CCTV and Surveillance Policy

St Barnabas CofE Primary School

Approved by:	St Barnabas LGB
Last reviewed on:	March 2026
Next review due by:	March 2029

This policy supersedes all previous CCTV and Surveillance policies

Fioretti Trust

Aspiration Wisdom Compassion

Contents:

Statement of intent

At St Barnabas C of E Primary School, we take our responsibility for the safety of pupils, staff and visitors seriously.

We use CCTV to deter and detect crime, to protect people and property, and to support our wider safeguarding arrangements.

We will always operate CCTV proportionately and transparently, in line with:

- the UK General Data Protection Regulation (UK GDPR)
- the Data Protection Act 2018 (DPA 2018)
- the Human Rights Act 1998 (Article 8)
- the Home Office Surveillance Camera Code of Practice (2022).

CCTV forms part of our safeguarding governance and is operated consistently with Keeping Children Safe in Education (KCSIE).

Legal framework

This policy has due regard to the following legislation and guidance:

• UK General Data Protection Regulation (UK GDPR)
• Data Protection Act 2018
• Protection of Freedoms Act 2012 and the Surveillance Camera Code of Practice (updated 2022)
• Human Rights Act 1998 (Article 8 – right to private and family life)
• Regulation of Investigatory Powers Act 2000 (covert surveillance – in exceptional circumstances only)
• Freedom of Information Act 2000 and associated Fees Regulations 2004
• Education (Pupil Information) (England) Regulations 2005 (as amended)
• Equality Act 2010
• Relevant ICO CCTV and video surveillance guidance (under ongoing review following the Data (Use and Access) Act 2025)

Definitions

Surveillance – monitoring movements and behaviour of individuals; for this policy, this refers to video images only.

Overt surveillance – surveillance where people are informed via signage/policy.

Covert surveillance – surveillance intentionally not shared with subjects. The school will not use covert surveillance except in extreme circumstances, and only where lawful and necessary (e.g., with police advice and in accordance with RIPA).

Roles and responsibilities

Data controller – Fioretti Trust (with delegated responsibility to the Local Governing Body of St Barnabas C of E Primary School for day-to-day compliance).

Data Protection Officer (DPO) – Sarah Wisdom (CEO Fioretti Trust) with consultancy and advice from Savvy IT. The DPO advises on compliance, oversees DPIAs, monitors processing and is the contact point with the ICO.

Head Teacher – ensures lawful operation of CCTV, approves locations and purposes with the School Business Manager, ensures policy implementation and staff communication.
School Business Manager (Data Processor role for operational purposes) – manages day-to-day operation, access controls, retention and deletion in line with this policy; maintains access logs; ensures secure configuration and contractor compliance.
Governing Body – has regard to the Surveillance Camera Code of Practice, ensures adequate resources and oversight, and reviews annual CCTV compliance within safeguarding governance.

Purpose and lawful basis
Purpose – to maintain a safe and secure school environment; deter and detect crime; protect pupils, staff, visitors and school property; and support the investigation of incidents.
Lawful basis – the primary lawful basis for processing is 'public task' (performing a task in the public interest/exercise of official authority). In limited circumstances, 'legitimate interests' may also apply (e.g., crime prevention where appropriate).
CCTV is not used for routine monitoring of staff performance. Cameras will not be installed in classrooms, changing rooms or toilets. Any exceptional placement would require a documented, specific DPIA and legal justification.

The data protection principles
• We process personal data lawfully, fairly and transparently.
• We collect data for specified, explicit and legitimate purposes, and do not process further in incompatible ways.
• We minimise data – only adequate, relevant and necessary footage is captured.
• We ensure accuracy and take steps to erase or rectify inaccuracies without delay.
• We limit storage – standard retention is 30 days unless footage is required for an ongoing investigation or legal proceedings, in which case it may be retained only as long as necessary and then securely deleted.
• We ensure integrity and confidentiality – appropriate technical and organisational measures are applied, and we demonstrate accountability (e.g., policies, DPIAs, training, logs).

Objectives
• Maintain a safe environment.
• Safeguard pupils, staff and visitors.
• Deter and prosecute criminal acts against persons and property.
• Assist the police in identifying persons who have committed an offence.

Protocols
• The school pays the ICO data protection fee, where required, and maintains an up-to-date Record of Processing Activities (RoPA).
• CCTV signage is prominently displayed at all entrances and within the site, stating the purpose, data controller and contact details.
• Cameras are positioned for maximum effectiveness and minimum intrusion. Cameras are not directed at private property beyond the school perimeter.
• The system records video images only; audio is not recorded.
• The retention period is 14 days, reviewed annually and justified via the DPIA.
• Any proposal to introduce new cameras, analytics or change locations requires a DPIA before

implementation.

Security

• Access is restricted to authorised operators: Head Teacher, School Business Manager, Pastoral Manager, and the DPO or audit/advice.
• Systems are protected with strong, unique passwords and multi-factor authentication where available. Remote access is restricted to approved devices and encrypted connections.
• Footage is encrypted at rest (where supported) and in transit. The main control facility is locked when not in use.
• All access to live view or playback is logged and retained for a minimum of 12 months.
• CCTV equipment is checked monthly for faults, with remedial action taken promptly to prevent data breaches.
• Third-party suppliers are subject to due diligence and data processing agreements that meet UK GDPR standards.

Privacy by design

• A DPIA is completed before installation or any significant change (e.g., new locations, new analytics, cloud migration).
• If high risk remains after mitigations, the school will consult the ICO prior to proceeding.
• We ensure necessity and proportionality, and seek less intrusive alternatives where appropriate.

Code of practice

• The school has regard to the Home Office Surveillance Camera Code of Practice (2022) and its 12 guiding principles, including transparency, accountability, clear governance, data minimisation, security and regular review.
• Images and information are used only for their intended purposes and access is strictly controlled.

Access

Individuals have the right to request access to their personal data (Subject Access Request – SAR). Identity will be verified prior to disclosure.
Where footage contains third parties, we will consider redaction or whether disclosure would adversely affect the rights of others.
We normally respond within one month; complex or numerous requests may be extended by two months with notification within one month.
Police requests: disclosures will be recorded and only made where lawful, noting officer details, case reference and legal basis.
All media containing images remains the property of the Trust.

Monitoring and review

This policy is reviewed at least every three years, or sooner if legislation or technology changes.
An annual CCTV compliance review is undertaken by SLT (including the DSL) and reported to the Governing Body as part of safeguarding governance.
The DPO and data controller monitor legal changes and update this policy and associated DPIAs accordingly.