.

1.2.3. Using images of individuals that could affect their privacy.

2. Legal Framework

2.1. This policy has due regard to legislation and statutory guidance, including, but not limited to the following:

2.1.1. The Regulation of Investigatory Powers Act 2000

2.1.2. The Protection of Freedoms Act 2012

2.1.3. The General Data Protection Regulation (GDPR)

2.1.4. The Data Protection Act 1998
2.1.5. The Freedom of Information Act 2000
2.1.6. The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
2.1.7. The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
2.1.8. The School Standards and Framework Act 1998
2.1.9. The Children Act 1989
2.1.10. The Children Act 2004
2.1.11. The Equality Act 2010

2.2. This policy has been created with regard to the following statutory and non-statutory guidance:
2.2.1. Home Office (2013) The Surveillance Camera Code of Practice
2.2.2. Information Commissioner's Office (ICO) (2017) 'Overview of the General Data Protection Regulation (GDPR)'
2.2.3. ICO (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
2.2.4. ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'

2.3. This policy operations in conjunction with the following ICMP Management policies:
2.3.1. ICT Acceptable Use Policy
2.3.2. Facilities Acceptable Use Policy
2.3.3. Health and Safety Policies and Procedures
2.3.4. Access and Monitoring Policy

3. Definitions

3.1. For the purpose of this policy a set of definitions will be outlines, in accordance with the surveillance code of conduct:
3.1.1. **Surveillance** – monitoring the movements and behaviour of individuals; this can include video, audio or live footage. For the purpose of this policy only video footage is currently applicable.
3.1.2. **Overt surveillance** – any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000.

3.1.3. **Covert surveillance** – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.

3.2. ICMP Management does not condone the use of covert surveillance when monitoring ICMP Management's staff, students and/ or volunteers.

3.3. Any overt surveillance will be clearly signposted around ICMP Management campuses .

4. Roles and responsibilities

4.1. The role of the Data Protection Officer (DPO) includes:

4.1.1. Dealing with freedom of information requests and subject access requests (SAR) in line with legislation, including the Freedom of Information Act 2000.

4.1.2. Ensuring that all data controllers in ICMP Management handle and process surveillance and CCTV footage in accordance with data protection legislation.

4.1.3. Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.

4.1.4. Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.

4.1.5. Keeping comprehensive and accurate records of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity and making these records public upon request.

4.1.6. Informing data subjects of how their data captured in surveillance and CCTV footage will be used by ICMP Management, their rights for the data to be destroyed and the measures implemented by ICMP Management to individuals' personal information.

4.2. ICMP Management, as the corporate body, is the data controller. The governing board of ICMP Management therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

4.3. ICMP Management is the data controller.

4.4. On behalf of ICMP Management the day to day role of the Estates Team

4.4.1. Archiving surveillance Archiving surveillance and CCTV footage only for legitimate reasons and ensuring that it is used accordingly.

4.4.2. Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection.

4.4.3. Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.

4.4.4. Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure - especially when processing over networks.

4.4.5. Meeting with the DPO to decide where CCTV is needed to justify its means.

4.4.6. Conferring with the DPO with regard to the lawful archiving of the surveillance and CCTV footage.

4.4.7. Reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation.

4.4.8. Monitoring legislation to ensure ICMP Management is using surveillance fairly and lawfully.

5. Purpose and justification

5.1. The purpose of ICMP Management CCTV surveillance footage is for the legitimate health and safety concerns for the staff, students and property.

5.2. ICMP Management will only use surveillance cameras for the safety and security of the campus and its staff, students and visitors.

5.3. Surveillance will be used as a deterrent for violent behaviour and damage to the college.

5.4. ICMP Management will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in classrooms or any changing facility.

5.5. If the surveillance and CCTV systems fulfil their purpose and are no longer required the campus team will deactivate them.

5.6. Systems with cameras that overlap with areas outside of the campus are set to only record when motion is detected on the portions of the image that are within ICMP Management property (recording is not triggered by motion outside of ICMP Management property).

5.7. The privacy impact of the ICMP Management CCTV system is minimal with archiving only in the event of a reported incident and cameras only recording when motion is detected within campus grounds.

6. The data protection principles

6.1. Data collected from surveillance and CCTV will be:

6.1.1. Processed lawfully, fairly and in a transparent manner in relation to individuals.

6.1.2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

6.1.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6.1.4. 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. Objectives

7.1. The surveillance system will be used to:

7.1.1. Maintain a safe environment.

7.1.2. Ensure the welfare of students, staff and visitors.

7.1.3. Deter criminal acts against persons and property.

7.1.4. Assist the police in identifying persons who have committed an offence.

7.2. **Storage**

7.2.1. In all locations, the CCTV systems are set to ‘rolling record’ whereby older footage is automatically overwritten by newer footage ensuring that without intervention no footage is automatically archived.

7.2.2. Only in the event of a known or reported incident is the CCTV footage copied from the devices in order to be processed and/or stored for longer periods,

and then only for as long as is needed for the defined purposes within this policy.

7.2.3. The maximum time of rolling footage stored on systems is limited to a period of one calendar month. This should be long enough that in the event of a major incident requiring police attention we can access footage that may be of use but not so long that footage is kept unnecessarily.

8. Protocols

8.1. The surveillance system will be registered with the ICO in line with data protection legislation, https://ico.org.uk/

8.2. The surveillance system is a closed system which does not record audio.

8.3. Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice.

8.4. The surveillance system will not be trained on private vehicles or property outside the perimeter of ICMP Management campuses but will be covering the ICMP Management designated car park areas.

9. Security

9.1. Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected.

9.2. ICMP Management's authorised CCTV system operators/viewers are:

9.2.1. Head of IT & DPO

9.2.2. Head of Estates and Facilities, Facilities Manager and Facilities Supervisor

9.2.3. Campus Manager

9.2.4. Chief Operating Officer

9.2.5. Chief Executive Officer

9.3. The main CCTV facility is kept secure and locked when not in use.

9.4. Surveillance and CCTV systems will be tested for security flaws annually to ensure that they are being properly maintained at all times.

9.5. Surveillance and CCTV systems will not be intrusive.

9.6. Any unnecessary footage captured will be securely deleted from ICMP Management systems.

9.7. Any cameras that present faults will be repaired as soon as is possible as to avoid any risk of a data breach.

9.8. The CCTV system can be accessed on the personal computers of the Head of IT, Head of Estates and Facilities, Facilities Manager, Facilities Supervisor, CEO, COO and IT Support team.

10. Code of practice

10.1. ICMP Management understands that recording images of identifiable individual constitutes as processing personal information, so it is done in line with data protection principles.

10.2. ICMP Management notifies all students, staff and visitors of the purpose for collecting surveillance data via signs in the school grounds.

10.3. CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

10.4. All surveillance footage will be kept for approximately one month for security purposes; the Head of Estates and Facilities & Head of IT and the data controller are responsible for keeping the records secure and allowing access.

10.5. ICMP Management has a surveillance system for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, students and visitors.

10.6. The surveillance and CCTV system is owned by ICMP Management and images from the system are strictly controlled and monitored by authorised personnel only.

10.7. ICMP Management will ensure that the surveillance and CCTV system is used to create a safer environment for staff, students and visitors to the college, and to

ensure that its operation is consistent with the obligations outlined in data protection legislation.

10.8. The surveillance and CCTV system will:

10.8.1. Be designed to take into account its effect on individuals and their privacy and personal data.

10.8.2. Be transparent and include a contact point, the DPO, through which people can access information and submit complaints.

10.8.3. Have clear responsibility and accountability procedures for images and information collected, held and used.

10.8.4. Have defined policies and procedures in place which are communicated throughout ICMP Management

10.8.5. Only keep images and information for as long as required.

10.8.6. Restrict access to retained images and information with clear rules on who can gain access.

10.8.7. Consider all operational, technical and competency standards, relevant to the surveillance and CCTV system and its purpose, and work to meet and maintain those standards in accordance with the law.

10.8.8. Be subject to stringent security measures to safeguard against unauthorised access.

10.8.9. Be subject to regular review and audit to ensure that policies and standards are maintained.

10.8.10. Only be used for the purposes for which it is intended, including supporting public safety, the protection of students, staff and volunteers, and law enforcement.

11. Access

11.1. Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed.

11.2. All disks containing images belong to, and remain the property of, ICMP Management.

11.3. Individuals have the right to submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing.

11.4. ICMP Management will verify the identity of the person making the request before any information is supplied.

11.5. A copy of the information will be supplied to the individual free of charge; however, ICMP Management may impose a 'reasonable fee' to comply with requests for further copies of the same information.

11.6. Where an SAR has been made electronically, the information will be provided in a commonly used electronic format.

11.7. Requests by persons outside ICMP Management for viewing or copying disks, or obtaining digital recordings, will be assessed by the Head of Estates and Facilities & Head of IT, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.

11.8. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

11.9. Requests for information should be submitted in writing (via letter or email) in order that the process can be documented.

11.10. All fees will be based on the administrative cost of providing the information.

11.11. All requests will be responded to as soon as is practical and at the latest within one month of receipt. Unless footage has been archived there will be no scope for accessing CCTV footage beyond that.

11.12. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

11.13. Where a request is manifestly unfounded or excessive, ICMP Management holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal.

11.14. In the event that a large quantity of information is being processed about an individual, ICMP Management will ask the individual to specify the information the request is in relation to.

11.15. It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.

11.16. Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

11.16.1. The police - where the images recorded would assist in a specific criminal inquiry.

11.16.2. Prosecution agencies - such as the Crown Prosecution Service (CPS).

11.16.3. Relevant legal representatives - such as lawyers and barristers.

11.16.4. Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000.

11.17. Requests for access or disclosure will be recorded and the DPO will make the final decision as to whether recorded images may be released to persons other than the police.

12. Monitoring and review

12.1. This policy will be monitored and reviewed periodically, or in light of any changes to relevant legislation by the DPO and the data controllers.

12.2. The data controllers will be responsible for monitoring any changes to legislation that may affect this policy and make the appropriate changes accordingly.

12.3. The data controllers will communicate changes to this policy to all members of staff.

Version number	Date approved (including committee)	Reason for production/revision	Author	Proposed next review date
V1.3	Mar 2025, ExCo	Review following merger	Head of Estates	Triennially and as required
V1.2	Nov 2020 HSS	Annual review	IT Manager	Biennially and as required

Related policies
• ICT Acceptable Use Policy • ICT Acceptable Use Policy • Facilities Acceptable Use Policy • Health and Safety Policies and Procedures • Access and Monitoring Policy • FOI Policy

External Reference
• The Regulation of Investigatory Powers Act 2000 • The Protection of Freedoms Act 2012 • The General Data Protection Regulation (GDPR) • The Data Protection Act 1998 • The Freedom of Information Act 2000 • The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016) • The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 • The School Standards and Framework Act 1998 • The Children Act 1989 • The Children Act 2004 • The Equality Act 2010