ST. MARK'S CE SCHOOL

ONE SCHOOL - SERVING ALL - THROUGH EXCELLENCE

CCTV Policy

Policy Statement and Guidelines

Date: Spring 2024

Review: Spring 2025

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

1.1 Statement of intent

The purpose of the CCTV system is to:

- Make members of the school community feel safe
- Protect members of the school community from harm to themselves or to their property
- Deter criminality in the school
- Protect school assets and buildings
- Assist in managing the school
- Assist police to deter and detect crime including identifying, apprehending and prosecuting offenders
- Determine the cause of accidents
- 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 CCTV system 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 (i.e changing rooms and toilet cubicles themselves)
- Follow particular individuals, unless there is an ongoing emergency incident occurring
- Pursue any other purposes than the ones stated above

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

The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018. The system and all associated images/recordings comply with the requirements of the Data Protection Act 2018 and UK GDPR. The policy acknowledges that processing the CCTV data includes potentially official sensitive and will take appropriate steps to manage this information as described in this procedure and associated documents
The CCTV system does not have sound recording capability and only a limited number of cameras a movable, however they remain focused on a specific section of the school to provide coverage of the site, the remaining are fixed.

The CCTV system is part of the electronic infrastructure of the building developed by Morgan Sindall and JP Hopkins, but is operated by the school (as Data Controller) and therefore deployment of which is determined by the school.

Footage or any information gleaned through the CCTV 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.

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

St. Mark's CE School has chosen to use CCTV (Closed circuit television) in various areas across the school including external entrances and identified areas within the building. The Data Protection Legislation including GDPR, and Regulation of Investigatory Powers Act 2000 (RIPA) and CCTV Code of Practice issued by the Information Commissioner explains how CCTV systems should be used, so that schools and individuals can enjoy security and safety whilst ensuring that individual rights are upheld. St. Mark's CE School complies with the Code and adopts good standards of practice which helps towards realising this objective.

CCTV may also be mentioned within and through other legal frameworks.

The school has undertaken the following checklist, which will be reviewed bi-annually to ensure that the CCTV system remains within the law and that images can be used for crime prevention. • The school has specified that the CCTV cameras have been installed for the safeguarding of staff and students and for detection and prevention of vandalism across the school estate.

- Signage is found in prominent positions in all areas where CCTV cameras operate to inform staff, students and the general public that they are entering an area where their images are being recorded either as still or video footage.
- The school retains the right to be the data controller for all footage recorded through the use of its CCTV cameras.
- The equipment is sited so that it only monitors those spaces that are intended to be covered by the equipment.
- All operators (staff who operate and monitor CCTV) are aware of the purposes for which the scheme has been established.

Any breach of the Code of Practice by the school will be initially investigated by the Executive Headteacher or nominee, in order for them to take the appropriate disciplinary action.

The following Dos and Don'ts are as advised as part of the Data Protection Legislation and must be adhered to by all named staff.

Do

- Assess the appropriateness of and reasons for, using CCTV.
- Ensure that all relevant information is obtained prior to CCTV investigation so that the most relevant sections of CCTV are scrutinised.
- Undertake regular reviews of both the use of the CCTV system and the procedures to ensure compliance with the law.
- Be aware that video / images are not kept for longer than 34 days but may be stored in a more secure location during the period of an investigation.
- Process (working with, using, passing on data) images in a lawful manner and only to relevant parties.

Don't

- Film areas that could amount to an infringement of personal privacy.
- Use CCTV footage for any other purpose other than what it was originally used for e.g. Prevention and detection of a crime.
- Use covertly (i.e. where it is calculated to ensure that the persons are unaware) monitoring without seeking advice and contrary to section 4.
- Use inadequate equipment. Blurred or indistinct images could constitute as inadequate data, whilst poorly maintained equipment may not provide legally sound evidence.
- Disclose data to third parties, unless it is lawful to do so.
- Systematically monitor people by use of CCTV

This policy is based on:

2.1 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
- Regulation of Investigatory Powers Act (RIPA) 2000

2.2 Guidance

- Surveillance Camera Code of Practice (2021)
- CCTV Code of Practice Revised Edition 2008 (published by the Information Commissioners Office)
- www.ico.gov.uk

3. Definitions

Surveillance: the act of watching a person or a place

CCTV: closed circuit television; video cameras used for surveillance

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

4. Covert surveillance

Covert surveillance will only be used in extreme circumstances, such as where there is suspicion of a criminal offense. 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.
Additionally, the proper authorisation forms from the Home Office will be completed and retained where necessary.

5. Location of the cameras

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

Cameras are located in various locations around the school site to give coverage:

- A list of camera locations is held by the school, which is available to staff authorised to have access to the CCTV system, but not listed in this policy for security purposes.

Wherever cameras are installed appropriate signage is in place at each access point to the school site to warn members of the school community that they are under surveillance. The signage:

- Identifies the school as the operator of the CCTV system
- Identifies the school as the data controller
- Provides contact details for the school

Care has been taken to ensure as practically as possible that cameras are not and will not be aimed off

school grounds into public spaces or people's private property. Where this has inevitably occurred due to the building location and structure black out blocks have been placed onto camera setups.

CCTV is not used in standard classrooms.

Cameras are positioned in order to maximise coverage, but there is no guarantee that all incidents will be captured on camera. As such a yearly review (or ad-hoc review if deemed necessary) of any area/locations considered to be blind spots and whether remedial action needs to be taken (i.e. the sitting of new cameras or the movement of existing ones).

Where possible CCTV cameras have been positioned to observe fire alarm activation points to prevent malicious activations.

6. Roles and responsibilities

6.1 The governing board

The governing board has the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation (defined in section 2.1) is complied with.

6.2 The Executive Headteacher

The Executive Headteacher will:

- 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 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
- Decide, in consultation with the DPO, whether to comply with disclosure of footage requests from third parties

6.3 The data protection officer

The data protection officer (DPO) or other delegated staff member 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 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
- Carry out yearly 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

6.4 The Systems 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 termly
- Ensure the data and time stamps are accurate termly

7. Operation of the CCTV system

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

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

The system will not record audio.

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

8. Storage of CCTV footage

Footage will be retained securely for 34 days with the integrity of the recordings maintained. At the end of the retention period, the data will be overwritten automatically.

On occasion footage may be retained for longer than 34 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 or for litigation purposes.

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. Files will be named appropriately

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

9. Access to CCTV footage

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. In doing so they are deemed to be acting on behalf of the Executive Headteacher.

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.

All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All operators are trained by the school data controller in their responsibilities under the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images.

9.1 Staff access

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

- The Executive Headteacher: Stephanie Bryant
- The Head of School Primary: Lorraine Hoad
- The Director of Operations: Helen Crowhurst
- The Director of Pastoral and Inclusion: Amir Fakhoury
- The Site Manager: Chris Durham
- The Systems Manager: Chris Lovett
- The IT Technician: Cheuk Leung
- The Assistant Head (Primary): Steve Causley
- The Assistant Head (Secondary): Sam Genovese
- Anyone with express permission of the Executive Headteacher

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 offense, and will face disciplinary action.

9.2 Subject access requests (SAR)

According to UK GDPR and Data Protection Act 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 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 the still images may be released instead.

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.
Images or video footage will be downloaded and saved on to an encrypted USB key, which will then be give to the person making the request with necessary passwords sent separately.

Records will 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 – if appropriate), 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.

9.3 Third-party access

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) or where there is a legal duty/requirement to do so.

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 Executive Headteacher and the DPO.

The school 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 will be recorded by the DPO.

10. Data protection impact assessment (DPIA)

The school 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.

The system is used only for the purpose of fulfilling its aims (stated in section 1.1).

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 the DPO or the Data Protection Compliance Lead.

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 or whenever cameras are moved, 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.

11. Security

- The Systems Manager will be responsible for overseeing the security of the CCTV system and footage in conjunction with the site and IT Technician
- The system will be checked for faults once a term or as alerts are displayed
- 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 will 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

12. Complaints

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

13. Monitoring

The policy will be reviewed bi-annually by the DPO to consider whether the continued use of a surveillance camera remains necessary, proportionate and effective in meeting its stated purposes.

14. Links to other policies

- Data Protection Policy and Procedures
- Privacy notices for parents, pupils, staff and governors

Safeguarding policy