CONSILIUM ACADEMIES

Closed Circuit Television (CCTV) Policy

2023

PARTNERSHIPS | OPPORTUNITY | INTEGRITY | EQUITY | EXCELLENCE | PEOPLE-CENTRED

Date of Approval:	March 2023
Approved by:	N. Millington (Director of Estates and Operations)
Date of next Review:	March 2025

Consilium Academies

Contents

1. Purpose

This policy aims to set out the trust approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems on trust premises.

This policy overarches school specific CCTV procedures which identify the detail of each school arrangement.

2. Statement of Intent

CCTV has been installed in all Consilium premises with the specific purpose of:

- Make members of the school community feel safe and reduce fear of crime,
- Protect members of the school community from harm, to themselves or their property,
- Deter criminality in the school,
- Protect school assets and buildings,
- Assist police to deter and detect crime,
- Determine the cause of accidents, incidents and near misses,
- Assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings,
- To assist in the defense of any litigation proceedings,

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

CCTV will not be used to:

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

3. Statement of Control

CCTV systems are registered with the Information Commissioner under the terms of the Data Protection Act 2018. Systems are compliant with the requirements of the Data Protection Act 2018 and UK GDPR.

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

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.

4. Roles and Responsibilities

The Board of Trustees

The Board of Trustees 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.

The Headteacher

The Headteacher will:

- Take responsibility for all day-to-day leadership and management of the local 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 legislation
- Ensure all persons with authorisation to access the CCTV system and footage have received proper training from the DPO 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 and taken into account the result of a data protection impact assessment (DPIA)
- Decide, in consultation with the DPO, whether to comply with disclosure of footage requests from third parties

The Data Protection Officer (DPO)

The Data Protection Officer (DPO) will:

- Train persons with authorisation to access the CCTV system and footage in the use of the system and in data protection
- Train all staff to recognise a subject access request
- Deal with subject access requests (SARs) 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 (DPIAs)
- Act as a point of contact for communications from the Information Commissioner's Office
- Conduct data protection impact assessments (DPIAs)
- 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 occupants 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
- Carry out termly checks 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

The Head of Operations

The Head of Operations will:

- Monitor all school to ensure compliance with this policy, reporting to the DPO and Board of Trustees.
- Be responsible for the management, review and maintenance of this policy and subsequent procedures.

The System Manager

The System Manager will:

- 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 each term, or when issues are reported
- Ensure the data and time stamps are accurate each term, or when issues are reported

5. Relevant Legislation and Guidance

Legislation

- 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

Guidance

- Surveillance Camera Code of Practice (2021)

6. Definitions

Title	Definition
Bring your own Device (BYOD)	Also called bring your own technology, bring your own phone and bring your own personal computer. This could also include Dashcams.
Closed Circuit Television (CCTV)	A self-contained surveillance system, comprising cameras, recorders and displays for monitoring activities on trust premises.
Collateral Intrusion	Capturing of images of individuals not covered by the stated purpose of the system. Background images.
Covert Surveillance	Recording of images or individuals without their knowledge or consent.
Data Protection Act	UK Act of Parliament designed to protect personal data stored on computers or an organised paper filing system.
Data Protection Impact Assessment (DPIA)	A process that helps organisations identify and minimise risks that result from data processing. DPIAs are usually undertaken when introducing new data processing processes, systems or technologies.
Data Protection Officer (DPO)	Legally mandated position within the trust responsible for ensuring that the trust is compliant with all UK data protection legislation.
Freedom of Information Act 2000 (FOI)	Provides the public access to information held by public authorities. The Act covers any recorded information that is held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland.

Information Commissioners Office (ICO)	The independent regulatory office in charge of upholding information rights in the interest of the public. The organisation covers the Data Protection Act, the Freedom of Information Act and the Environmental Information Regulations.
Regulation of Investigatory Powers Act (RIPA)	UK Act of Parliament, regulating the powers of public bodies to carry out surveillance and investigation. And covering the interception of communications.
Subject Access Request (SAR)	A statutory right that students/parents/staff have under the Data Protection Act 2018 to obtain from the Trust a copy of the information that is held about them.

7. Covert Surveillance

All CCTV use will be overt unless a specified operation for a specific purpose is being undertaken in circumstances necessary for the prevention and detection of crime.

If the situation arises where covert surveillance is needed, a request from the Police under the Regulation of Investigatory Powers Act (RIPA) 2000 will be required. The RIPA request must be approved by the DPO to ensure there are grounds for suspecting criminal activity or equivalent malpractice and that notifying the individuals about the monitoring would prejudice its prevention or detection.

8. Dashcams

Under the DPA 2018, the image of a person recorded by a Dashcam will constitute personal data, since it allows for the identification of an individual, in the same way as CCTV and other Trust Surveillance systems.

A DPIA should be completed for any Dashcams used in Trust vehicles to ensure the purpose of their usage is clearly defined.

Dashcam recordings should be saved as securely as any other instance of personal data, and should not be used for social media purposes.

Sharing of Dashcam footage without proper authorisation constitutes a reportable data protection security breach, and should be treated as such.

9. BYOD (Bring your own device)

BYOD refers to the policy of permitting staff to bring personally owned devices to the workplace, and to use those devices to access Trust information and applications.

Under no circumstances should staff use their own equipment to record students or staff.

10. Location of Cameras

Cameras will be positioned in places that require monitoring in order to achieve the aims of the CCTV system.

A schedule of camera locations must be identified in the local CCTV procedure.

Wherever cameras are installed, appropriate signage must be in place to warn members of the school community that they are under surveillance. The signage should:

- Identify the school as the operator of the CCTV system
- Identify the school as the data controller
- Provide contact details for the school

Cameras must not and will not be aimed off school grounds into public spaces or people's private property. This includes perimeter and gate control systems.

Cameras should be positioned in order to maximise coverage, but there is no guarantee that all incidents will be captured on camera. Camera positioning should be periodically reviewed to ensure maximum effectiveness.

11. Operation of the CCTV System

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

The system must be registered with the Information Commissioner's Office.

The system should not record audio.

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

12. Retention of CCTV footage

Footage should be retained for up to 30 days. At the end of the retention period, the files will be overwritten automatically.

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. In this instance, footage may be retained indefinitely.

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.

The DPO will ensure termly checks are carried out to determine whether footage is being stored accurately and being deleted after the retention period.

13. Access to CCTV footage

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

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

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

Staff access

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

- The Headteacher
- The Deputy Headteacher
- The Data Protection Officer
- The System Manager
- Anyone with express written permission of the Headteacher

A schedule of persons in the above roles must be identified in the school CCTV Procedure.

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

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

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

Subject access requests (SAR)

According to UK GDPR and DPA 2018, individuals have the right to request a copy of any CCTV footage of themselves.

Upon receiving the request the school will immediately issue a receipt and will then respond within 30 days during term time. The school reserves the right to extend that deadline during holidays due to difficulties accessing appropriate staff members.

All staff must have received training to recognise SARs. When a SAR is received, staff should inform the DPO in writing. When making a request, individuals should provide the school with reasonable information such as the date, time and location the footage was taken to aid school staff in locating the footage.

On occasion the school will reserve the right to refuse a SAR, if, for example, the release of the footage to the subject would prejudice an ongoing investigation.

Images that may identify other individuals need to be obscured to prevent unwarranted identification. The school will attempt to conceal their identities by blurring out their faces, or redacting parts of the footage. If this is not possible the school will seek their consent before releasing the footage. If consent is not forthcoming images may be released. There might be circumstances where it is not possible to physically share copies of CCTV footage to comply with GDPR laws and, in this case, individuals might be invited to view footage.

The school reserves the right to charge a reasonable fee to cover the administrative costs of complying with an SAR that is repetitive, unfounded, or excessive.

Footage that is disclosed in a SAR will be disclosed securely to ensure only the intended recipient has access to it.

Schools must identify how they will share files in the school CCTV Procedure.

Records must be kept that show the date of the disclosure, details of who was provided with the information (the name of the person and the organisation they represent), and why they required it.

Individuals wishing to make an SAR can find more information about their rights, the process of making a request, and what to do if they are dissatisfied with the response to the request on the ICO website.

Third-party access

CCTV footage will only be shared with a third party to further the aims set out in this Policy (e.g. assisting the police in investigating a crime).

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).

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

The Trust will comply with any court orders that grant access to the CCTV footage. The school 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.

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

All disclosures must be recorded by the DPO.

14. Data protection impact assessment (DPIA)

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 the replacement, development and upgrading.

The system is used only for the purpose of fulfilling the aims of this Policy.

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.

The DPO will provide guidance on how to carry out the DPIA. The DPIA will be carried out by a competent person nominated by the Headteacher or DPO.

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.

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

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

15. Infrastructure Changes

Any new CCTV system or major change to an existing system must have a DPIA carried out to establish the specified purpose which meets the aims of this Policy.

Factors that will influence the installation of CCTV include:

- Remote or isolated locations,
- Locations where crime is a particular issue,
- Where high value assets are maintained, for example plan rooms or storage facilities,
- Locations of lone or late workers
- Entrances where admittance is restricted to authorized persons only

In collaboration with the Central Estates department, a formal specification for the functionality of the new system will be developed. Every effort should be taken to ensure that new systems utilize technology to enable restricted access and data security as well as remote viewing by authorized personnel.

16. Security

The System Manager will be responsible for overseeing the security of the CCTV system and footage.

The system will be checked for faults once a term or when issues are reported.

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.

Footage must be stored securely, and encrypted wherever possible.

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

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

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

Deviations to this arrangement (relative to system capabilities) must be identified in the school CCTV Procedure.

17. Complaints

Complaints should be directed to the Headteacher or the DPO and should be made according to the school's complaints policy.

18. Monitoring Compliance

This policy will be reviewed Bi-Annually by the Head of Operations.

School CCTV Procedures must be reviewed annually by the DPO/Headteacher to consider whether the continued use of a surveillance camera remains necessary, proportionate and effective in meeting the aims of this Policy.

19. Links to other policies

- Data protection policy
- Biometric data policy
- Privacy notices for parents, pupils, staff, governors and suppliers
- Safeguarding policy

Links to local school policies should be identified in the School CCTV Procedure.

20. Non-Compliance

This Policy concerns the safe and compliant use of CCTV and Surveillance systems in trust premises and assets. Non-Compliance with this policy may leave the trust subject to legal action and/or criminal prosecution. Staff found to be acting in breach of this policy may be subject to disciplinary proceedings.