CCTV Policy

Date Published	**June 2016**
Version	**3**
Last Approved Date	**February 2024**
Review Cycle	**Triennial**
Review Date	**March 2027**

"Learning together, to be the best we can be"

1. Policy statement

1.1 This policy aims to set out the Trust's approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems on Trust property.

1.2 The purpose of the CCTV system is to:

- 1.2.1 Make members of the school community feel safe
- 1.2.2 Protect members of the school community from harm to themselves or to their property
- 1.2.3 Deter criminality in the schools
- 1.2.4 Protect Trust assets and buildings
- 1.2.5 Assist police to deter and detect crime
- 1.2.6 Determine the cause of accidents
- 1.2.7 Assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings
- 1.2.8 To assist in the defense of any litigation proceedings

1.3 The CCTV system will not be used to:

- 1.3.1 Encroach on an individual's right to privacy
- 1.3.2 Monitor people in spaces where they have a heightened expectation of privacy (including toilets and changing rooms)
- 1.3.3 Follow particular individuals, unless there is an ongoing emergency incident occurring
- 1.3.4 Pursue any other purposes than the ones stated above

1.4 The list of uses of CCTV is not exhaustive and other purposes may be or become relevant.

1.5 The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018. The system complies with the requirements of the Data Protection Act 2018 and UK GDPR.

1.6 Footage or any information gleaned through the CCTV system will never be used for commercial purposes.

1.7 In the unlikely event that the police request that CCTV footage be released to the media, the request will only be complied with when written authority has been provided by the police, and only to assist in the investigation of a specific crime.

1.8 The footage generated by the system should be of good enough quality to be of use to the police or the court in identifying suspects.

2. Relevant legislation and guidance

2.1 This policy is based on:

- UK General Data Protection Regulation
- Data Protection Act 2018
- Human Rights Act 1998
- European Convention on Human Rights
- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- 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
- Surveillance Camera Code of Practice (2021)

3. Definitions

3.1 CCTV: closed circuit television; video cameras used for surveillance.

3.2 Covert surveillance: operation of cameras in a place where people have not been made aware they are under surveillance.

3.3 Covert surveillance will only be used in extreme circumstances, such as where there is suspicion of a criminal offence. If the situation arises where covert surveillance is needed (such as following police advice for the prevention or detection of crime or where there is a risk to public safety), a data protection impact assessment will be completed in order to comply with data protection law.

3.4 Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system (stated in section 1.1).

3.5 Cameras are located in some but not all Nexus buildings.

3.6 Wherever cameras are installed appropriate signage is in place to warn members of the school community that they are under surveillance. The signage:

3.6.1 Identifies the Trust/school as the operator of the CCTV system;
3.6.2 Identifies the school as the data controller;
3.6.3 Provides contact details for the school/Trust.

3.7 Cameras are not and will not be aimed off school grounds into public spaces or people's private property.

3.8 Cameras are positioned in order to maximise coverage, but there is no guarantee that all incidents will be captured on camera.

4. Roles & Responsibilities

4.1 The **Trust Board** has the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation is complied with.

4.2 The **Headteacher** must:

- Take responsibility for all day-to-day leadership and management of the CCTV system
- Liaise with the data protection officer (DPO) to ensure that the use of the CCTV system is in accordance with the stated aims and that its use is needed and justified
- Ensure that the guidance set out in this policy is followed by all staff
- Review the CCTV policy to check that the school is compliant with the policy
- Ensure all persons with authorisation to access the CCTV system and footage have received proper training in the use of the system and in data protection
- Sign off on any expansion or upgrading to the CCTV system, after having taken advice from the DPO or delegate and taken into account the result of a data protection impact assessment
- Decide, in consultation with the DPO, whether to comply with disclosure of footage requests from third parties

4.3 The **Data Protection Officer** (DPO) must:

- Ensure training of persons with authorisation to access the CCTV system and footage in the use of the system and in data protection
- Ensure training of all staff to recognise a subject access request
- Deal with subject access requests in line with the Freedom of Information Act (2000)
- Monitor compliance with UK data protection law
- Advise on and assist the school with carrying out data protection impact assessments
- Act as a point of contact for communications from the Information Commissioner's Office

- Conduct data protection impact assessments
- Ensure data is handled in accordance with data protection legislation
- Ensure footage is obtained in a legal, fair and transparent manner
- Ensure footage is destroyed when it falls out of the retention period
- Keep accurate records of all data processing activities and make the records public on request
- Inform subjects of how footage of them will be used by the school, what their rights are, and how the school will endeavour to protect their personal information
- Ensure that the CCTV systems are working properly and that the footage they produce is of high quality so that individuals pictured in the footage can be identified
- Ensure that the CCTV system is not infringing on any individual's reasonable right to privacy in public spaces
- Ensure termly checks are carried out to determine whether footage is being stored accurately, and being deleted after the retention period
- Receive and consider requests for third-party access to CCTV footage
- Review the CCTV policy to check that the Trust is compliant with the legislation

4.4 The system manager, who is the Head of Digital Technology, must:

- Take care of the day-to-day maintenance and operation of the CCTV system
- Oversee the security of the CCTV system and footage
- Check the system for faults and security flaws termly
- Ensure the data and time stamps are accurate termly

5. Operation of the CCTV system

5.1 The CCTV system will be operational 24 hours a day, 365 days a year.

5.2 The system is registered with the Information Commissioner's Office.

5.3 The system will not record audio.

5.4 Recordings will have date and time stamps. This will be checked by the system manager termly and when the clocks change.

6. Storage of CCTV footage

6.1 Footage will be retained for around 30 days depending on the technology in use within the schools. At the end of the retention period, the files will be overwritten automatically.

6.2 On occasion footage may be retained for longer than 30 days, for example where a law enforcement body is investigating a crime, to give them the opportunity to view the images as part of an active investigation.

6.3 Recordings will be downloaded and encrypted, so that the data will be secure and its integrity maintained, so that it can be used as evidence if required.

6.4 The DPO will carry out termly checks to determine whether footage is being stored accurately, and being deleted after the retention period.

7. Access to CCTV footage

7.1 Access will only be given to authorised persons, for the purpose of pursuing the aims stated in section 1.1, or if there is a lawful reason to access the footage.

7.2 Any individuals that access the footage must record their name, the date and time, and the reason for access in the access log.

7.3 Any visual display monitors will be positioned so only authorised personnel will be able to see the footage.

7.4 The following members of staff have authorisation to access the CCTV footage:

- Trust executive leaders;
- The Headteacher
- Office\Business Manager
- Anyone with express permission of the headteacher

7.5 CCTV footage will only be accessed from authorised personnel's work devices, or from the visual display monitors.

7.6 All members of staff who have access will undergo training to ensure proper handling of the system and footage.

7.7 Any member of staff who misuses the surveillance system may be committing a criminal offence, and will face disciplinary action.

7.8 CCTV footage will only be shared with a third party to further the aims of the CCTV system set out in section 1.1 (e.g. assisting the police in investigating a crime).

7.9 Footage will only ever be shared with authorised personnel such as law enforcement agencies or other service providers who reasonably need access to the footage (e.g. investigators).

7.10 All requests for access should be set out in writing and sent to the Headteacher/CEO and the DPO.

7.11 The Trust will comply with any court orders that grant access to the CCTV footage. The Trust will provide the courts with the footage they need without giving them unrestricted access. The DPO will consider very carefully how much footage to disclose, and seek legal advice if necessary.

7.12 The DPO will ensure that any disclosures that are made are done in compliance with UK GDPR.

7.13 All disclosures will be recorded by the DPO.

8. Data protection impact assessment (DPIA)

8.1 The Trust follows the principle of privacy by design. Privacy is taken into account during every stage of the deployment of the CCTV system, including its replacement, development and upgrading.

8.2 When the CCTV system is replaced, developed or upgraded a DPIA will be carried out to be sure the aim of the system is still justifiable, necessary and proportionate.

8.3 The DPO will provide guidance on how to carry out the DPIA. The DPIA will be carried out by the Trust.

8.4 Those whose privacy is most likely to be affected, including the school community and neighbouring residents, will be consulted during the DPIA, and any appropriate safeguards will be put in place.

8.5 A new DPIA will be done annually and/or whenever cameras are moved, and/or new cameras are installed.

8.6 If any security risks are identified in the course of the DPIA, the Trust will address them as soon as possible.

9. Security

9.1 The system manager will be responsible for overseeing the security of the CCTV system and footage

9.2 The system will be checked for faults once a term

9.3 Any faults in the system will be reported as soon as they are detected and repaired as soon as possible, according to the proper procedure

9.4 Footage will be stored securely and encrypted wherever possible

9.5 The CCTV footage will be password protected and any camera operation equipment will be securely locked away when not in use

9.6 Proper cyber security measures will be put in place to protect the footage from cyber attacks

9.7 Any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied, will be applied as soon as possible