



Slough and East Berkshire
C of E Multi Academy Trust

CCTV Policy

Owner:	Board of Directors/Trustees
Ratified by:	SEBMAT Directors
Date Ratified:	6 July 2026
Date Policy to be reviewed:	July 2027

SEBMAT is committed to compliance with the Data Protection Act (2018) and the Data Use and Access Act (2025). This policy sets out how we handle the personal data of our pupils, employees, parents and third parties and the precautions we take in order to protect this data. All employees are required to familiarize themselves with the content of this policy and adhere to the provisions set out in it. Failure to comply with this policy is considered an offence which may result in disciplinary action, according to the Trusts disciplinary policy.

Data Protection Regulations Act (2018)

The Data Protection Act 2018 controls how personal information is used by organisations, businesses and government. The EU GDPR has been incorporated into the UK data protection law as the UK GDPR. This act clarifies the data protection principles, rights and obligations.

Key Definitions

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data subject – any living individual who is the subject of personal data held by an organisation.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the rights and freedoms of the data subject

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child - Although, in the UK a child is considered to be anyone aged under 18, if you are relying on consent as your lawful basis for processing, in the UK the child may provide their own consent when they are aged 13 or over. If the child is under 13, any consent required will need to be obtained from the parent or custodian.

Third party – a natural or legal person, public authority, agency or body other than the data subject,

controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Data Protection Impact Assessment (DPIAs) – DPIA's are a tool used to identify risks in data processing activities with a view to reducing them.

The **DATA MANAGER** is responsible for the maintenance of this register and this will be reviewed on a regular basis by the Data Protection Officer (DPO).

SEBMAT adheres to the key principles of GDPR when processing personal data, as detailed below.

1. Personal data must be processed lawfully, fairly and in a transparent manner;
2. Personal data must be collected only for specified, explicit and legitimate purposes;
3. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
4. Personal data must be accurate and, where necessary, kept up to date;
5. Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed; and
6. Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

In order to achieve this SEBMAT has implemented the following Closed Circuit Television (CCTV) Policy which must be adhered to at all times.

Roles and responsibilities

This policy applies to all staff employed by the Trusts Schools, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Directors/Governing Body

Ensure school's policies and procedures are compliant with all relevant data protection obligations and that Data Protection is a standing agenda item at board meetings

Data Protection Officer (DPO)

The Data Protection Officer is Jo Holloway (AzteQ) who is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. She will provide an annual report on activities and, where relevant, report advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Chris Fisher is the Data Protection Liaison for the Trust.

If employees have any questions about the operation of this policy, the GDPR or any concerns about the protection of data within the organisation, please contact the DPO –

DPO: AzteQ Group Ltd

Address: First Floor, Italy House, 16 Warwick Road, Beaconsfield, Bucks, HP9 2PE

Telephone: 01442 244444

Email: SEBMAT-DPO@torix.co.uk

In the event of a data breach/suspected data breach; employees should contact the DATA MANAGER **immediately, who will liaise with the DPO.**

Closed Circuit Television (CCTV) Policy

This policy will be reviewed annually.

Date of next review: Spring 2027

Introduction

Closed Circuit Television (CCTV) systems are installed and operated across all schools in the Trust by IT Support, with the aim to help protect staff, students, visitors and property on the school sites.

The CCTV system will be regularly maintained and improved to ensure a wide coverage of the school to ensure that if an incident were to arise sufficient CCTV footage would be available to lead to a positive outcome.

The CCTV Policy will be available to all staff, students, parents and visitors to the various sites via the school's website and intranet. This policy describes the purpose and location of CCTV monitoring, a contact number for those wishing to discuss CCTV monitoring and guidelines for its use.

A Data Protection Impact Assessment has been carried out on the usage of CTV across the Trust.

The Lawful basis for processing in this case is Public Task (site security, crime prevention (balanced and proportionate)).

1. Purpose of this policy

CCTV systems are installed (both internally and externally) for the purpose of enhancing security of the building, its occupants and its associated equipment.

CCTV surveillance 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;
- preventing bullying;
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- assisting in identifying, apprehending and prosecuting offenders; and
- ensuring that the school rules are respected so that the school can be properly managed.

2. Scope

This policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material.. Coverages facilitated only to ensure the safety and security of staff and students in environments deemed to be of higher risk to safety or those demanding surveillance for

safeguarding purposes. We will ensure that CCTV systems, where installed, are operated only in a way that is compatible with the provisions of this policy.

3. General principles

SEBMAT, and each school, as established institutions, have a statutory responsibility for the protection of its property and equipment as well providing a sense of security to its employees, students and visitors to its premises. The Trust owes a duty of care under the provisions of the Health and Safety at Work etc. Act 1974 and associated legislation and utilises CCTV systems and their associated monitoring and recording equipment as an added mode of security and surveillance for the purpose of enhancing the quality of life of the school community. The operation of the CCTV system will be conducted in a professional, ethical and legal manner and any use of CCTV security technologies for other purposes is prohibited by this policy e.g. CCTV will not be used for monitoring employee performance.

Members of Senior Leadership Team (SLT), pastoral leaders, members of the Safeguarding team, the Estates team, the Lettings Manager and the SEN Department may request, and review information obtained through the CCTV system. Other staff members may be authorised to review information through CCTV after requesting permission from members of SLT. Any request for CCTV recordings must be documented in the CCTV log to show who requested the footage, the nature and approximate time and date of the footage, who recovered the recordings and when they were recovered. (See "Access" below). If a law enforcement authority seeks a recording for a specific investigation, they may require a warrant. Any such request made should be requested in writing and the school may seek legal advice.

Only the SLT and IT Support can recover CCTV recordings.

The Lettings Manager and the Estates team have a limited viewing of the CCTV system. This is limited to cameras that cover: external areas of the site, key internal areas of interest and designated buildings that fall under the responsibility of the employee. IT Support and the SLT will have access to all cameras onsite.

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the school and the provisions set down in equality, educational, and other associated legislation.

This policy prohibits monitoring based on the characteristics and classifications contained in equality and other related legislation e.g. race, gender, sexual orientation, national origin, disability etc.

Video monitoring of public areas for security purposes within the school premises is limited to uses that do not violate the individual's reasonable expectation of privacy.

4. Justification for use of CCTV

The General Data Protection Regulations require that all data collected is "adequate, relevant and not excessive" for the purpose for which it is collected. This means that the school 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 the perimeter of the school buildings for security purposes is a justified reason to help to capture images of intruders or of individuals damaging property or removing goods without authorisation.

CCTV systems will not be used to monitor normal teacher/student classroom activity in school.

In other areas of the school where CCTV has been installed (e.g. hallways, stairwells and communal areas), it has been demonstrated that the installation of CCTV is proportionate in addressing such issues that have posed a risk to security and/or health & safety.

5. Justification of camera locations

The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. The schools have endeavoured to select locations for the installation of CCTV cameras which provide clear images and adequate coverage of the site

while not intruding on the privacy of individuals. Cameras are placed so as to record external/communal areas and are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

CCTV footage may, on occasion, incidentally, capture information that could constitute special category personal data (for example, information revealing racial or ethnic origin, religious beliefs, health or disability) and/or criminal offence data (for example, where footage is used in connection with the prevention, investigation or prosecution of criminal activity). The Trust does not use CCTV to deliberately record or infer such information, and does not use CCTV to make decisions about individuals based on these characteristics. Where special category and/or criminal offence data is captured incidentally, access to the footage will be strictly limited to authorised staff on a need-to-know basis, handled with additional care, and only used and disclosed where it is necessary and proportionate for the purposes set out in this policy (for example, safeguarding, health and safety, or the prevention and detection of crime). Any viewing, export, sharing or retention of such footage will be documented in the CCTV log and retained only for as long as required for the relevant purpose.

CCTV Video Monitoring and Recording of Public Areas at each school may include the following:

- **Protection of school buildings and property:** The buildings' perimeter, entrances and exits, lobbies and corridors, special storage areas, cashier locations, receiving areas for goods/services
- **Protection of Staff, Students and Visitors:** External and internal locations within the school grounds
- **Monitoring of Access Control Systems:** Monitor and record restricted access areas at entrances to buildings and other areas
- **Verification of Security Alarms:** Intrusion alarms, exit door controls, external alarms
- **Video Patrol of Public Areas:** Parking areas, Main entrance/exit gates, traffic Control
- **Criminal Investigations (carried out by the police):** Robbery, burglary and theft surveillance

6. Covert surveillance

No school in the Trust will engage in covert surveillance.

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

7. Notification (Signage)

Adequate signage will be installed at key locations to indicate that CCTV is in operation. Adequate signage will also be prominently displayed at the entrance to the school.

Appropriate locations for signage will include but are not limited to, entrances to the premises (external doors and school gates), reception areas and hallways.

8. Storage and Retention

The General Data Protection Regulations state that data "shall not be kept for longer than is necessary" for the purposes for which it was obtained. The images captured by the CCTV system will be retained for a maximum of 30 days (less in some schools), except where the image identifies an issue and is 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 kept. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis. No physical copies of these recordings will be made unless requested by a law enforcement body.

9. Access requests

To formally request access to personal data captured via our closed-circuit television (CCTV) systems, data subjects must submit a written **Subject Access Request (SAR)** to our Data Protection Office. To facilitate a timely search, the request must specify the exact date, time, and geographical location of the recording. In accordance with statutory requirements, we will provide a formal response within **one calendar month** of receiving a verified request and sufficient identification. Please be advised that where footage contains the personal data of third parties, we are obligated to apply **technical redaction (masking or blurring)** to protect their privacy rights, unless their explicit consent is obtained. Upon completion of the review, the data will be dispatched via a **secure, encrypted electronic transfer** or an equivalent high-security method to ensure the integrity and confidentiality of the personal data throughout the transmission process..

10. Live Feeds

In some areas we use live feeds of CCTV to assist staff and act as a deterrent, these will be for key areas identified as being areas of higher risk where immediate action may be required.

- Premises have live feeds of all cameras for security purposes
- The Business Manager has live feeds of all cameras for security purpose

11. Responsibilities

The schools will:

- Ensure that CCTV systems are operated in accordance with this policy.
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within the school.
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy.
- Ensure that the CCTV monitoring at the school is consistent with the highest standards and protections.
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy.
- Maintain a record of access (e.g. an access log) for the release of any material recorded or stored in the system.
- Ensure that recorded footage is not duplicated for unjustified or unwarranted release.
- 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.
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the school and be mindful that no such infringement should take place.
- Ensure adequate signage at appropriate and prominent locations is displayed as detailed above.
- Ensure that external cameras are not intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy".
- Ensure that recordings are stored in a secure place with access by authorised personnel only.
- Ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy.
- Ensure that camera control is solely to promote safeguarding and security, including monitoring suspicious behaviour, criminal damage etc. and not to monitor individuals.
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas.