Growing as we learn. Learning as we grow.

Rooted in Jesus.

ST MARGARET'S COLLIER STREET CE SCHOOL

CCTV POLICY

Review:	September 2024
Agreed by Governors:	September 2024
Next Review:	September 2026

CCTV Policy

1 Policy Statement

This policy outlines the school's approach to operating, managing, and using surveillance and closed-circuit television (CCTV) systems on school property. The school only has CCTV externally.

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 their property
- Deter criminality on the school site
- Protect school assets and buildings
- Assist police to deter and detect crime
- 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 defence of any litigation proceedings

The CCTV system will not be used to:

- Encroach on an individual's right to privacy
- 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 or may not be relevant.

The CCTV system is registered with the Information Commissioner under the terms of the DPA. The system complies with the DPA requirements and GDPR.

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 investigating 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 Definitions

Term	Definition
School	St. Margaret's Collier Street CE Primary
Department of Education (DfE)	is the government department which deals with education
Local Authority	Kent
Headteacher	Mr T Wyatt-Hughes

Term	Definition
Chair of Governors (CoG)	Mr S Randell
Senior Teacher	Mrs A Drury
Designated Safeguarding Leads (DSL)	Mr T Wyatt-Hughes
Parents	Are either the parents, carers, or guardians
Schools Data Protection Officer (DPO)	Satswana Ltd, Suite G12 Ferneberga House, Alexandra Road, Farnborough, GU14 6DQ. info@satswana.com
Website Service	Zulogic
Data Protection Act (DPA)	The Data Protection Act 2018 act makes a provision about the processing of personal data and is it subject to GDPR. With amendment in 2023.
UK General Data Protection Regulation (GDPR)	which applies across the European Union (including in the United Kingdom)
Freedom of Information Act (FoI)	The Freedom of Information Act 2000 discloses information held by public authorities or persons providing services for them and amends the Data Protection Act.
Educations Act (EA)	The Education Act 1996 consolidates the Education Act 1944 and certain other educational enactments.
Information Commissioners Office (ICO)	This organisation ensures compliance with the Data Protection Act, Freedom of Information Act, and GDPR and handles formal complaints.
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
Electronic Platform	An electronic platform is any means the school communicates. This could include, but is not limited to, Email, Online Portals, and Social Media platforms.

3 Relevant legislation and guidance

This policy is based on:

3.1 Legislation

- GDPR
- DPA
- Human Rights Act 1998
- European Convention on Human Rights
- The Regulation of Investigatory Powers Act 2000

- The Protection of Freedoms Act 2012
- FOI
- EA
- 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

3.2 Guidance

- Surveillance Camera Code of Practice (2021).

4 Covert surveillance

Covert surveillance will only be used in extreme circumstances, such as suspicion of a criminal offence. Suppose a 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). In that case, a data protection impact assessment will be completed 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 to achieve the CCTV system's aims (stated in section 1.1).

Cameras are located in around the outside of the main school building. There are no devices inside.

Wherever cameras are installed, appropriate signage is in place to warn school community members 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

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

Cameras are positioned to maximise coverage, but it is not guaranteed that all incidents will be captured on camera.

6 Roles and responsibilities

6.1 The governing board

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

6.2 The headteacher

The 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 CCTV system's use is within the stated aims and is needed and justified.
- Ensure that all staff follows the guidance set out in this policy.
- Review the CCTV policy to ensure the school complies with legislation.
- Ensure all persons authorised to access the CCTV system and footage have received proper training from the DPO in using the Electronic Platform and data protection.
- Sign off on any expansion or upgrading of the CCTV system after consulting the DPO and considering the result of a data protection impact assessment.
- Decide, in consultation with the DPO, whether to comply with third-party requests for disclosure of footage.
- Train persons authorised to access the CCTV system and footage using the system and data protection.
- Train all staff to recognise a subject access request.
- Conduct checks to determine whether the footage is stored accurately and deleted after the retention period.
- Ensure footage is destroyed when it falls out of the retention period

6.3 The data protection officer

The data protection officer (DPO) will:

- Deal with subject access requests in line with the FOI.
- Monitor compliance with DPA and GDP.
- Advise and assist the school with carrying out data protection impact assessments.
- Act as a point of contact for communications from the ICO.
- Ensure data is handled under data protection legislation.
- Ensure footage is obtained in a legal, fair and transparent manner.
- Keep accurate records of all data processing activities and make the documents public on request.
- Inform subjects of how the school will use footage of them, their rights, and how the school will endeavour to protect their personal information.
- Ensure that the CCTV system does not infringe on any individual’s reasonable right to privacy in public spaces.
- Receive and consider requests for third-party access to CCTV footage.

6.4 The system manager

The system manager will:

- Take care of the day-to-day maintenance and operation of the CCTV system.
- Conduct data protection impact assessments.
- Oversee the security of the CCTV system and footage.
- Ensure that the CCTV systems are working correctly and that the footage they produce is of high quality so that individuals pictured in the footage can be identified.
- 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 a date and time stamps. The system manager will check these periodically and when the clocks change.

8 Storage of CCTV footage

Footage will be retained for 28 days. The files will be overwritten automatically at the end of the retention period.

Occasionally, footage may be retained for longer than 28 days, for example, when a law enforcement body is investigating a crime, to allow them to view the images as part of an active investigation.

Recordings will be downloaded and encrypted, ensuring the data is secure and maintained in integrity. This will allow for the use of the recordings as evidence if required.

The Headteacher will conduct checks to determine whether the footage is being stored accurately and deleted after the retention period.

9 Access to CCTV footage

Access will only be given to authorised persons to pursue the aims stated in section 1.1 or if there is a lawful reason to access the footage.

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

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

9.1 Staff Access

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

- The Headteacher/ System Manager
- Anyone with express permission from the headteacher

CCTV footage will only be accessed from authorised personnel's work devices or 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.

9.2 Subject Access Requests (SAR)

According to GDPR and DPA, individuals can request a copy of any CCTV footage of themselves and only themselves.

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

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 of the footage taken to aid school staff in locating the footage.

Occasionally, the school will reserve the right to refuse a SAR if, for example, releasing the footage to the subject would prejudice an ongoing investigation or person(s).

Images that may identify other individuals must be obscured to prevent unwarranted identification. The school will provide still images to conceal their identities by blurring out their faces. If this is not possible, the school will seek their consent before releasing the footage. If consent is not forthcoming, we will refuse the release of the footage.

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

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

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), and why they required it.

Individuals wishing to make a SAR can find more information about their rights, the process of creating 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).

Footage will only 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 access requests should be set out in writing and sent to the 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 necessary footage without giving them unrestricted access. The DPO will carefully consider how much footage to disclose and seek legal advice if necessary.

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

The DPO will record all disclosures.

10 Data protection impact assessment (DPIA)

The school follows the principle of privacy by design. Privacy is considered during every stage of the deployment of the CCTV system, including its replacement, development, and upgrading.

The system is used only to fulfil its aims (stated in section 1.1).

When the CCTV system is replaced, developed, or upgraded, a DPIA will be carried out to ensure that its aim remains justifiable, necessary, and proportionate.

The DPO will provide guidance on how to conduct the DPIA, which will be conducted by the System Manager.

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 implemented.

A new DPIA will be performed whenever cameras are moved or new cameras are installed.

If at any time any security risks are identified during the DPIA, the school will address them immediately.

11 Security

- The System Manager will be responsible for overseeing the security of the CCTV system, footage and the Electronic Platform.
- The system will be checked for faults once a term.

- Any faults in the system will be reported as soon as they are detected and repaired as quickly 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 used.
- Any software updates (mainly security updates) published by the equipment manufacturer that need to be applied will be applied as soon as possible.

12 Complaints

If you have any concerns about how we handle your data, please get in touch with our DPO. If you are unsatisfied with our response, you can complain to the Information Commissioner's Office (ICO). You can contact the ICO at:

Information Commissioner's Office Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF

Tel: 0303 123 1113

Report a concern online at https://ico.org.uk/make-a-complaint/

13 Monitoring

The Headteacher and CoG will review the policy annually to determine whether the continued use of surveillance cameras remains necessary, proportionate, and effective in meeting its stated purposes.