Surveillance and CCTV Policy

Responsibility for Review: School and college trust leaders
Date of Last Review: July 2025

Surveillance and CCTV policy: document provenance

Approver	School and college trust leaders
Date of approval	2 July 2025
Policy owner	Accounting officer
Policy authors	School and college trust leaders, data protection officer
Version	2.0
Date of next review	September 2027
Summary of changes in this review	• Additional information relating to data subjects' rights for subject access requests is included in item 12 • Additional information relating to how CCTV footage links with safeguarding has been added in item 12 • New clause in section 12 to provide clarity regarding parents viewing CCTV footage • New clause in section 12 to provide clarity around viewing CCTV footage for disciplinary hearings • New clause in section 12 to explain that staff and parents cannot access CCTV footage to provide evidence to car insurance companies with a personal insurance claim.
Related policies and documents	• The Freedom of Information Policy • Data Protection Policy • The Surveillance Camera Code of Practice March 2022 • Home Office (2013) 'The Surveillance Camera Code of Practice' • ICO (2017) 'Overview of the General Data Protection Regulation (GDPR)' • ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information' • Keeping Children Safe in Education (current version)

Unless there are legislative or regulatory changes in the interim, the policy will be reviewed as per the review cycle. Should no substantive change be required at this point, the policy will move to the next review cycle.

Contents

1.0 Policy statement

At Dixons Academies Trust, we take our responsibility towards the safety of students, staff and visitors very seriously, and in particular our duty to safeguard and promote the welfare of our students, including through effective behaviour management and maintaining a safe environment. To that end, we use surveillance cameras to monitor any instances of inappropriate behaviour, or physical damage to our academies, whether it is by a student, staff member or another person.

The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at the academy and ensure that:

- the images that are captured are useable for the purposes we require them for
- the images that are captured are used appropriately and in the best interests of our students first and foremost
- we reassure those persons whose images are being captured that the images are being handled in accordance with GDPR and data protection legislation

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:

- observing what an individual is doing
- taking action to prevent a crime
- using images of individuals that could affect their privacy
- investigating any accidents (or 'near misses'), incidents, allegations

2.0 Legal framework

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

- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The General Data Protection Regulation
- 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

2.2 This policy has been created with regard to the following statutory and non-statutory guidance:

- Home Office (2013) 'The Surveillance Camera Code of Practice'
- ICO (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'
- Keeping Children Safe in Education 2024
- Freedom of Information Policy
- GDPR Data Protection Policy
- The Surveillance Camera Code of Practice March 2022, issued by The Biometrics and Surveillance Camera Commissioner

3.1 Definitions

3.1 For the purpose of this policy a set of definitions will be outlined, in accordance with the surveillance code of conduct:

- surveillance – monitoring the movements and behaviour of individuals; this can include video, audio or live footage. For the purpose of this policy only video and audio footage will be applicable

- overt surveillance – any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000
- 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 Dixons Academies Trust does not condone the use of covert surveillance when monitoring the academy's staff, students and / or volunteers. Covert surveillance will only be operable in extreme circumstances.

3.3 Any overt surveillance footage will be clearly signposted around the academy.

4.0 Objectives

4.1 The surveillance system will be used to:

- maintain a safe environment
- promote the welfare of students, staff, and visitors
- deter criminal acts against persons and property
- assist the police in identifying persons who have or may have committed an offence
- inform other investigations or meet our trusts regulatory or other legal obligations as necessary.

5.1 Roles and responsibilities

5.1 The role of the data protection officer (DPO) includes:

- dealing with freedom of information requests and subject access requests (SAR) in line with legislation, including the Freedom of Information Act 2000
- ensuring that all data controllers at the academy handle and process surveillance and CCTV footage in accordance with data protection legislation
- ensuring that surveillance and CCTV footage is obtained in line with legal requirements
- ensuring consent is clear, positive and unambiguous - pre-ticked boxes and answers inferred from silence are non-compliant with the GDPR
- ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- 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
- informing data subjects of how their data captured in surveillance and CCTV footage will be used by the academy, their rights for the data to be destroyed and the measures implemented by the academy to protect individuals' personal information
- preparing reports and management information on the academy's level of risk related to data protection and processing performance
- reporting to the highest management level of the trust, ie the board of trustees
- abiding by confidentiality requirements in relation to the duties undertaken while in the role
- monitoring the performance of the academy's data protection impact assessment (DPIA) and providing advice where requested
- presenting reports regarding data processing at the academy to senior leaders and the trust

5.2 Dixons Academies Trust, as the corporate body, is the data controller. The board of trustees of Dixons Academies Trust therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

5.3 The administration manager deals with the day-to-day matters relating to data protection and thus, for the benefit of this policy will act as the data controller.

5.4 The role of the data controller includes:

- processing surveillance and CCTV footage legally and fairly
- collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly

- collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection
- ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary
- protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure – especially when processing over networks

5.5 The role of the principal includes:

- meeting with the DPO to decide where CCTV is needed to justify its means
- conferring with the DPO with regard to the lawful processing of the surveillance and CCTV footage
- reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation
- monitoring legislation to ensure the academy is using surveillance fairly and lawfully
- communicating any changes to legislation with all members of staff

5.6 The role of the Designated Safeguarding Lead includes:

- working closely with the wider senior leadership and pastoral teams to identify when CCTV should be accessed
- ensuring that CCTV access is being used appropriately as part of the academy's duty to safeguard and promote the welfare of students
- being able to access CCTV efficiently in safeguarding and welfare situations where time is an exacerbating factor
- being able to delegate review of CCTV footage to a Deputy Designated Safeguarding lead or, when appropriate, another colleague
- taking a lead on ensuring any safeguarding or welfare concern raised is followed up and recorded in line with the Safeguarding Child Protection Policy and the most recent version of Keeping Children Safe in Education
- communicate any issues with their academy's surveillance and CCTV system to the principal

6.0 Purpose and justification

6.1 The academy will only use surveillance cameras for the safety and security of the academy and its staff, students, and visitors.

6.2 Surveillance will be used as a deterrent for inappropriate behaviour and damage to the academy.

6.3 The academy will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in toilet cubicles or any changing facility.

7.0 The data protection principles

7.1 Data collected from surveillance and CCTV will be:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and, where necessary, kept up to date; every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- 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

8.0 Protocols

8.1 The surveillance system will be registered with the ICO in line with data protection legislation.

8.2 The surveillance system is a closed digital system.

8.3 Signage is placed at our premises where there is CCTV surveillance.

8.4 The surveillance system has been designed for maximum effectiveness and efficiency; however, the academy cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

8.5 The surveillance system will not be trained on individuals unless an immediate response to an incident is required.

8.6 The surveillance system will not be trained on private vehicles or property outside the perimeter of the academy.

9.0 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 The authorised CCTV system operators are: principals, DSLs, DDSLs and the DPO (Trust). In some cases (depending on the type of CCTV installed), a member of estates can be appointed by the principal to be an authorised operator.

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

9.4 If, in exceptional circumstances, covert surveillance is planned, or has taken place, copies of the Home Office's authorisation forms will be completed and retained.

9.5 Any unnecessary footage captured will be securely deleted from the academy system.

10.0 Privacy by design

10.1 The use of surveillance cameras and CCTV will be critically analysed using a DPIA, in consultation with the DPO.

10.2 A DPIA will be carried out prior to the installation of any surveillance and CCTV system.

10.3 If the DPIA reveals any potential security risks or other data protection issues, the academy will ensure they have provisions in place to overcome these issues.

10.4 Where the academy identifies a high risk to an individual's interests, and it cannot be overcome, the academy will consult the ICO before they use CCTV, and the academy will act on the ICO's advice.

10.5 The academy will ensure that the installation of the surveillance and CCTV systems will always justify its means.

10.6 If the use of a surveillance and CCTV system is too privacy intrusive, the academy will seek alternative provision.

11.0 Code of practice

11.1 Our trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

11.2 The school notifies all students, staff and visitors of the purpose for collecting surveillance data via notice boards, letters and emails.

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

11.4 All surveillance footage will be kept for 30 days for security purposes; the principal and the data controller are responsible for keeping the records secure and allowing access.

11.5 Schools have 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.

11.6 The surveillance and CCTV system is owned by the school and images from the system are strictly controlled and monitored by authorised personnel only.

11.7 The surveillance and CCTV system is used to create a safer environment for staff, students and visitors to the school, and to ensure that its operation is consistent with the obligations outlined in data protection legislation.

11.8 The surveillance and CCTV system will:

- be designed to take into account its effect on individuals and their privacy and personal data
- be transparent and include a contact point, the DPO, through which people can access information and submit complaints
- have clear responsibility and accountability procedures for images and information collected, held and used
- have defined policies and procedures in place which are communicated throughout the school
- only keep images and information for as long as required
- restrict access to retained images and information with clear rules on who can gain access

- 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
- be subject to stringent security measures to safeguard against unauthorised access
- be regularly reviewed and audited to ensure that policies and standards are maintained
- 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
- be accurate and well-maintained to ensure information is up to date

12.0 Access

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

12.2 All disks containing images belong to, and remain the property of, the school.

12.3 Individuals have the right to submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing. The school will verify the identity of the person making the request before any information is supplied. 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. In order to ensure the rights of any other students, staff or visitors appearing in CCTV footage, any subject access request (SAR) would be complied with to our fullest capability and with careful and thorough redactions made. Statutory exemptions will be made as applicable.

12.4 Parents or others with parental responsibility may request to view CCTV footage that relates specifically to their child, subject to data protection considerations. Such access will only be granted where it is feasible to protect the privacy of other individuals captured in the recording, including by blurring or otherwise obscuring the identities of other data subjects. Requests must be made in writing, and our trust will assess each request on a case-by-case basis to ensure compliance with data protection legislation. Copies of footage will not normally be provided; instead, parents will be invited to view the relevant footage on trust premises under supervision.

12.5 CCTV footage may be used as evidence in disciplinary investigations and hearings where it is necessary to address alleged misconduct or breaches of trust policies and procedures. Such use of footage will be reactive, meaning it will only be accessed and reviewed in response to specific incidents or allegations brought to the attention of our trust, and not proactively monitored for the purpose of staff performance management. Access to footage for these purposes will be strictly controlled and limited to the Head of HR Centre of Excellence.

12.6 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:

- the police – where the images recorded would assist in a specific criminal inquiry
- prosecution agencies – such as the Crown Prosecution Service (CPS)

12.7 Requests for access or disclosure will be recorded and the principal (in conjunction with the DPO, if appropriate) will make the final decision as to whether recorded images may be released to persons other than the police.

12.8 Footage to support an insurance claim will not be released to insurers or via third parties because our trust does not have a lawful basis for doing so.

13.0 Monitoring and review

13.1 This policy will be monitored and reviewed on an annual basis by the DPO and who will communicate changes to this policy to all members of staff.

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