Autumn | 26-28

St Joseph's Catholic Primary School

CCTV Policy

Date ratified by Governors:	Autumn 2026-27
Date of next review of the policy:	Autumn 2028-29
This policy is reviewed:	**2 Years**

Learn together and grow in God's love

Aspiration - Compassion - Community - Faith - Respect – Responsibility

St Joseph's Catholic Primary School
Commerell Street
East Greenwich
London SE10 9AN

Table of Contents

Section 1: Introduction 3
Section 2: Legal framework 3
Section 3: The CCTV system 3
Section 4: Purposes and lawful basis 3
Section 5: Privacy, camera siting and signs 4
Section 6: Roles and responsibilities 4
Section 7: Access to the system and security 4
Section 8: Retention and deletion 5
Section 9: Sharing footage 5
Section 10: Covert surveillance 5
Section 11: Use of CCTV in staff matters 6
Section 12: Your rights and subject access requests 6
Section 13: Complaints 6
Section 14: Data breaches 6
Section 15: Data Protection Impact Assessment and review 7
Appendix 1: CCTV access and disclosure log 8

Section 1: Introduction

St Joseph's Catholic Primary School uses a small CCTV system of five external cameras to help keep pupils, staff, parents, visitors and the school site safe. The school recognises that CCTV can intrude on privacy, so this policy sets out how the system is used fairly, lawfully and only for the purposes stated here.

This policy applies to everyone whose image may be captured by the school's cameras, including pupils, staff, parents, visitors, contractors, hirers and members of the public passing the site. It applies to all school staff, governors and contractors who operate, view or manage the system.

It should be read alongside the school's Data Protection Policy and Privacy Notices, Safeguarding and Child Protection Policy, Lockdown Policy, Lettings Policy, Staff Disciplinary Policy and Complaints Policy.

Section 2: Legal framework

The school operates its CCTV system in line with:

- the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025
- the Information Commissioner's Office (ICO) guidance on video surveillance, including CCTV
- the Human Rights Act 1998, in particular the right to respect for private and family life (Article 8)
- the Protection of Freedoms Act 2012 and the Surveillance Camera Code of Practice, which the school follows as good practice although it is not legally bound by it
- the Freedom of Information Act 2000, where requests relate to the CCTV system rather than to individuals

The Governing Body of St Joseph's Catholic Primary School is the data controller for CCTV images. The school pays the annual data protection fee and is registered with the ICO.

Section 3: The CCTV system

Item	Detail
Number of cameras	Five, all external. There are no cameras inside the school buildings
Camera locations	The front gate and the two playgrounds
What is recorded	Images only. The system does not record audio, and audio recording must not be switched on
Hours of operation	24 hours a day, every day of the year. The school does not guarantee that every camera will be working at all times
Recording equipment	A recorder kept in the premises office, which is locked when unattended
Live and remote viewing	Footage can only be viewed on the designated school computer on site. There is no remote viewing
Retention	Footage is automatically overwritten after 30 days
Maintenance contractor	ATS, under a written data processing contract

No camera uses facial recognition or any other biometric technology. Any change to the number, position or capability of cameras requires an updated Data Protection Impact Assessment (Section 15) before it goes ahead.

Section 4: Purposes and lawful basis

The CCTV system is used only to:

- protect pupils, staff, parents and visitors from harm

- support the safeguarding of pupils, including during a lockdown or other emergency
- protect the school buildings, grounds and property from crime, vandalism and trespass
- support the police in preventing and detecting crime and in identifying and prosecuting offenders
- help establish the cause of accidents and other serious incidents on site, so they can be prevented in future

The school processes CCTV images because it is necessary to carry out its official functions as a school in the public interest (UK GDPR Article 6(1)(e), "public task"), including its duties to safeguard pupils and to provide a safe environment.

Where footage relates to a suspected criminal offence, the school relies on the relevant conditions in Schedule 1 of the Data Protection Act 2018 and its Appropriate Policy Document. CCTV is not used to process special category data (for example, information about health or ethnicity), although such information may sometimes be visible in images.

CCTV images will never be used for commercial purposes, for entertainment, or for any purpose not listed in this section.

Section 5: Privacy, camera siting and signs

Cameras are positioned only where they are needed for the purposes in Section 4, and have been sited to avoid, as far as possible, views into neighbouring homes, gardens and other private property. Where a camera's view includes private property, privacy masking is used.

Cameras will never be placed in or pointed into toilets, changing areas or any other place where people would reasonably expect privacy.

Clear signs are displayed at each entrance and near each camera. They state that CCTV is in operation, that St Joseph's Catholic Primary School is responsible for it, the purpose (safety and security), and how to contact the school office for more information.

The school's privacy notices for pupils, parents, staff and visitors explain the use of CCTV. This policy is available on the school website and from the school office.

Section 6: Roles and responsibilities

Role	Responsibilities
Governing Body	Approves this policy and makes sure the school complies with data protection law
Headteacher (Suzanne Long)	Has overall responsibility for the CCTV system; authorises access to footage and any disclosure; decides on any covert surveillance (Section 10)
System Manager: Site Manager (Kavin Ferreira)	Day-to-day management of the system; checks cameras and recording work properly; keeps the access and disclosure log; manages the maintenance contractor; in his absence, a member of the Senior Leadership Team takes this role
Data Protection Officer: Judicium Consulting Limited (dataservices@judicium.com)	Advises on compliance; reviews the DPIA; advises on requests for footage, complaints and data breaches
Senior Leadership Team	May view footage when authorised by the Headteacher for a purpose in Section 4
All staff	Report any concerns about the CCTV system or its misuse to the Headteacher or the DPO

Section 7: Access to the system and security

Access to live and recorded footage is limited to the System Manager, the Headteacher and members of the

Senior Leadership Team authorised by the Headteacher. Each authorised user has their own password, and passwords are not shared.

Footage is viewed only for a purpose in Section 4, in a private area where it cannot be seen by others. Every viewing is recorded in the CCTV access and disclosure log (Appendix 1), showing the date, who viewed it, what was viewed and why.

The recording equipment is kept in a locked, secure location. The system's software and firmware are kept up to date, default passwords are changed, and any wireless connections between cameras and the recorder are encrypted.

Footage can only be viewed on the designated school computer on site. Remote viewing, including on phones, tablets or home computers, is not permitted. Footage must not be viewed on, copied to or recorded with personal devices, including by filming a screen on a mobile phone.

The maintenance contractor acts as a data processor. It works under a written contract that meets UK GDPR Article 28, accesses the system only when needed for maintenance, and is supervised by the System Manager.

Section 8: Retention and deletion

Recorded footage is kept for 30 days and then automatically overwritten. This gives enough time for most incidents to come to light and be investigated.

Footage needed for a specific purpose, such as a police investigation, a safeguarding concern, an insurance claim or legal proceedings, is copied and kept securely only for as long as that purpose requires. Copies are reviewed at least every six months and securely deleted when no longer needed. Each copy and its deletion are recorded in the log.

Section 9: Sharing footage

Police and other authorities. The police and other law enforcement bodies may request footage to prevent or detect crime. Requests must be made in writing on the force's data request form, or in an email from an official address, explaining why the footage is needed. The Headteacher, advised by the DPO where needed, decides whether to disclose under the crime and taxation exemption in Schedule 2 of the Data Protection Act 2018. In an emergency where there is a risk to life, footage may be shared immediately and the paperwork completed afterwards.

How footage is shared. Footage is exported only by the System Manager, onto an encrypted device or by a secure digital transfer method. Each export is given a reference number and recorded in the log, including what was shared, with whom and on whose authority. Once footage has been disclosed to the police, they become responsible for it under data protection law.

Other requests. Requests from others, such as insurers, solicitors or parents, are referred to the DPO. Footage is shared only where the law allows it, and images of other people are blurred or removed where necessary.

Social services and safeguarding. Footage may be shared with children's social care or other safeguarding partners where this is necessary to protect a child, in line with the school's Safeguarding and Child Protection Policy.

The media. Footage is never given to the media, except at the written request of the police to help identify a suspect in a specific crime.

Witnesses. Where a member of staff may later be a witness to an offence, they should avoid viewing the footage until the police advise them to do so.

Section 10: Covert surveillance

The school will not normally use hidden cameras. In exceptional circumstances, such as a serious crime that cannot be investigated in any other way, covert recording may be considered. It must be:

- authorised in writing by the Headteacher, after advice from the DPO, with the Chair of Governors

informed

- supported by a written assessment of why it is necessary and proportionate
- limited to a specific location and a fixed, short period
- never used in toilets, changing areas or any other private space

Where the police wish to carry out covert surveillance on school property, they are responsible for obtaining the necessary authorisation under the Regulation of Investigatory Powers Act 2000.

Section 11: Use of CCTV in staff matters

CCTV is not used to monitor staff performance or for routine supervision of staff. Footage may be used in a staff investigation or disciplinary matter only where it shows a possible safeguarding concern, a criminal offence or serious misconduct that comes to light during a purpose listed in Section 4. In those cases the member of staff will be told that CCTV footage is being considered and will be given the chance to see and respond to it.

Section 12: Your rights and subject access requests

Anyone whose image is recorded can ask to see the footage of themselves. Requests can be made to the school office or the DPO, in writing or verbally, and should include the date, approximate time and location so the footage can be found before it is overwritten.

- The school will check the identity of the person making the request. Parents may make requests on behalf of their child where the child is not mature enough to make the request themselves.
- The school will respond within one calendar month. This can be extended by up to two further months for complex requests. If the school needs to confirm the requester's identity or clarify the request, the time limit pauses until that information is received.
- The school will carry out a reasonable and proportionate search for the footage.
- There is normally no charge.
- Images of other people will be blurred or removed where necessary to protect their privacy. If this is not possible, the school may provide still images or a written description instead.
- If footage has already been overwritten, the school will explain this.

People also have the right to object to CCTV processing, and to ask for footage to be deleted or its use restricted. The school will consider each request in line with data protection law.

Section 13: Complaints

Anyone can complain to the school about how its CCTV system is used or about how their personal data has been handled.

1. Complaints should be sent to the Headteacher or the DPO, by email to support@stjosephs.greenwich.sch.uk, by letter, or by using the data protection complaints form on the school website.
2. The school will acknowledge the complaint within 30 days.
3. The school will look into the complaint without undue delay and tell the complainant the outcome.

If someone is not satisfied with the outcome, they can complain to the Information Commissioner's Office at ico.org.uk or on 0303 123 1113. Complaints about other aspects of CCTV, not involving personal data, follow the school's Complaints Policy.

Section 14: Data breaches

Any loss, theft, unauthorised access to or misuse of CCTV footage must be reported straight away to the Headteacher and the DPO. The school will follow its data breach procedure and, where the breach is likely to put people's rights at risk, report it to the ICO within 72 hours. Misuse of the CCTV system by staff may

be dealt with under the Staff Disciplinary Policy.

Section 15: Data Protection Impact Assessment and review

The school has completed a Data Protection Impact Assessment (DPIA) for its CCTV system, which considers whether CCTV is necessary, whether less intrusive options would work, and how privacy risks are reduced. The DPIA is reviewed with the DPO whenever cameras are added, moved or upgraded, and at each review of this policy.

The System Manager checks regularly that the cameras are working, that the date and time are correct, and that images are clear enough for their purpose.

The Governing Body reviews this policy every two years, or sooner if the law, guidance or the CCTV system changes.

Appendix 1: CCTV access and disclosure log

Kept by the System Manager. One entry for every viewing, copy, disclosure and deletion of footage.

Date and time	Name and role	Viewed, copied, disclosed or deleted	Camera, date and time of footage	Reason	Authorised by	Reference no.