CCTV Policy

2026-27

Document Date: September 2026

Contents Page

Document Control	**3**
Version Changes	**3**
Vision and Values	**4**
1 Introduction	**4**
2 Statement of Intent	**5**
3 Siting the Cameras	**5**
4 Covert Monitoring	**6**
5 Storage and Retention of CCTV Images	**6**
6 Access to CCTV Images	**7**
7 Subject Access Requests (SAR)	**7**
8 Access to and Disclosure of Images to Third Parties	**7**
9 Complaints	**8**
10 Further Information	**8**

©2026 Firebird Data Protection Consultancy Limited

Document Control

Review Frequency	Annual
Review Date	September 2027
Ratified By	CAST SELT
Date of Ratification	22.09.26
Lead/Owner	Chief Operating Officer
Target Audience	Headteachers, senior staff, and Trust leaders who operate and oversee CCTV systems within Plymouth CAST schools.
Document Version	1.3

The electronic version is the definitive version of this document.

The content of this procedure may be subject to revision from time to time in line with the policy review schedule or when legislation changes or operational reasons arise. Consultation with the recognised trade unions will be completed before any changes are made.

Version Changes

Version	Page Number	Details of Change	Agreed By	Date
1.3	Various	Updated CCTV Policy aligned with the school CCTV DPIA, current data protection requirements and school CCTV controls.	SELT	22.09.26

©2026 Firebird Data Protection Consultancy Limited

Vision and Values

Plymouth CAST is a multi-academy trust of Catholic schools which is part of the mission of the Catholic Church dedicated to human flourishing and the building of a kingdom of peace, truth and justice. The Trust is to be conducted in all aspects in accordance with canon law and the teachings of the Roman Catholic Church and at all times to serve as a witness to the Catholic faith in Our Lord Jesus Christ.

Our vision and values are derived from our identity as a Catholic Trust. Central to our vision is the dignity of the human person, especially the most vulnerable. Our academies are dedicated to providing an education and formation where all our pupils and young people flourish in a safe, nurturing, enriching environment. All governors in our academies are expected to be familiar with the vision, mission, values and principles of the Trust and not in any way to undermine them. They should support and promote the vision and conduct themselves at all times in school and on school business according to the vision and principles of the Trust.

Plymouth CAST expects all its employees to recognise their obligations to each school within the Multi-Academy Trust, the public, pupils and other employees and to provide consistently high standards of education and performance at all times and in accordance with Plymouth CAST's vision, mission and principles.

1. Introduction and purpose

1. This policy sets out the school's arrangements for the use of Closed-Circuit Television (CCTV) in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other applicable data protection legislation (collectively referred to as the 'data protection legislation').
2. The school is the data controller for personal data captured through its CCTV system and is responsible for ensuring that CCTV is used lawfully, fairly, transparently and only where it is necessary and proportionate.
3. The purpose of this policy is to explain why CCTV is used, how cameras and footage are managed, who may access or receive footage, how long recordings are kept and the controls the school applies to protect the rights and privacy of individuals.

2. Scope

1. This policy applies to CCTV operated by or on behalf of the school and to images of pupils/students, employees, volunteers, governors/trustees, contractors, parents/carers, visitors, members of the public and any other identifiable person captured by the cameras.
2. This policy covers visual CCTV only. Audio recording, facial recognition, biometric identification, automatic number plate recognition (ANPR), automated identification and other materially more intrusive surveillance technologies are outside its scope and shall not be enabled unless separately assessed and approved.
3. This policy should be read alongside the school's other policies, procedures and documentation, including:

©2026 Firebird Data Protection Consultancy Limited

- Privacy Notice
- Data Protection Policy
- CCTV Data Protection Impact Assessment (DPIA)
- Record Retention Schedule
- Personal Data Breach Handling Procedure
- Data Protection Request Handling Procedure
- Data Protection Complaints Handling Procedure
- Safeguarding / Child Protection Policy

3. Definitions

1. Key terms used in this policy are explained in Appendix 1.

4. Roles and responsibilities

1. Governing Body

2. The Governing Body has overall responsibility for ensuring that the school operates CCTV in accordance with this policy and the data protection legislation. It shall receive appropriate assurance that the purposes, camera locations, access arrangements, retention and review arrangements remain appropriate.

3. Headteacher

4. The Headteacher has day-to-day responsibility for ensuring that this policy is implemented and that CCTV is used only for approved purposes. Material changes to camera coverage, purpose or functionality shall be appropriately assessed before implementation.

5. Data Protection Officer

6. The Data Protection Officer (DPO) advises the school on compliance, necessity and proportionality, Data Protection Impact Assessments, individual rights, disclosure and complaints relating to CCTV. The school's DPO is Firebird Data Protection Consultancy Limited and can be contacted through the school or directly at DPO@firebirdltd.co.uk.

7. CCTV responsible person

8. The school shall nominate a person with operational responsibility for CCTV: J Merriman, senior administrator. They shall oversee authorised access, retention and deletion, disclosures, signage, camera reviews and liaison with relevant suppliers or IT support.

9. Employees, contractors and authorised users

10. Employees, contractors and other authorised users shall access CCTV only where they have a legitimate reason and permission to do so. Footage shall be kept confidential and shall not be copied, downloaded, photographed, shared or used for personal purposes unless specifically authorised.

5. Purposes and lawful basis

©2026 Firebird Data Protection Consultancy Limited

1. The school may use CCTV where this is necessary and proportionate to support safeguarding and the safe management of the site; protect pupils/students, staff, visitors, buildings and property; deter or investigate crime, vandalism and serious incidents; assist in emergencies; and provide a reliable visual record where an incident, complaint, insurance matter or legal claim requires investigation.
2. CCTV shall not be installed or used simply because surveillance technology is available, and it shall not routinely be used to monitor staff performance or to watch particular individuals without a defined, necessary and lawful purpose.
3. For maintained and academy schools, Article 6(1)(e) UK GDPR - Public Task / Official Authority will commonly be the appropriate lawful basis where CCTV is necessary for safeguarding, site safety or other official school functions. Article 6(1)(c). Consent will not normally be relied upon because individuals cannot realistically opt out of being captured when using monitored areas of the school site.
4. Where footage is used in circumstances which reveal special category data or criminal offence information, the school shall identify and document any additional condition required under the UK GDPR and Data Protection Act 2018 in their Privacy Notices and Appropriate Policy Document.

6. Camera locations and operation

1. Each camera shall have a defined purpose and shall be positioned only where CCTV is reasonably necessary. Before installing or materially extending CCTV, the school shall consider whether less intrusive measures such as improved supervision, lighting, access control, site layout or staffing could reasonably achieve the same purpose.
2. Camera angles, zoom and recording schedules shall be configured to avoid unnecessary capture. Privacy masking shall be used where appropriate to block or obscure areas which do not need to be monitored, such as neighbouring homes, private property or parts of public areas outside the school's legitimate coverage.
3. Cameras shall not normally be placed in toilets, changing rooms or other areas where individuals have a particularly high expectation of privacy. Any exceptional proposal shall require a separate, specific assessment and very strong justification before implementation.
4. Audio recording and facial recognition shall remain switched off. The school shall check, where appropriate following system updates or configuration changes, that disabled features have not been inadvertently enabled.
5. Where live viewing is used, it shall be restricted to authorised staff and necessary operational, safeguarding or security purposes. Screens shall be positioned to prevent casual viewing by unauthorised individuals.

7. Access to and use of CCTV footage

1. Recorded footage shall be accessed only where there is a genuine reason, for example to investigate a safeguarding concern, accident, security incident, suspected crime, property damage, serious behaviour incident or other significant matter affecting the school community.
2. Access shall be limited according to role and genuine need. Where available, the school shall use suitable authentication, role-based permissions and audit logging to protect footage and maintain accountability for access.
3. CCTV footage shall be treated as one source of evidence rather than automatic proof. Images may show only part of an incident and, because audio is not recorded, may not provide the full context.

©2026 Firebird Data Protection Consultancy Limited

The school shall consider the wider circumstances and other relevant evidence before making significant safeguarding, behaviour, disciplinary or employment decisions.

8. Retention and deletion

1. Routine CCTV footage shall be retained for no longer than is necessary for the purposes for which CCTV is operated. The school's normal CCTV retention period is: one month.
2. At the end of the normal retention period, footage shall normally be automatically overwritten or securely deleted. The school shall periodically review the retention period to ensure that it remains necessary and proportionate.
3. A relevant clip may be retained for longer where this is necessary for a defined purpose, such as an active safeguarding matter, investigation, police request, complaint, disciplinary process, insurance matter or legal claim. It shall be deleted when no longer required for that purpose.

9. Sharing and disclosure

1. The school may disclose CCTV footage where this is necessary, lawful and proportionate. Recipients may include the police, local authority, safeguarding professionals, insurers, legal advisers, courts or tribunals, or another authorised body or individual where there is an appropriate lawful reason.
2. Before disclosure, the school shall verify the identity and authority of the requester, consider the purpose and necessity of the request, disclose only the footage required and consider whether images or information relating to other people need to be blurred, withheld or otherwise protected. All disclosures should be recorded.
3. A request from the police or another public authority does not automatically require disclosure of all footage requested. The school shall consider the request in accordance with its data sharing procedures and may seek written confirmation of the purpose and legal basis where appropriate.

10. Individual rights and requests

1. Individuals may exercise their data protection rights in relation to CCTV footage, subject to any lawful exemptions. Requests for access shall be handled under the school's Data Protection Request Handling Procedure.
2. The school may ask for information needed to locate footage, such as the date, approximate time, location, description of the individual and details of the incident or circumstances. Before releasing footage, the school shall consider the rights and privacy of other people appearing in it and any safeguarding implications.
3. A parent or carer does not have an automatic right to receive CCTV footage merely because their child appears in it. Requests shall be considered in accordance with data protection law, taking account of the child's rights, age and understanding, third-party information and any safeguarding considerations.

11. Security, suppliers and remote access

1. The school shall protect live and recorded footage against unauthorised or unlawful access, alteration, loss or disclosure. Appropriate controls shall include role-based access, secure authentication, restricted administrator privileges, secure storage, controlled exports and downloads, secure transfer and prompt removal of access when staff change role or leave.

©2026 Firebird Data Protection Consultancy Limited

2. Portable copies of footage shall not be created unless necessary. Any suspected loss, unauthorised access or disclosure shall be managed under the school's Personal Data Breach Handling Procedure.
3. Where a CCTV supplier, cloud-hosting provider, maintenance company, IT provider or remote-monitoring service processes footage on the school's behalf, the school shall complete appropriate supplier due diligence and ensure Article 28 UK GDPR processor terms are in place where required.
4. The school shall establish where footage is stored or remotely accessed, who can access it, which subprocessors are involved, the security and deletion arrangements, and whether processing or access takes place outside the UK. Appropriate safeguards shall be documented for any restricted international transfer.

12. Transparency and signage

1. Clear CCTV signs shall be displayed at appropriate entrances and monitored areas so that individuals know CCTV is in operation. Signage shall identify the school as the organisation responsible for the CCTV and provide an appropriate contact route or indicate where further privacy information can be obtained.
2. The school's Privacy Notice and this policy shall explain the main purposes for which CCTV footage is processed, who it may be shared with, the applicable retention arrangements and how individuals can exercise their data protection rights.

13. New technology and changes to the system

1. The school shall review its CCTV DPIA before making a material change to the system, including adding or repositioning cameras, materially widening coverage, changing the purpose, introducing remote viewing or cloud hosting, or enabling analytics or other enhanced functionality.
2. Audio recording, ANPR, facial recognition, biometric identification, automated identification or tracking and other materially more intrusive surveillance shall not be introduced under this policy without a separate or revised DPIA, appropriate legal assessment and formal approval.
3. Where a change materially affects what individuals are told or reasonably expect, the school shall update signage, privacy information and consultation arrangements as appropriate before the change is implemented.

14. Complaints, monitoring and review

1. Concerns or complaints about the school's use of CCTV or handling of footage shall be managed under the Data Protection Complaints Handling Procedure. The school's Data Protection Officer shall be consulted where appropriate. Individuals who remain dissatisfied may complain to the Information Commissioner's Office.
2. The school shall review its CCTV arrangements and this policy at least annually and sooner where cameras, purposes, retention, remote access, suppliers, hosting or surveillance features change materially, or where a significant incident or complaint identifies a concern.
3. The review shall consider whether each camera remains necessary, whether coverage remains proportionate, whether access permissions remain appropriate, whether the retention period remains justified and whether disabled features remain disabled.

©2026 Firebird Data Protection Consultancy Limited

Appendix 1

CCTV Policy Definitions

Term Used	Summary Definition
CCTV	Closed-circuit television used to capture and, where configured, record visual images of identifiable individuals.
Personal data	Information relating to an identified or identifiable living individual. CCTV images are personal data where a person can be identified directly or indirectly.
Data controller	The organisation which determines the purposes and means of processing personal data. For CCTV covered by this policy, this is the school.
Data processor	An organisation which processes personal data on behalf of the school and on its instructions, for example certain hosted CCTV or maintenance providers.
Privacy masking	A camera configuration which blocks or obscures areas that do not need to be monitored, such as neighbouring private property.
Live viewing	Viewing camera images in real time rather than reviewing recorded footage.
Footage	Recorded or live visual images captured by the CCTV system.

©2026 Firebird Data Protection Consultancy Limited



Our mission is to be a community of outstanding schools in which our pupils flourish in safe, happy and stimulating environments and leave us with the knowledge and skills, personal qualities and aspirations, to make the world a better place, inspired by the gospel.

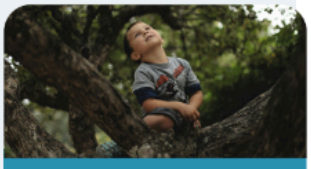
Plymouth CAST



Collaboration

We are one team, being the best we can be. We achieve more altogether - one Trust, one family of schools, one community.

We are united through our faith, families and staff.



Ambition

We want our children to be happy and to flourish, achieving well.

Across all areas, we work as one team to drive up standards. We are courageous in our decision making and aspirations.

Through the strength of our ambition, we create a distinct brand and culture.



Stewardship

Justice, forgiveness and integrity are central to the gospels and drive our decision-making. Underpinning this is a relentless approach to safety, reliability and consistency.

As key influencers of our children's impact on society and the environment, we encourage sustainable and brave decision-making, based on a beliefs-led approach.



Trust

We are authentic, transparent, open and honest.

Through compassion and kindness, we show humility to each other.

This page contains Plymouth CAST branding graphics and visual representations of the Trust's mission and values. The Trust's mission is to create outstanding schools where pupils flourish in safe, happy and stimulating environments inspired by the Gospel. The Trust's core values are collaboration, ambition, stewardship and trust.

©2026 Firebird Data Protection Consultancy Limited