CCTV Policy

Review Due:	**July 2023**
Last Review	July 2022
Applicable to:	All Trust Schools
Reviewed By:	SV
Approved By:	Trust Board Feb 2021

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.

1. Introduction

Closed Circuit Television (CCTV) Systems are installed in some schools within The Partnership Trust. This policy applies to all schools within The Partnership Trust that have CCTV Systems installed. Those schools are listed in Appendix 3 to this policy.

New CCTV systems will be introduced in consultation with school staff, the Trust's Executive Team, the school's Local Governing Body and the Board of Trustees. Where systems are already in operation, their operation will be reviewed regularly by the school's Headteacher in consultation with staff, the Local Governing Body and Trust Executive Team.

2. Purpose

The purpose of this policy is to regulate the use of Closed Circuit Television 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 includes schools within the Partnership Trust).

CCTV systems are installed in premises for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation within and/or in the external environs of the premises during both the daylight and night hours each day.

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

- protecting the school buildings and school assets, both during and after school hours;
- promoting the health and safety of staff, pupils and visitors;
- 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 identifying, apprehending and prosecuting offenders; and
- ensuring that the school rules are respected so that the school can be properly managed.

3. Scope

This policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material. It will specify the effective governance of CCTV equipment and the related processing activities. The Policy will ensure that Data Protection is incorporated into all school's CCTV processes and that the rights of Data Subjects are appropriately observed.

4. General Principles

The Partnership Trust as the corporate body for all its schools has a statutory responsibility for the protection of its property, equipment and other plant as well providing a sense of security to its employees, students and invitees to its premises. The Partnership Trust owes a duty of care to students, parents, staff and visitors amongst others under the provisions of Safety, Health and Welfare at Work Act 2005 and associated legislation and utilises CCTV systems and their associated monitoring and recording equipment as an added mode of security and surveillance for those purposes. The use of a CCTV system by a school within the Partnership Trust will observe the 12 principles of the Surveillance Camera Code of Practice.

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.

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the school, including Equality Policy and Codes of Practice for dealing with complaints of Bullying & Harassment and other relevant policies, including the provisions set down in equality and other educational and related legislation.

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.

Information obtained in violation of this policy may not be used in a disciplinary proceeding against an employee of the school or a student attending one of its schools.

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

5. CCTV 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 Head Teacher 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 Surveillance Camera Commissioner's (SCC) CCTV DPIA format will be used as the standard template. It is accessible via the DPO and on the SCC's website;

https://www.gov.uk/government/publications/data-protection-impact-assessments-for-surveillance-cameras

6. Location of cameras

The location of cameras is a key consideration. The Partnership Trust and the schools within it have endeavoured to select locations for the installation of CCTCV cameras which are least intrusive to protect the privacy of individuals. Cameras placed so as to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

CCTV Video Monitoring and Recording of Public Areas in the schools within The Partnership Trust may include the following locations:

- The building's perimeter, entrances and exits, lobbies and corridors, special storage areas, cashier locations, receiving areas for goods/services for the purpose of ***protecting school buildings and property.***
- 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, Traffic Control for the purpose of video patrolling in the event that an incident occurs involving the wellbeing or Pupils, Staff or individuals associated to the School.

7. Covert surveillance

The Partnership Trust and the schools within it will not engage in covert surveillance.

Where the police may request to carry out covert surveillance on school premises, such covert surveillance may require the consent of a judge or magistrate. Accordingly, any such request made by the police will be requested in writing and the school will seek legal advice.

8. Notification, signage and awareness

Adequate signage will be placed at each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation. Adequate signage will also be prominently displayed at the entrance to the school. Signage shall include the name and contact details of the data controller as well as the specific

purpose(s) for which the CCTV camera is in place in each location. A template for the signage is set out 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 [*the named 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 [*name of commercial security company where used/ school]*

For more information contact [*insert school contact details*]

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

9. Storage & Retention

The Data Protection Act 2018 states that data "shall not be kept for longer than is necessary for" the purposes for which it was obtained. The CCTV security system should not retain general footage beyond 28 days, except where the images identify an issue – such as a break in or theft and those particular images/recordings are retained specifically in the context of an investigation/ prosecution of that issue.

The images/recordings will be stored in a secure environment with a log of access maintained that will show who accessed the system at what time and for what purpose. Access will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the school's Headteacher, who may delegate the administration of the CCTV System to another staff member.

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.

10. Access

Unauthorised access to live feeds, equipment used to store images and any additional equipment that is used to support the system will not be permitted at any time. Such areas will be appropriately secured when not in use by authorised personnel. A log of access to tapes/images will be maintained.

CCTV footage may be accessed for the purposes in paragraph 2 of this Policy:

- By the police where The Partnership Trust, its schools (or its agents) are required by law to make a report regarding the commission of a suspected crime; or
- 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 property of The Partnership Trust or the schools within it, or
- To the HSE and/or any other statutory body charged with child safeguarding; or
- To assist the CEO of The Partnership Trust or school's Headteacher in establishing facts in cases of unacceptable student behaviour, in which case, the parents/guardians will be informed; or
- To data subjects (or their legal representatives) in response to a Subject Access Request
- To individuals (or their legal representatives) subject to a court order.
- To the school's insurance company where the insurance company requires same in order to pursue a claim for damage done 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) Where the image/recording identifies another individual, those images may only be released where they can be redacted/anonymised or with the explicit consent of the other people identifiable in the footage. The School's SAR Guidance contained within The Partnership Trust Data Protection Policy should be referred to if such a request is made.

A person should provide all the necessary information to assist The Partnership Trust and schools within it in locating the CCTV recorded data, such as the date, time and location of the recording. If the image is of such poor quality as not to clearly identify an individual, that image may be considered to be not personal data and there is no obligation for the image to be handed over by the school.

In giving a person a copy of their data, the school may provide a still/series of still pictures, a tape or a disk with relevant images. However, other images of other individuals must be obscured before the data is released unless they have provided explicit consent for its disclosure.

11. Responsibilities

The individual school's Headteacher will:

- In collaboration with the CEO and DPO keep this policy up to date reflecting any changes to National Guidance, best practice or statutory instruments that determine the use of CCTVE or personal data.
- Ensure that the use of CCTV systems is implemented and controlled in accordance with the policy set down by the Partnership Trust
- Complete a Data Protection Impact Assessment (DPIA) for any CCTV system/s and carry out a review of the DPIA/s on an annual basis
- Be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy.
- Ensure that monitoring recorded tapes are not duplicated for release
- Ensure that the field of view of cameras conforms to this policy both internally and externally
- Approve the location of temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events. *NOTE: [Temporary cameras do not include mobile video equipment or hidden surveillance cameras used for authorised criminal investigations by the Police].*
- Give consideration to both students and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment
- Co-operate with the School's Headteacher and The Trust Executive in reporting on the CCTV system in operation in the school
- Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy"
- Ensure that monitoring tapes are stored in a secure place with access by authorised personnel only
- Ensure that images recorded on tapes/DVDs/digital recordings are stored for a period not longer than 28 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by the CEO in consultation with the Chair of the LGB.
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas
- Ensure that where the Police request to set up mobile video equipment for criminal investigations, legal advice has been obtained and such activities have the approval of the CEO.

SECURITY COMPANIES

Where the school's CCTV system is controlled by a security company contracted by the school
The following applies:

The school has a written contract with the security company in place, specifying the School as the Data Controller and the contractor as the Data Processor with the meaning stated in Article 4(7) and (8) of the GDPR. Specific clauses within the contract detail the areas to be monitored, how long the data is to be stored, what the security company may do with the data, what security standards should be in place and what verification procedures apply. The written contract also states that the security company will give the school all reasonable assistance with the compilation of the DPIA and any necessary support in responding to the Data Subject's exercise of their rights including a SAR.

12. Implementation & Review

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 is approved by the Board of Trustees.

APPENDIX 1 – DEFINITIONS

Definitions of words/phrases used in relation to the protection of personal data and referred to in the text of the policy;

- **CCTV –** Closed-circuit television is the use of video cameras to transmit a signal to a specific place on a limited set of monitors. The images may then be recorded on video tape or DVD or other digital recording mechanism.
- **The Data Protection Act** – The Data Protection Acts 2018 rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All school staff must comply with the provisions of the Data Protection Act when collecting and storing personal information. This applies to personal information relating both to employees of the organisation and individuals who interact with the organisation
- **Data** - information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system).
- **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 Act 2018.
- **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 Subject** – an individual who is the subject of personal data.
- **Data Controller** - a person who (either alone or with others) controls the contents and determines the use of personal data.
- **Data Processor** - a person who processes personal information on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of their employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Data Protection Act 2018place responsibilities on such entities in relation to their processing of the data.

APPENDIX 2 - DATA PROTECTION IMPACT ASSESSMENT(DPIA)

It is a statutory requirement that any activity involving a high risk to the data protection rights of the individual when processing personal data be assessed by the Data Protection Impact Assessment (DPIA). Prior to the assumption of any such activity The Partnership Trust (including the schools within it) will consult with its Data Protection Officer at One West assess risks based on an initial screening process. The DPIA will:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

Upon completion of a DPIA the regulator (ICO) maintains the right to cease the proposed processing should it remain high risk.

Before a school installs a new CCTV system, a documented privacy impact assessment must be carried out. A school which properly conducts such an assessment is less likely to introduce a system that contravenes the provisions of the Data Protection Act 2018. This is an important procedure to adopt as a contravention may result in action being taking against a school by the ICO, or may expose a school to a claim for damages from a student.

Some of the points that might be included in a Data Protection Impact Assessment are:

- What is the school's purpose for using CCTV images and what issues is it meant to address?
- Is it intended that CCTV cameras will operate both inside and outside of the building and is that justified
- Is it justified and proportionate to the problem it is designed to deal with?
- Have you sought and taken into account the views of staff, parents, Governors and the Trust, including regarding the location of camera?
- Can CCTV systems realistically deliver the aims? Can less privacy-intrusive solutions, such as improved lighting, achieve the same objectives?
- Does the school need images of identifiable individuals, or could the system use other images which are not capable of identifying the individual?
- Is the system future proofed? Where a management company is in place, is the school satisfied that it complies with the Data Protection Act with regard to the processing of images of staff, students and visitors to your school captured on any CCTV systems under its management?
- Can the location of each internal camera be justified in accordance with the overall purpose for the use of the CCTV system?
- What security measures are in place to protect the CCTV system and recordings/images and is there a procedure in place to ensure that recordings/images are erased or deleted as soon as the retention period (28 days) has expired?
- Is the room(s) which houses the camera monitors and the CCTV system securely locked when unattended and who has access to the recordings?
- Does the school have a procedure in place to handle access requests seeking a copy of images recorded by the CCTV system (within the statutory timeframe of forty days)?

- Has the school communicated its policy on the use of CCTV (including rights of access) to staff, students and visitors and how has this been done? How are new students and new staff informed of the school's policy on the use of CCTV?

APPENDIX 3 – DETAILS OF SCHOOLS WITHIN THE PARTNERSHIP TRUST WHO HAVE CCTV ON THEIR SCHOOL SITE

Abbot Alphege Academy Beckford Drive Lansdown Bath BA1 9AU	Telephone: (01225) 580 281 Email: office@abbot-alphege.org.uk	The CCTV at this school is recording
Cameley CofE Primary School Meadway, Temple Cloud Bristol BS30 5BD	Tel: 01761 452644 office@cameleyprimary.org.uk	The CCTV at this school is non-recording
Fosse Way School Longfellow Road Midsomer Norton Radstock BA3 3AL	01761 412198 office@fossewayschool.com	The CCTV at this school is non recording
Hayesdown First School Wyville Road Frome Somerset BA11 2BN	01373 462718 office@hayesdownschool.com	The CCTV at this school is recording
The Mendip School Edmund Rack Road Prestleigh, Shepton Mallet Somerset BA4 4FZ	01749 838040 office@themendipschool.com	The CCTV at this school is recording
Roundhill Primary School, Mount Rd, Bath BA2 1LG	01225 424950 office@roundhill-pri.co.uk	The CCTV at this school is recording
Nunney First School Catch Road Nunney, Frome Somerset BA11 4NE	01373 836429 office@nunneyschool.com	The CCTV at this school is recording