Kent Catholic Schools' Partnership

'Academies in Christ'
Part of the Archdiocese of Southwark

CCTV Policy

Date of last review	November 2020	Date of next review:	November 2022
Author:	Policy & Projects Mgr	Owner:	Trust Data Protection Officer
Type of policy:	Trust-wide	Approval:	Audit Committee

Contents

1. Purpose

1.1 The Purpose of this Policy is to regulate the management, operation and use of the CCTV System (Closed Circuit Television) within all academies that are part of the Kent Catholic Schools Partnership ("the Trust"). CCTV systems are installed on academy premises for the purpose of enhancing security of the buildings and its associated equipment as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation within and/or in the external environs of the premises during both the daylight and night hours each day.

1.2 As set out in the Trust Data Protection Policy, CCTV surveillance is intended to:

- protect the academy buildings and their assets;
- increase personal safety and reduce the fear of crime;
- support the Police in a bid to deter and detect crime;
- assist in identifying, apprehending and prosecuting offenders;
- provide evidence for the Trust to use in its internal investigations and / or disciplinary processes in the event of behaviour by staff, pupils or other visitors on the site which breaches or is alleged to breach the Trust's policies;
- protect members of the academy community, public and private property; and
- assist in managing the academy.

1.3 The system does not have sound recording capability.

1.4 The CCTV system is owned and operated by the academy, the deployment of which is determined by the Executive Principal or Headteacher.

1.5 The use of CCTV in Trust academies is registered with the Information Commissioner under the terms of the Data Protection Act 2018 and the General Data Protection Regulations (GDPR).

2. Scope

2.1 This Policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material. The academy complies with the Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and

safeguards both trust and confidence in its use. The Code of Practice is published at: https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

2.2 CCTV warning signs will be clearly and prominently placed at the main external entrance to the academy. Signs will contain details of the purpose for using CCTV. In areas where CCTV is used, the academy will ensure that there are prominent signs placed within the controlled area.

2.3 The planning and design have endeavoured to ensure that the system will give maximum effectiveness and efficiency, but it is not guaranteed that the system will cover or detect every single incident taking place in the areas of coverage.

2.4 CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with the provisions set down in equality and other educational and related legislation. This Policy prohibits monitoring based on the characteristics and classifications contained in equality and other related legislation e.g. race, gender, sexual orientation, national origin, disability etc. Video monitoring of public areas for security purposes within academy premises is limited to uses that do not violate the individual's reasonable expectation to privacy.

2.5 Information obtained in violation of this Policy may not be used in a disciplinary proceeding against an employee of the academy or a student attending the academy.

2.6 All CCTV systems and associated equipment will be required to be compliant with this Policy. Recognisable images captured by CCTV systems are 'personal data'. They are therefore subject to the provisions of the General Data Protection Regulation and Data Protection Act 2018.

3. Location of cameras

3.1 Cameras must be sited so that they only capture images relevant to the purposes for which they have been installed (as described above), and care will be taken to ensure that reasonable privacy expectations are not violated. The academy will ensure that the location of equipment is carefully considered to ensure that the images captured comply with the legislation.

3.2 The academy will make every effort to position the cameras so that their coverage is restricted to the academy premises, which includes both indoor and outdoor areas.

3.3 CCTV will not be used in staff rooms, classrooms, changing rooms or toilet facilities but may be positioned to monitor corridors and access to these locations, and will be used in limited areas within the academy that have been identified by staff as not being easily monitored.

3.4 Cameras will be in plain sight and not hidden from view and members of staff will have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring.

3.5 CCTV Video Monitoring and Recording of Public Areas may include the following:

- Protection of academy buildings and property: The building's perimeter, entrances and exits, lobbies and corridors, special storage areas, cashier locations, receiving areas for goods/services
- Monitoring of Access Control Systems: Monitor and record restricted access areas at entrances to buildings and other areas
- Verification of Security Alarms: Intrusion alarms, exit door controls, external alarms
- Video Patrol of Public Areas: Parking areas, Main entrance/exit gates, Traffic Control
- Criminal Investigations (carried out by the police): Robbery, burglary and theft surveillance

4. Notification - Signage

4.1 Adequate signage must be clearly and prominently placed where CCTV cameras are sited to indicate that CCTV is in operation. Signage should be placed at Academy external entrance(s), in the reception area and entrance areas and be in a visible location readable by all staff, pupils and visitors.

4.2 Signs must contain details of the purpose for using CCTV for example: security of academy estate and property.

5. Covert Monitoring

5.1 The Trust retains the right in exceptional circumstances to set up temporary covert monitoring. For example:

- Where there is good cause to suspect that an illegal or serious unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;
- Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

5.2 In circumstances where covert monitoring may be required, authorisation must be obtained beforehand from the Executive Principal/ Headteacher and the Trust Data Protection Officer prior to any purchase or use of equipment.

5.3 Covert Monitoring may take place in classrooms when circumstances as above are satisfied. Covert Monitoring used in classrooms will never be used to observe or assess a teacher's professional performance, or to contribute to capability proceedings. Covert Monitoring will cease following completion of an investigation. Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example, toilets.

6. Storage and retention of CCTV images

6.1 The Data Protection Act and GDPR does not prescribe any specific minimum or maximum retention periods that apply to all systems or footage. Therefore, retention will reflect the Trust's purposes for recording information, and how long it is needed to achieve this purpose.

6.2 Where possible, CCTV storage must be contained in a secure lockable location, i.e. a server room.

7. Access to CCTV Images

7.1 Access to, and disclosure of, recorded images will be restricted. This is to safeguard the rights of individuals and also to ensure that evidence remains intact should images be required for criminal or disciplinary purposes.

7.2 The Viewing Station for the CCTV system must be in a secure location and not overlooked by pupils. The Viewing Station must contain a log-in and password and the User must lock the screen when not in use.

7.3 The Executive Principal/Headteacher may delegate the administration of the CCTV System to another staff member. When CCTV recordings are being viewed, access will be limited to authorised staff members only.

8. Subject Access Requests (SAR)

8.1 Individuals have the right to request CCTV footage relating to themselves under the Data Protection Act and the GDPR. All requests should be made in writing to the Data Protection Officer who can be contacted by email to dpo@kcsp.org.uk. Individuals submitting requests for access will be asked to provide sufficient information to enable footage relating to them to be identified. For example: name, time, date and location of footage, contact details.

8.2 Any CCTV footage which may be provided to an individual as part of a SAR, must have images of other Data Subjects redacted. Where the academy does not have a facility to provide copies of CCTV footage to an individual upon receipt of a SAR, the applicant may be able to view the CCTV footage if available under supervision.

8.3 The Trust reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

9. Access and disclosure of images to third parties

9.1 There will be no disclosure of recorded data to third parties other than authorised personnel such as the Police and service providers to the academy where these would reasonably need access to the data (e.g. investigators).

9.2 If an order is granted by a Court for disclosure of CCTV images, then this should be complied with. However, very careful consideration must be given to exactly what the Court order requires. The Trust Data Protection Officer must be contacted (dpo@kcsp.org.uk) in the first instance before being complied with and appropriate legal advice may be required.

9.3 The data may be used within the Trust's behaviour, discipline and grievance procedures for staff and pupils as required and will be subject to the usual confidentiality requirements of those procedures.

10. Breaches of this Policy

10.1 Any breach of this Policy will be immediately investigated by the Executive Principal / Headteacher or the Trust Data Protection Officer, who will investigate and take appropriate, corrective action.

10.2 There are no exceptions to this Policy.

11. Responsibilities

11.1 The Executive Principal/Headteacher will:

- Ensure that all authorised operators with access to images are aware of the procedures that need to be followed when accessing the recorded images.
- Ensure that all operators are made aware of their responsibilities in following the ICO CCTV Code of Practice.
- Ensure that all employees are aware of the restrictions in relation to access to, and disclosure of recorded images.
- Ensure that the use of CCTV systems is implemented in accordance with this Policy.
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within the Academy.
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this Policy.

- Ensure that the CCTV monitoring is consistent with the highest standards and protections.
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this Policy.
- Maintain a record of access (e.g. an access log) to or the release of tapes or any material recorded or stored in the system.
- Ensure that monitoring recorded tapes are not duplicated for release without authorisation from the Data Protection Officer.
- Ensure that the perimeter of view from fixed location cameras conforms to this Policy both internally and externally.
- Consider both pupil and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment.
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the academy and be mindful that no such infringement is likely to take place.
- Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy"
- Ensure that monitoring tapes are stored in a secure place with access by authorised personnel only
- Ensure that images recorded on tapes/DVDs/digital recordings are stored for a period not longer than is necessary and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by the Executive Principal/ Headteacher.
- Ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy.
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics.
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas.

11.2 The Data Protection Officer will:

- Oversee the response to any Subject Access Requests and the release of any CCTV footage
- Approve any plans for covert monitoring.

11.3 The CCTV Operator(s) will :

- Keep the system secure and operate within the constraints of this Policy;
- Provide footage when requested from the Executive Principal/Headteacher or Data Protection Officer within the data protection mandated timeframes;
- Manage the day-to-day use of the system;
- Ensure that no unauthorised individuals have access to the CCTV at any time;
- Lock any Viewing Station when away from the system.

12. Data Protection Impact Assessments and Privacy by Design

12.1 CCTV has the potential to be privacy intrusive. The academy, in consultation with the DPO, will perform a Data Protection Impact Assessment when installing or moving CCTV cameras to consider the privacy issues involved with using new surveillance systems to ensure that the use is necessary and proportionate and address a pressing need identified.