Pathway Trust

CCTV Policy

Policy effective from	1 September 2026
Policy owner	Head of Governance
Policy applies to	Berrow Church Primary School Burnham-on-Sea Infant School Castle Batch Primary School Charfield Primary School Cherry Garden Primary School Downend School East Huntspill Primary School Lyde Green Primary School Mangotsfield School Marlwood School Pawlett Primary School Priory Community School Severn Beach Primary School St Andrew's Church Junior School St Anne's Church Primary School The Castle School The King Alfred School Tortworth Primary School West Huntspill Primary School Worle Community School Pathway Partnership Teams
Policy changes since last version	New policy

1. About this Policy

This CCTV Policy has been developed for Pathway Trust (trust) in accordance with the latest Department for Education (DfE) guidance, ensuring compliance with the following legal framework and statutory guidance:

1.1. Data Protection & Privacy

- UK General Data Protection Regulation (UK GDPR): Governs the lawful basis for processing personal data (images). The trust primarily relies on Article 6(1)(e) (Public Task), Article (6)(1)(f) (Legitimate Interests) and additionally with regards to special category/criminal offence data, Article 9(2)(g) (Substantial Public Interest) for safeguarding and crime prevention.
- Data Protection Act 2018 (DPA): specific provisions for preventing and detecting unlawful acts (Schedule 1, Paragraph 10).
- Human Rights Act 1998: Specifically, Article 8 (Right to Respect for Private and Family Life). Any surveillance must be a "proportionate" interference with this right and have a clear legal basis.

1.2. Surveillance Specifics

- Protection of Freedoms Act 2012 (PoFA): Governs the use of surveillance camera systems by relevant authorities. It requires the trust to have regard for the Surveillance Camera Code of Practice.
- Surveillance Camera Code of Practice (The "12 Guiding Principles"): Issued by the Biometrics and Surveillance Camera Commissioner. It demands that surveillance be necessary, transparent, and meet a "pressing social need."
- ICO Video Surveillance Guidance: Practical standards set by the Information Commissioner's Office on how to manage recordings, storage, and Subject Access Requests.

1.3. Education & Safeguarding

- Keeping Children Safe in Education (KCSIE 2026): The DfE's statutory guidance which identifies CCTV as a tool for a "strong safeguarding culture" when used appropriately to monitor busy areas or deter harm.
- Education (Pupil Information) (England) Regulations 2005: Relates to how schools manage and share information regarding their students.
- DfE Digital Standards (2025/26): Technical requirements for school networks, ensuring that CCTV systems are secure, updated, and protected from cyber-attacks.

1.4. Transparency & Access

- Freedom of Information Act 2000 (FOIA): As public authorities, schools must respond to requests for information about their CCTV systems (e.g., number of cameras, costs, or policies), provided it does not compromise security.

2. Policy Statement & Purpose

2.1 The trust uses Closed Circuit Television (CCTV) across its primary and secondary schools to enhance safety and security. We are committed to ensuring that our use of CCTV is necessary, proportionate, and respects the privacy of our pupils, staff, and visitors.

In line with DfE guidance, we use CCTV for the following specific purposes:

- Maintain a safe environment.
- Support in safeguarding the welfare of pupils, staff and visitors.
- Deter criminal acts against persons and property.
- Assist the police in identifying persons to have committed an offence.

3. Lawful Basis for Processing

3.1 The trust processes personal data captured by CCTV under the following lawful bases:

- Public Task: Where the use of CCTV is necessary for the school to carry out its official duties as an educational provider.
- Legitimate Interests: Where the trust or a third party has a clear recognised legitimate interest in using CCTV (e.g., crime prevention).
- Substantial Public Interest: Where the trust or a third party needs to process special category/criminal offence data for safeguarding and crime prevention purposes.

4. Privacy by Design & Proportionality

4.1 Before installing or updating any system, the trust will:

- Assess Alternatives: Explore less intrusive methods first (e.g. changing canteen layouts or staggering breaks to manage overcrowding).
- Conduct a DPIA: Complete a Data Protection Impact Assessment for every school to identify and mitigate risks to individuals' rights.
- Technical Standards: Ensure systems are of good quality and "limited to what is necessary."
    - Facial Recognition: Live facial recognition is prohibited and must be switched off by default.
    - Audio Recording: Continuous audio recording is prohibited as it is highly intrusive. This feature must be disabled.

5. Camera Placement & Sensitive Areas

5.1 Cameras will be positioned only where there is a justified and proportionate need. Schools must consult with the trust's estates team if they are looking to change or expand their CCTV provision.

- Restricted Areas: If cameras have a wider range than required, the field of vision will be restricted/masked to capture only the relevant area.
- High Privacy Areas: Any use in these areas (e.g., communal washbasins to prevent vandalism) must be specifically justified in the DPIA and never monitor cubicles, changing areas, showers or urinals.

6. Transparency & Consultation

6.1 The trust is committed to being "open and honest" about surveillance:

- Signage: Clearly visible signs are placed at all site entrances and near cameras, explaining the purpose of the CCTV and providing contact details.
- Privacy Notices: The trust and school websites will host updated Privacy Notices detailing why footage is kept, for how long, and with whom it is shared.

7. Retention & Data Security

- Retention Period: Footage is kept for the shortest period necessary to meet the intended purpose, 30 days (unless extended retention is required for an investigation). Footage will not be kept longer simply because storage space allows it.
- Storage: Data is stored securely and encrypted where possible. Rooms hosting CCTV hardware (NVRs/Servers) remain locked and accessible only to authorised staff.
- Access: Only staff trained by the IT team are approved to access the CCTV system. In all schools this is the Headteacher, DSL and one additional member of staff appointed by the Headteacher. Where single screens are in operation two members of staff must be present when viewing the CCTV. Where the application is installed on to an approved staff member's computer, two approved staff members must be present to view the CCTV. No copies of the footage should be made. All viewing of the CCTV should be via the system.
- Log: An up to date sheet must be kept of all access to the CCTV, copies should not be made of the footage (unless this is necessary as per section 8) or it should not be shared outside of the individuals viewing it (unless there is a lawful purpose as per section 8).
- Breaches: Any breach or suspected breach must be reported immediately to the Information Governance Manager.

8. Access for third parties

8.1 Under the UK GDPR and Data Protection Act 2018, individuals have the right to obtain confirmation that their personal information is being processed.

8.2 All images belong to, and remain the property of, the respective school.

8.3 Individuals have the right to submit a Subject Access Request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. Requests must be submitted in writing to dataprotection@pathwaytrust.uk

8.4 The school will verify the identity of the person making the request before any information is supplied and consult with the Information Governance Manager on how to respond to the request. Due care must be given to the confidentiality of third parties captured in images including blurring third parties where technically possible and/or withholding images/metadata that identifies third parties.

8.5 A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

8.6 Where an SAR has been made electronically, the information will be provided in a commonly used electronic format.

8.7 All requests will be responded to without delay and at the latest, within one month of receipt.

8.8 In the event of numerous or complex requests, the period of compliance may be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

8.9 Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the Information Commissioner's Office (ICO) within one month of the refusal.

8.10 In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

8.11 It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.

8.12 Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

- The police – where the images recorded would assist in a specific criminal inquiry.
- Prosecution agencies – such as the Crown Prosecution Service (CPS).
- Relevant legal representatives – such as lawyers and barristers.

- Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000.

8.13 Requests by persons outside the school for viewing or copying disks, or obtaining digital recordings, will be assessed by the Headteacher and Information Governance Manager on a case-by-case basis with close regard to data protection and freedom of information legislation.

8.14 Requests for access or disclosure will be recorded and the Headteacher and Information Governance Manager will make the final decision as to whether recorded images may be released to persons other than the police. Generally, police should submit their relevant force's data release form unless access is required for an emergency situation such as a missing person.

9. Review

9.1 This policy will be reviewed annually unless a change in legislation or statutory guidance necessitates earlier review.