CCTV Policy

Policy Group:	**Admin & Data**
Policy Ref:	**ADD/02**
Responsible Reviewing Officer and Job Title:	**Mike Jones Head of Facilities**
Date Written:	**January 2026**
Date Approved by the Board:	**January 2026**
Date of Next Review:	**January 2028** or earlier in the event of significant change to the system, national guidance, best practice of legislation relating to the capture of images by CCTV.

1. Introduction

a. 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.
b. This document sets out the policy covering the use and management of CCTV equipment and images to ensure that Pickwick Academy Trust (The Trust) complies with the Data Protection Legislation and other relevant legislation. Crucially personal data is processed in line with the Trust's Data Protection Policy and the use of such equipment is cognisant of the Guiding Principles of the Surveillance Camera Code of Practice updated and published by the Home Office in 2021.
c. The Trust uses CCTV for the purposes of the prevention and detection of crime, keeping safe the children, staff and visitors alike and to recognise and identify individuals with a view to taking appropriate action where necessary.
d. This policy and related procedures apply to all schools within the Pickwick family

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/organisation 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 – is covert surveillance in places other than residential premises or private vehicles.
Personal Data – is data that relates 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 - is where a person makes a request to the organisation for the disclosure of their personal data under data protection law.

3. Purpose and Scope

a. 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 premises under the remit of Pickwick Academy Trust.
b. 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 Trust's CCTV processes and helps protect the rights of data subjects
c. CCTV at any Trust property 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.

d. Any decision to use CCTV to monitor staff for time management would be preceded by a consultation process.
e. This policy will be published on the Trust's website with a link provided to schools for their website and the existence of this policy and any subsequent changes to the policy will be notified to pupils, parents, staff and volunteers.
f. 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.

4. Responsibilities and Accountabilities

a. The Trust CEO is responsible for broadcasting the policy and its requirements and the Trust Executive Team/Headteachers and Heads of School are responsible for ensuring that the policy is adhered to. This will include familiarisation of all staff including those with specific roles associated with CCTV within their responsibilities. It will also include the establishment of arrangements for conducting annual reviews and obtaining their findings/remedial actions.
b. School Facilities Managers/ Site Managers are responsible for the day-to-day operation of the CCTV. Their contact details are presented on external signage displayed where CCTV cameras are used, as indicated in Appendix 1.
c. The introduction of, or changes to, CCTV monitoring across any Trust site is agreed in advance by the CFOO of the Trust and is subject to a Data Protection Impact Assessment (DPIA).

d. The CFOO of the Trust is 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
e. 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 the Chief Finance and Operating Officer in consultation with the DPO.

f. The Trust will not contract out the operation of their CCTV.
g. The Data Protection Officer (DPO) for Pickwick Academy Trust is One West who can be contacted at: i-west@bathnes.gov.uk

5. Principles of Use

a The use of a CCTV system by Pickwick Academy Trust 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 consider 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

a. The 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, there is a duty of care under the Health and Safety at Work etc. Act 1974 and associated legislation. Hence the use of CCTV and associated monitoring and recording equipment is an additional mode of security and surveillance for each of these purposes. CCTV systems are installed internally and externally and will operate constantly.
b. 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 Trust including its Equality & Diversity Policy and codes of practice for dealing with complaints of bullying & harassment and sexual harassment.
c. Importantly CCTV will not be used to monitor normal staff activity on site.
d. 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 Trust’s grounds 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.
e. In other areas where CCTV has been installed, the 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.
f. 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.
g. 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

a. At each site throughout the Trust, the Headteacher is accountable for operation of the CCTV on their site and responsible for:
   - 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.
   - Ensuring that a Data Protection Impact Assessment (DPIA) is in place 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, staff and members of the public.

b. The CFOO is the overall CCTV Data Controller for the Trust

8. Location of the Cameras

a. The planning and design process has set out to ensure that the system will give maximum effectiveness and efficiency, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage. The Trust has endeavoured to select locations for the installation of CCTV cameras to achieve its aim/s, 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.

b. Cameras will be sited so they only capture images relevant to the purposes for which they are installed, and care will be taken to ensure that reasonable privacy expectations are not violated. The Trust will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

c. The Trust will make every effort to position cameras so that their coverage is restricted to the Trust premises, which may include outdoor areas. The following locations may be covered by CCTV:

- The building's perimeter, entrances and exits, lobbies and corridors, special storage areas, 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 verification of 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.

d. CCTV will not in general be used in classrooms but in areas within schools that have been identified by staff as not being easily monitored (they can be installed in classrooms but only if there is justification for doing so).
e. Members of staff should have access to details of where CCTV cameras are situated, except for cameras placed for covert monitoring as detailed in Section 9.

9. Covert Surveillance

a. The Trust will not engage in covert surveillance using CCTV except in the circumstances explained below. 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 in writing to the CFOO and the school may seek legal advice. In the case of urgency this request may be verbally approved if the circumstances dictate, the investigation of serious crime.
The Trust may in exceptional circumstances set up covert monitoring. For example:

- Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;
- Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

b. In these circumstances, authorisation must be obtained in advance from the Trust CEO/CFOO and Data Protection Officer.
c. Covert monitoring must cease following completion of an investigation.
d. Cameras sited for covert monitoring will not be used in areas which are reasonably expected to be private, for example toilet cubicles or changing rooms.

10. Data gathering & storage, and retention

a. The CCTV systems will vary at the different school sites within the organisation and will comprise 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 not normally monitored. Where an incident does occur video footage may be referred to as part of an investigation.
b. 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 who may delegate this responsibility to the Site Manager or SBM, whichever is appropriate.
c. 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 and approved by the CFOO.
d. Importantly, data processed by the CCTV shall not be kept for longer than is necessary for' the purposes for which it was obtained. The 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. All retained data will be stored securely.

e. 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 Trust's CCTV system
f. 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.

11. Subject Access Requests (SAR)

a. Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act 2018 and General Data Protection Regulation (GDPR) using a Subject Access Request Form.
b. All Subject Access Requests should be directed to the Trust Data Protection Officer in the first instance. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.
c. The Trust will respond to requests within one calendar month of receiving the written request.
d. The Trust reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

12. Access to and Disclosure of Images to Third Parties

a. There will be no disclosure of recorded data to third parties' other than to authorised personnel such as the Police and service providers to the Trust where these would reasonably need access to the data (e.g. investigators).
b. Requests should be made in writing to the Trust Data Protection Officer and CEO/CFOO
c. The data may be viewed and used as part of an investigation where it is necessary to use it within the Trust's discipline and grievance procedures and will be subject to the usual confidentiality requirements of those procedures.

13. Access to data (Video Footage)

a. Unauthorised access to live feeds, equipment used to store images and any additional equipment that is used to operate the CCTV systems within Pickwick Academy Trust is prohibited. A log of access to the CCTV system and its components and images / video footage is to be maintained.
b. Access to the CCTV system and video footage may be granted by Pickwick Academy Trust for the following reasons:

- Where Pickwick Academy 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 Pickwick Academy Trust 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.

c. 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.

13.Complaints

a. Complaints and enquiries about the operation of CCTV within the Trust should be directed to the Headteacher in the first instance.

14. Equal Opportunities

a. An Equality and Diversity Impact Assessment has been completed in order to ensure it complies with equality obligations outlined in discrimination legislation. The policy positively reflects the aims and ambitions of Pickwick Academy Trust.

Appendix 1 – CCTV Signage

It is a requirement of the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The school and the Trust are to ensure that this requirement is fulfilled.

The CCTV sign should include the following:

- Inside the School building:

- Outside the School Building: