# CCTV Policy

| | |
|---|---|
| **Review Due:** | **November 2026** |
| **Last Review** | November 2025 |
| **Applicable to:** | All Trust Schools |
| **Reviewed By:** | SV |
| **Approved By:** | Trust Board |

| **Policy Review Notes** | |
|---|---|
| **Date** | **Action** |
| February 2022 | Policy approval by Trust Board |
| July 2022 | Review to bring in line with all GDPR related policies and privacy notices, proposed changes to para 3 to align with One West Template Policy and requires school level personalisation. |
| September 2023 | To align with latest One West Template Policy. |
| September 2024 | To align with updated OneWest Template Policy |
| November 2025 | To align with updated OneWest Template Policy |

## Contents

1. Introduction ..... 3
2. Definitions ..... 3
3. Purpose ..... 4
4. Scope ..... 4
5. Principles of Use ..... 5
6. Justification for use of CCTV ..... 6
7. Governance of CCTV ..... 6
8. Responsibilities ..... 7
9. Data Protection Impact Assessment ..... 8
10. Location of Cameras ..... 8
11. Covert surveillance ..... 8
12. Transparency - Notification, Signage and Awareness ..... 8
13. Storage & Retention ..... 10
14. Access to data (video footage) ..... 11
15. Review of policy ..... 12

Appendix 1 – Schools with CCTV ..... 12

# 1. Introduction

Since its widespread introduction to retailers in 1960s and then to town centres in 1980s, the use of Closed-Circuit Television (CCTV) across the UK has become increasingly popular. CCTV is a valuable tool to assist with efforts to combat crime and disorder, while enhancing safety in schools.

This policy is published on behalf of the Board of Trustees of The Partnership Trust. This document sets out the policy covering the use and management of CCTV equipment and images to ensure that The Partnership Trust complies with the Data Protection Legislation and other relevant legislation. Crucially personal data is processed in line with The Partnership Trust's Data Protection Policy. The Partnership Trust's use of CCTV is cognisant of the Guiding Principles of the Surveillance Camera Code of Practice updated and published by the Home Office in 2021.

The Partnership Trust uses CCTV for the purposes of the prevention and detection of crime, keeping pupils, parents, residents, staff, volunteers and visitors safe and to recognise and identify individuals with a view to taking appropriate action where necessary.

This policy and related procedures apply to all sites managed by The Partnership Trust. CCTV systems are installed in some schools in the trust – these are listed in Appendix 1.

# 2. Definitions

**CCTV** – CCTV (closed-circuit television) is a video surveillance system in which signals are transmitted to a specific set of monitors and are not publicly broadcast. It is primarily used for security and monitoring purposes.

**Data Controller** - a person who (either alone or with others) controls the contents and use of personal data.

**Data Processing** - performing any operation or set of operations on data, including:

- Obtaining, recording, or keeping the data,
- Collecting, organising, storing, altering, or adapting the data,
- Retrieving, consulting, or using the data,
- Disclosing the data by transmitting, disseminating, or otherwise making it available,
- Aligning, combining, blocking, erasing, or destroying the data.

**Data Processor** - a person/organisation who processes personal data on behalf of a data controller. Employees of a controller are not processors as long as they are acting within the scope of their duties as an employee.

**Data Protection Legislation –** this means the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR).

**Data Subject** – a living individual who can be identified, directly or indirectly, from the personal data that is held about them.

**Directed Surveillance** – covert surveillance in places other than residential premises or private vehicles.

**Personal Data** – data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

**Subject Access Request** - this is where a person makes a request to the organisation for the disclosure of their personal data under the Data Protection Laws.

## 3. Purpose

The purpose of this policy is to regulate the use of CCTV and its associated technology in the monitoring of both the internal and external environs of the premises under the remit of The Partnership Trust.

This policy has been used as the basis for siting CCTV cameras and associated equipment and defines the governance of surrounding use of CCTV equipment and the related processing activities. The policy ensures that ***Data Protection by Design*** is a key consideration in all The Partnership Trust's CCTV processes and help ensure that the rights of data subjects are always met.

CCTV at The Partnership Trust (and its schools) is intended for the purposes of:

- Protecting buildings and assets, both during and after working hours.
- Promoting the health and safety of staff, pupils, and visitors.
- Preventing bullying.
- Reducing the incidence of crime and anti-social behaviour (including theft and vandalism).
- Supporting the Police in a bid to deter and detect crime.
- Assisting in the identification, apprehension, and prosecution of offenders.
- Ensuring that the school rules are respected so that the school can be properly managed.

This policy will be published on the Trust's website and the existence of this policy and any subsequent changes to the policy will be notified to pupils, parents, staff and volunteers.

## 4. Scope

This policy applies to the use of CCTV regardless of whether there is any live viewing or recording of images or information or associated data. Covert surveillance using CCTV is not covered by this policy.

## 5. Principles of Use

The use of a CCTV system by Hayesdown First School follows the 12 Guiding Principles of the Surveillance Camera Code of Practice updated and published by the Home Office in 2021. Each principle is summarised below:

**Principle 1** - Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

**Principle 2** - The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

**Principle 3** - There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

**Principle 4** - There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

**Principle 5** - Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

**Principle 6** - No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

**Principle 7** - Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

**Principle 8** - Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

**Principle 9** - Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

**Principle 10** - There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

**Principle 11** - When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

**Principle 12** - Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

## 6. Justification for use of CCTV

The Partnership Trust has responsibility for the protection of its property and equipment as well providing security to its employees, students and visitors to its premises. Moreover, The Partnership Trust owes a duty of care under the Health and Safety at Work etc. Act 1974 and associated legislation. Hence The Partnership Trust uses CCTV and associated monitoring and recording equipment as an additional mode of security and surveillance for each of these purposes. CCTV systems are installed externally and will operate constantly.

Use of CCTV for security purposes will be conducted in a manner consistent with educational and related legislation and all existing policies adopted by the Partnership Trust, including its Equality & Diversity Policy, Dignity at Work Policy, and codes of practice for dealing with complaints of bullying & harassment and sexual harassment.

Importantly CCTV will not be used to monitor normal staff activity on site.

Data Protection Laws requires that personal data is 'adequate, relevant and not excessive' for the purpose for which it is collected. This means that an organisation needs to be able to justify the obtaining and use of personal data by means of a CCTV system. The use of CCTV to monitor and help control the perimeter of The Partnership Trust for security purposes has been justified by the board of trustees. The system is intended to capture images of intruders or of individuals damaging property or removing goods without authorisation.

In other areas where CCTV has been installed, The Partnership Trust has demonstrated that there is a proven risk to security and/or health & safety and that the installation of CCTV is proportionate in addressing such issues that have arisen prior to the installation of the system.

All CCTV systems and associated equipment will be required to be compliant with this policy following its adoption. Recognisable images captured by CCTV systems are 'personal data.' They are therefore subject to the provisions of the Data Protection Act 2018.

It is likely that information obtained in ways that violate this policy may not be used in any legal or disciplinary proceedings.

## 7. Governance of CCTV

The school's CCTV system is a standalone one (it is not connected to (networked) and / or operated by a third-party, such as another school, a local council or a contractor). The use of the school's CCTV is governed by this policy and related processes.

The Data Controller, which is the Head Teacher, is accountable for operation of the CCTV at The Partnership Trust and responsible for:

- Working with the DPO to keep this policy up to date reflecting any changes to national guidance, best practice or statutory instruments that determine the use of CCTV or personal data.
- Ensuring the CCTV is setup, operated and controlled, and is periodically checked for compliance according to this policy.
- Processes and procedures covering day-to-day operation of the CCTV and the subsequent oversight of activities covered by these processes and procedures.
- Completion of a Data Protection Impact Assessment (DPIA) for the CCTV system/s and then annual review of this DPIA.
- Consulting the school's / trust's senior leadership team and legal advisors should the Police request permission to install any surveillance equipment for criminal investigations.
- Considering any feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment from students / members of the public and staff.

## 8. Responsibilities

The Schools Headteacher is responsible day-to-day for operation of the CCTV. They can be contacted on office@hayesdownschool.com. Their contact details are also presented on signage displayed where CCTV cameras are used.

Processes and procedures that have been delegated to them and will be monitored and checked for compliance periodically include:

- Ensuring compliance with the principle of 'Reasonable Expectation of Privacy' by periodically checking that cameras are operating / operated as designed.
- Maintaining the security of the CCTV and any data held on the system.
- Keeping a record of access (e.g. an access log) to the system and to imagery / video footage held on the system.
- The initial processing of an application for release of any information or imagery / footage from the CCTV stored in compliance with this policy.
- Retaining data captured and stored by the CCTV only for the period specified in the school's / trust's data retention schedule unless it is required as part of a criminal investigation or court proceedings (criminal or civil) or other use approved by senior management in consultation with the DPO.

## 9. Data Protection Impact Assessment

Prior to the adoption of any new CCTV system or where an existing system is identified as not having been assessed, a comprehensive DPIA must be undertaken. This will include a review of the purpose or purposes for the use of CCTV; establish any impact it may have upon individuals; and any risks that may be involved with the system.

The Headteacher or delegated individual will be responsible for completing the DPIA in collaboration with the DPO. Should a third party be used to deliver CCTV the person from the school responsible for its implementation will work alongside the third party and the DPO to ensure that the DPIA is completed.

The One West DPIA for CCTV template should be used as the basis for The schools DPIA.

## 10. Location of Cameras

The Partnership Trust has endeavoured to select locations for the installation of CCTV cameras to achieve the aim/s of installing CCTV while having a minimum impact on the privacy of individuals. Cameras installed to record external areas are positioned to prevent or minimise the recording of passers-by or of another person's private property.

The following locations may be covered by CCTV at The Partnership Trust:

- The building's perimeter, entrances and exits, lobbies and corridors, special storage areas, cashier locations and receiving areas for goods and services.
- Restricted access areas at entrances to buildings and other areas for the purpose of controlling access.
- Intrusion alarms, exit door controls and areas covered by external alarm for the purpose of verifying such alarms.
- Parking areas, main entrance/exit gates, and places where there is traffic control, for the purpose of video patrolling if an incident occurs involving pupils, staff and/or visitors to the school.

## 11. Covert surveillance

The Partnership Trust will not engage in covert surveillance using CCTV. Very occasionally the police may request to carry out covert surveillance using the school's equipment. Covert surveillance will require the consent of an Authorising Officer, which may be a magistrate. Any such request made by the police will be in writing and the school may seek legal advice.

## 12. Transparency - Notification, Signage and Awareness

CCTV signage is necessary for transparency. Hence, to indicate that CCTV is in operation, The Partnership Trust displays adequate signage at the entrance/s to the schools and where a CCTV camera(s) is sited.

Signage shall include the name and contact details of the Data Controller, as well as details of why CCTV is used.

An example of the signage used by The Partnership Trust is shown below.

**WARNING**

**CCTV cameras in operation**

**Images are being monitored and recorded for the purpose of crime-prevention, the prevention of anti-social behaviour, the prevention of bullying, for the safety of our staff and students and for the protection of *Hayesdown First School* and its property. This system will be in operation 24 hours a day, every day.**

**These images may be passed to the police.**

**This scheme is controlled by and operated by Hayesdown First School**

**For more information contact *Hayesdown First School***

Appropriate locations for signage will include:

- At entrances to premises i.e. external doors, school gates.
- Reception area.
- At or close to each internal camera.

## 13. Storage & Retention

The Partnership Trust's CCTV comprises several CCTV cameras connected to a Network Video Recorder (NVR). Imagery / video footage is stored on the NVR and can be viewed either in real-time (live) or after an event via a console. The system is normally monitored. Where an incident does occur video footage may be referred to as part of an investigation.

A log of access will be maintained that will show who accessed the system at what time and for what purpose. Access to the console and the recorded data will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the Headteacher. They have delegated the day-to-day administration of the CCTV system to The Partnership Trust business manager.

The CCTV imagery is held in digital format that makes it easy to transmit to other organisations. The Partnership Trust CCTV system is isolated from any other system. Where an external organisation, such as the Police, seeks access to the school's imagery / video

footage from the CCTV, access will only be granted when a suitable application has been received by the school.

Importantly, data processed by The Partnership Trust's CCTV 'shall not be kept for longer than is necessary for' the purposes for which it was obtained. The Partnership Trust's CCTV system should not retain footage beyond one month (28 days). Where the images identify an issue, such as a break-in or theft etc., the images / video footage that relate to that event may be retained specifically for the purpose of an investigation/prosecution related to that issue.

The Data Controller will periodically (not less than once per year) review the justification for use of the CCTV to confirm it remains valid and review performance / compliance with process and procedures related to day-to-day operation of The Partnership Trust's CCTV.

Accordingly, the images captured by the CCTV system will be retained for a maximum of 28 days, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue.

Tapes/DVDs will be stored in a secure environment with a log of access to tapes kept. Access will be restricted to authorised personnel. Similar measures will be employed when using disk storage, with automatic logs of access to the images created.

## 14. Access to data (video footage)

Unauthorised access to live feeds, equipment used to store images and any additional equipment that is used to operate The Partnership Trust's CCTV system is prohibited. A log of access to the CCTV system and its components and images / video footage is to be maintained.

Access to the CCTV system and video footage may be granted by The Partnership Trust for the following reasons:

- Where The Partnership Trust (or its agents) are required by law to make a report regarding the commission of a suspected crime.
- Following a request by the police when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on The Partnership Trust's property.
- To provide a report to the Health and Safety Executive and/or any other statutory body with the powers of investigation.
- In response to a court order granted to individuals or their legal representatives.
- To the local authority, or any other statutory body charged with child safeguarding.
- To assist the Headteacher or an appointed representative, to establish facts in cases of unacceptable student behaviour, in which case, the parents/guardians will be informed.

- In response to a Subject Access Request (SAR) presented by data subjects or their legal representatives.
- To the school's insurance company where the company requires information to pursue a claim for damage(s) to the insured property.

Requests by the police should be made formally using a police request form. Any uncertainty regarding the validity of a request should be raised with the DPO.

Any person whose image has been recorded has a right to access the footage which relates to them as part of a Subject Access Request (SAR). Any person or organisation making a request for access to personal data (images / video footage) should provide information, such as the date, time and location of the recording to help The Partnership Trust find the recorded data. The Partnership Trust will follow the organisation's SAR policy that is described at The Partnership Trust's Data Protection Policy.

Importantly, where the image/recording identifies another individual(s), those images may only be released if they can be redacted/anonymised or with the explicit consent of the other people identifiable in the footage.

Depending on circumstances, The Partnership Trust may provide a data subject a copy of their data in the form of a still image / series of still images or as a video on a tape, disk or digital media (SDD).

## 15. Review of policy

The policy will be reviewed on an annual basis or in the event of significant change to the system, national guidance, best practice of legislation relating to the capture of images by CCTV.

This policy was approved by the Board of Trustees on November 2025.

## APPENDIX 1 – DETAILS OF SCHOOLS WITHIN THE PARTNERSHIP TRUST WHO HAVE CCTV ON THEIR SCHOOL SITE

| | | |
|---|---|---|
| Cameley CofE Primary School<br>Meadway,<br>Temple Cloud<br>Bristol<br>BS30 5BD | Tel: 01761 452644<br>office@cameleyprimary.org.uk | The CCTV at this school is non-recording |
| Castle Primary School<br>Newlands Road<br>Keynsham<br>Bristol<br>BS31 2TS | Tel: 0117 986 4489<br>office@castleprimary.uk | The CCTV at this school is recording |
| Fosse Way School<br>Longfellow Road<br>Midsomer Norton<br>Radstock BA3 3AL | 01761 412198<br>office@fossewayschool.com | The CCTV at this school is non recording |
| Hayesdown First School<br>Wyville Road<br>Frome Somerset BA11 2BN | 01373 462718<br>office@hayesdownschool.com | The CCTV at this school is recording |
| The Mendip School<br>Edmund Rack Road<br>Prestleigh, Shepton Mallet<br>Somerset BA4 4FZ | 01749 838040<br>office@themendipschool.com | The CCTV at this school is recording |
| Roundhill Primary School,<br>Mount Rd,<br>Bath BA2 1LG | 01225 424950<br>office@roundhill-pri.co.uk | The CCTV at this school is recording |
| Nunney First School<br>Catch Road<br>Nunney, Frome<br>Somerset BA11 4NE | 01373 836429<br>office@nunneyschool.com | The CCTV at this school is recording |