PDET

# CCTV Policy

| Date | Revision & Amendment Details | By Whom |
|---|---|---|
| April 2024 | First Edition | Central Executive Team |
| | | |

# CONTENTS


| | | | |
|---|---|---|---|
| 1 | | Aims | 3 |
| | 1.1 | Statement of Intent | 3 |
| 2 | | Relevant Legislation and Guidance | 3 |
| | 2.1 | Legislation | 3 |
| | 2.2 | Guidance | 4 |
| 3 | | Definitions | 4 |
| 4 | | Covert Surveillance | 4 |
| 5 | | Location of the Cameras | 4 |
| 6 | | Roles and Responsibilities | 5 |
| | 6.1 | The Board of Directors (the Board) | 5 |
| | 6.2 | The Trust Central Team (Central Team) | 5 |
| | 6.3 | The Headteacher | 5 |
| | 6.4 | The Data Protection Officer (the DPO) | 5 |
| 7 | | Operation of the CCTV System | 6 |
| 8 | | Storage of CCTV Footage | 6 |
| 9 | | Access to CCTV Footage | 6 |
| | 9.1 | Staff Access | 6 |
| | 9.2 | Subject Access Request (SAR) | 7 |
| | 9.3 | Third-Party Access | 7 |
| 10 | | Data Protection Impact Assessment (DPIA) | 8 |
| 11 | | Security | 8 |
| 12 | | Complaints | 8 |
| 13 | | Monitoring | 9 |
| 14 | | Links to Other Policies | 9 |

Appendix 1 – CCTV log 10

## 1. Aims

This policy aims to set out Peterborough Diocese Education Trust's (the Trust) approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems on school property.

### 1.1 Statement of Intent

The purpose of the CCTV system is to:

- Make members of the school community feel safe
- Protect members of the school community from harm to themselves or to their property
- Deter criminality in the school
- Protect school assets and buildings
- Assist police to deter and detect crime
- Determine the cause of accidents
- Assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings
- To assist in the defense of any litigation proceedings.

The CCTV system will not be used to:

- Encroach on an individual's right to privacy
- Monitor people in spaces where they have a heightened expectation of privacy (including toilets and changing rooms)
- Follow particular individuals, unless there is an ongoing emergency incident occurring
- Pursue any other purposes than the ones stated above.

The list of uses of CCTV is not exhaustive and other purposes may be or become relevant.

The CCTV systems are registered with the Information Commissioner by the Trust under the terms of the Data Protection Act 2018. The systems comply with the requirements of the Data Protection Act 2018 and UK GDPR.

Footage or any information gleaned through the CCTV system will never be used for commercial purposes.

In the unlikely event that the police request that CCTV footage be released to the media, the request will only be complied with when written authority has been provided by the police, and only to assist in the investigation of a specific crime.

The footage generated by the system should be of good enough quality to be of use to the police or the court in identifying suspects.

## 2. Relevant Legislation and Guidance

This policy is based on:

### 2.1 Legislation

- UK General Data Protection Regulation
- Data Protection Act 2018
- Human Rights Act 1998

- European Convention on Human Rights
- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010

### 2.2 Guidance

- Surveillance Camera Code of Practice (2021)

## 3. Definitions

**Surveillance:** the act of watching a person or a place.

**CCTV:** closed circuit television; video cameras used for surveillance.

**Covert surveillance**: operation of cameras in a place where people have not been made aware they are under surveillance.

## 4. Covert Surveillance

Covert surveillance will only be used in extreme circumstances, such as where there is suspicion of a criminal offence. If the situation arises where covert surveillance is needed (such as following police advice for the prevention or detection of crime or where there is a risk to public safety), a data protection impact assessment will be completed in order to comply with data protection law.

Additionally, the proper authorisation forms from the Home Office will be completed and retained where necessary.

## 5. Location of the Cameras

Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system (stated in section 1.1).

Cameras are located in:

***Freeman's:***

- 1 external camera overlooking the Westfield Road gate.
- 1 external camera overlooking the Brickhill Road gate.
- 1 internal camera overlooking the reception area.

***St Barnabas:***

- 2 external cameras overlooking the staff car park.
- 2 external cameras overlooking the playground.
- 1 external camera overlooking the area between the fence and the school.
- 1 external camera overlooking the EYFS playground.

- 1 external overlooking the EYFS outdoor area.
- 1 internal camera overlooking the reception area.

Wherever cameras are installed appropriate signage is in place to warn members of the school community that they are under surveillance. The signage:

- Identifies the Trust as the operator of the CCTV system
- Identifies the Trust as the data controller
- Provides contact details for the school.

Cameras are not and will not be aimed off school grounds into public spaces or people's private property.

Cameras are positioned in order to maximise coverage, but there is no guarantee that all incidents will be captured on camera.

## 6. Roles and Responsibilities

### 6.1 The Board of Directors (the Board)

The Board is ultimately accountable, with responsibilities delegated as set out below, for ensuring the CCTV systems are operated within the parameters of this policy and that the relevant legislation (defined in section 2.1) is complied with.

### 6.2 The Trust's Central Team (Central Team)

The Central Team will:

- Liaise with the data protection officer (DPO) to ensure that the use of the CCTV systems is in accordance with the stated aims and that their use is needed and justified
- Review the CCTV policy to check that the Trust is compliant with legislation
- Conduct data protection impact assessments
- Keep accurate records of all data processing activities and make the records public on request
- Inform subjects of how footage of them will be used by the school, what their rights are, and how the school will endeavour to protect their personal information.

### 6.3 The Headteacher

The headteacher will:

- Take responsibility for all day-to-day leadership, management, maintenance and operation of the CCTV system
- Ensure that the guidance set out in this policy is followed by all staff
- Ensure all persons with authorisation to access the CCTV system and footage have received proper training from the DPO in the use of the system and in data protection
- Sign off on any expansion or upgrading to the CCTV system, after having taken advice from the DPO and taken into account the result of a data protection impact assessment
- Decide, in consultation with the DPO, whether to comply with disclosure of footage requests from third parties
- Ensure footage is destroyed when it falls out of the retention period
- Ensure that the CCTV system is not infringing on any individual's reasonable right to privacy in public spaces
- Ensure records are kept with clear justifications to view CCTV using the Trust CCTV log

- Oversee the security of the CCTV system and footage
- Regularly check for and report any faults and security flaws.

### 6.4 The Data Protection Officer (DPO)

The DPO will:

- Oversee training of persons with authorisation to access the CCTV systems and footage in the use of the systems and in data protection
- Oversee training of all staff to recognise a subject access request
- Deal with subject access requests in line with the Freedom of Information Act (2000)
- Monitor compliance with UK data protection law
- Advise on and assist the Trust with carrying out data protection impact assessments
- Act as a point of contact for communications from the Information Commissioner's Office
- Ensure data is handled in accordance with data protection legislation
- Ensure footage is obtained in a legal, fair and transparent manner
- Receive and consider requests for third-party access to CCTV footage.

## 7. Operation of the CCTV System

The CCTV system will be operational 24 hours a day, 365 days a year.

The system is registered with the Information Commissioner's Office.

The system will not record audio.

Recordings will have date and time stamps.

## 8. Storage of CCTV Footage

Footage will be retained for 30 days. At the end of the retention period, the files will be overwritten automatically.

On occasion footage may be retained for longer than 30 days, for example where a law enforcement body is investigating a crime, to give them the opportunity to view the images as part of an active investigation. Where this is the case, it will be recorded on the CCTV access log.

Recordings will be stored so that the data is secure, and its integrity maintained, so that it can be used as evidence if required.

## 9. Access to CCTV Footage

Access will only be given to authorised persons, for the purpose of pursuing the aims stated in section 1.1, or if there is a lawful reason to access the footage.

Any individuals that access the footage must record their name, the date and time, and the reason for access in the access log (see appendix).

Any visual display monitors will be positioned so only authorised personnel will be able to see the footage.

### 9.1 Staff Access

The following members of staff have authorisation to access the CCTV footage ('authorised operators'):

- The headteacher / head of school / executive head
- The deputy head
- The data protection officer
- Anyone with express permission of the headteacher /head of school / executive head.

CCTV footage will only be accessed from authorised staff member's work devices, or from the visual display monitors.

All authorised members of staff who have access will undergo training to ensure proper handling of the system and footage.

Any member of staff who misuses the surveillance system may be committing a criminal offence and will face disciplinary action.

### 9.2 Subject Access Requests (SAR)

According to UK GDPR and Data Protection Act 2018, individuals have the right to request a copy of any CCTV footage of themselves.

Upon receiving any such request the school will acknowledge receipt and will then respond within 30 days during term time. The school reserves the right to extend that deadline if following receipt of a request, the 30 days extends into school holidays.

All staff have received training to recognise SARs. When a SAR is received staff should inform the DPO. When making a request, individuals should provide the school with reasonable information such as the date, time and location the footage was taken to aid school staff in locating the footage.

On occasion the school will reserve the right to refuse a SAR, if, for example, the release of the footage to the subject would prejudice an ongoing investigation.

Images that may identify other individuals need to be obscured to prevent unwarranted identification. The school will attempt to conceal their identities by blurring out their faces, or redacting parts of the footage. If this is not possible the school will seek their consent before releasing the footage. If consent is not forthcoming the still images may be released instead. The school reserves the right to charge a reasonable fee to cover the administrative costs of complying with a SAR that is repetitive, unfounded or excessive.

Footage that is disclosed in a SAR will be disclosed securely to ensure only the intended recipient has access to it.

Records will be kept that show the date of the disclosure, details of who was provided with the information (the name of the person and the organisation they represent), and why they required it. Individuals wishing to make a SAR can find more information about their rights, the process of making a request, and what to do if they are dissatisfied with the response to the request on the ICO website.

### 9.3 Third-Party Access

CCTV footage will only be shared with a third party to further the aims of the CCTV system set out in section 1.1 (e.g. assisting the police in investigating a crime).

Footage will only ever be shared with authorised personnel such as law enforcement agencies or other service providers who reasonably need access to the footage (e.g. investigators).

All requests for access should be set out in writing and sent to the headteacher and the DPO.

The school will comply with any court orders that grant access to the CCTV footage. The school will provide the courts with the footage they need without giving them unrestricted access.

In all cases the DPO will consider very carefully how much footage to disclose and seek legal advice if necessary.

The DPO will ensure that any disclosures that are made are done in compliance with UK GDPR.
All disclosures will be recorded by the DPO.

## 10. Data protection Impact Assessment (DPIA)

The Trust follows the principle of privacy by design. Privacy is taken into account during every stage of the deployment of the CCTV system, including its replacement, development and upgrading.

The CCTV system will only be used only for the purpose of fulfilling its aims (stated in section 1.1).

When the CCTV system is replaced, developed or upgraded a DPIA will be carried out to be sure the aim of the system is still justifiable, necessary and proportionate.

The DPO will provide guidance on how to carry out the DPIA. The DPIA will be carried out by the Central Team.

Those whose privacy is most likely to be affected, including the school community and neighbouring residents, will be consulted during the DPIA, and any appropriate safeguards will be put in place.

A new DPIA / review of the DPIA will be done whenever cameras are moved to a different location, or new cameras are installed.

If any security risks are identified in the course of the DPIA, the school will address them as soon as possible.

## 11. Security

- The Headteacher will be responsible for overseeing the security of the CCTV system and footage
- The Headteacher will arrange for the system to be checked for faults on a regular basis
- Any faults in the system will be reported to the system provider as soon as they are detected and repaired as soon as possible, according to the proper procedure
- Footage will be stored securely and encrypted wherever possible
- The CCTV footage will be password protected and any camera operation equipment will be securely locked away when not in use
- Cyber security measures will be put in place to protect the footage from cyber-attacks where possible

- Any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied, will be applied as soon as possible.

## 12. Complaints

Any complaints should be directed to the headteacher / head of school / principal / executive head and should be made according to the Trust's complaints policy.

## 13. Monitoring

This document will be reviewed periodically but may be reviewed and updated more frequently if necessary.

## 14. Links to Other Policies

- Data Protection policy
- Privacy notices for parents, pupils, staff, volunteers and visitors.
- Safeguarding policy.

# Appendix 1 - CCTV Log

## Record of Requests to View CCTV

| Date and time of request | Person requesting | Reason for request / viewing | Action taken (include name of persons viewing if applicable - should be 2 people) | Was the recording taken off site? If so, where and why? | Notes |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |