



ELTHAM
CHURCH OF ENGLAND
PRIMARY SCHOOL
SINCE 1814

CCTV System Policy and Code Of Practice

Created: January 2019
Reviewed: May 2021
Next review: September 2024



CONTENTS PAGE

Statement of Intent	3
Application	5
Definitions	5
Legal Framework	5
Data Protection Principles	6
Protocols	7
The Role and Responsibilities of the Data Protection Officer	7
The Role of the Headteacher.....	8
Security	8
Captured Imagery Procedures	9
Access.....	11
Breaches of the Code (including breaches of security)	13
Assessment of the Policy	13
Complaints	13
Monitoring and Review	13
Public Information	13
Appendix A- CCTV Locations	14
Appendix B- CCTV Checklist	14
Appendix C- CCTV signage	16

Statement of Intent

Our Policy

We, Eltham C of E Primary School (hereinafter referred to as the “**School**”), believe that Closed Circuit Television (“**CCTV**”) and other surveillance systems have a legitimate role to play in helping to maintain a safe and secure environment for all our staff, students and visitors. However, we recognise that this may raise concerns about the effect on individuals and their privacy and as such this CCTV System Policy and Code of Practice (“**Policy**”) is intended to address such concerns.

Purpose

At Eltham C of E Primary School, we take our responsibility towards the safety of staff, students and visitors very seriously. To that end, we use CCTV (installed at the School premises) to:

- Monitor any instances of aggression or physical damage to our School and its members.
- Deter violent behaviour and damage to the School.
- Increase personal safety of staff, students and visitors alike.
- Reduce the fear of crime within the School.
- Protect the School premises and any School assets.
- Support the Police in a bid to deter and detect crime in order to reduce crime.
- Assist in the identifying and apprehension of offenders on the School property.
- Offer increased protection to members of the public and private property.
- Assist in managing the School and its day-to-day running plans and goals.

At our school, 14 cameras are located at various places on the School premises. Images from the cameras are recorded and stored onto a hard drive located within the School Business Manager's office. All imagery is only available to selected senior School staff, as directed by the Headteacher and the School Business Manager.

The purpose of this Policy is to manage and regulate the use of surveillance and CCTV systems at our School and ensure that:

- We comply with the requirements of the General Data Protection Regulation (“**GDPR**”), effective as of 25 May 2018.
- The images, all information and recordings that are captured are useable as data for the purposes we require them for and/or which are protected by the GDPR.
- We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

Cameras will be used to monitor activities within the School grounds, its car park, in the vicinity of the access gates and other public areas to:

- Observe what an individual is doing.
- Identify aggressive/criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of the School's students and staff, together with its visitors.
- Taking action to prevent a crime.

Restrictions

Unless an immediate response to events is required, staff must not direct cameras at an individual or a specific group of individuals, private property and/or homes, gardens and other areas of private property, without authorisation being obtained using the School's forms for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000.

Under no circumstances will the surveillance and the CCTV cameras be present in any changing facility within the School.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Recordings will never be released to the media for purposes of entertainment.

Effectiveness of our systems

The planning and design has endeavoured to ensure that the surveillance and CCTV 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.

Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at all access routes to areas covered by the School CCTV.

Ownership

The School owns the surveillance and/or CCTV system and all disks containing images.

The surveillance and/or CCTV system will be strictly controlled and monitored by authorised personnel only.

Key individuals

AGAS Data Protection Officer is the ("DPO").

Mr Matthew Willis is the Headteacher.

Application

This Policy covers all employees, workers, contractors, agency workers, consultants, directors, members, governors, past or present students and may also be relevant to visiting members of the public. This Policy is non-contractual and does not form part of the terms and conditions of any employment or other contract.

Signed: Date:

Definitions

For the purpose of this Policy and the GDPR, the following terms have the following meanings:

- **CCTV:** means fixed and domed cameras designed to capture and record images of individuals and property.
- **Data:** is information that is stored electronically or in certain paper-based filing systems and may include Personal Data. In respect of CCTV, this generally means video images. It may also include static pictures such as printed screen shots.
- **Data Controllers:** means the person or organisation that determines when, why and how to process Personal Data. We (the School) are the Data Controller of all Personal Data used for our own commercial and educational purposes.
- **Data Processors:** means the person or organisation that is not a Data User that processes Personal Data on our behalf and in accordance with our instructions (for example, a supplier which handles Personal Data on our behalf).
- **Data Users:** are those of our employees whose work involves processing Personal Data. This will include those whose duties are to operate CCTV cameras and other surveillance systems to record, monitor, store, retrieve and delete images. Data users must protect the data they handle in accordance with this Policy and the School's Data Protection Policy.
- **Data Subjects:** means a living, identified or identifiable individual about whom we hold Personal Data as a result of the operation of our CCTV (or other surveillance systems).
- **Personal Data:** means any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This will include video images of Data Subjects.

Legal Framework

Applicable legislation

This Policy (and the use of CCTV) has and will continue to have due regard to legislation in the United Kingdom including, but not limited to, the following:

- The Children Act 1989.

- The Children Act 2004.
- The School Standards and Framework Act 1998.
- The Freedom of information Act 2000 (“**FOA**”).
- The Regulation of Investigatory Powers Act 2000.
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004.
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016).
- The Equality Act 2010.
- The Protection of Freedoms Act 2012.
- The General Data Protection Regulation 2018.

Applicable statutory/non-statutory guidance notes

This Policy has been created with regard to the following statutory and/or non-statutory guidance notes:

- Home Office (2013) The Surveillance Camera Code of Practice - <https://www.gov.uk/government/publications/surveillance-camera-code-of-practice>
- **ICO** (2017) Overview of the General Data Protection Regulation (GDPR) - <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-dataprotection-regulation-gdpr/>
- ICO (2017) Guide to the General Data Protection Regulation - <https://ico.org.uk/media/fororganisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf>
- ICO (2017) In the picture: A data protection code of practice for surveillance cameras and personal information - <https://ico.org.uk/media/1542/cctv-code-of-practice.pdf>

Other School policies

This Policy operates in conjunction with the following School policies:

- Data Protection Policy
- Management and Retention of Data Policy

Data Protection Principles

What the School will do to comply with legislation

The School is the data Controller. In order to comply with the requirements of the applicable legislations (listed above), the School as the Data Controller will ensure that Data from CCTV footage will be:

- Legally and fairly processed in a transparent manner.

- Collected for specified, explicit and legitimate purposes and ensuring that it is used accordingly.
- Processed for limited purposes and not in any manner incompatible with those purposes.
- Stored for longer periods, in so far as such Data is processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (subject to implementation of the technical and organisational measures required under the GDPR).
- Adequate, relevant and not excessive in relation to the reason for its collection.
- Not kept for longer than is necessary and will be erased and rectified without delay (having due regard to the purpose for which such Data was processed).
- Processed in accordance with individuals' rights.
- Accurate and, where necessary, kept up-to-date.
- Secure (by way of protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

Protocols

The surveillance and/or CCTV system will be registered with the Information Commissioner's Office ("ICO") in line with data protection legislation.

The surveillance and/or CCTV system is a closed digital system.

Warning signs have been placed throughout the School premises where the surveillance and/or CCTV system is active, as mandated by the ICO's Code of Practice.

The surveillance and/or CCTV system has been designed for maximum effectiveness and efficiency as much as can be afforded from a school budget; however, the School cannot guarantee that every incident will be detected or covered and 'blind spots' may exist. There may be further investment in the future to cover more surveillance and/or CCTV of the school.

The surveillance and/or CCTV system will not be trained on individuals unless an immediate response to an incident is required.

The surveillance and/or CCTV system will not be trained on private vehicles or property outside the perimeter of the School.

The Role of the Data Protection Officer

The DPO is crucial and their key duties will include the following:

- Dealing with freedom of information requests and subject access requests in line with the GDPR, including the FOA.
- Ensuring that all Data Controllers at the School handle and process surveillance and CCTV footage in accordance with the GDPR.
- Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
- Ensuring consent is clear, positive and unambiguous.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Keeping a comprehensive and accurate record of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity and making these records public upon request.
- Informing Data Subjects of how their data captured in surveillance and CCTV footage will be used by the School, their rights for the data to be destroyed and the measures implemented by the School to protect individuals' personal information.
- Preparing reports and management information on the School's level of risk related to data protection and processing performance.
- Reporting to the highest management level of the School, e.g. the governing board.
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role.

The role of the Headteacher

The role of the Headteacher includes:

- Meeting with the DPO to decide where CCTV is needed to justify its means.
- Conferring with the DPO with regard to the lawful processing of the surveillance and CCTV footage.
- Reviewing the CCTV System Policy and Code of Practice to ensure it is compliant with current legislation.
- Monitoring legislation to ensure the School is using surveillance fairly and lawfully.
- Communicating any changes to legislation with all members of staff.

Security

Operation of the system

The surveillance and/or CCTV system will be administered and managed by the School Business Manager, in accordance with the principles and objectives expressed in the code.

The day-to-day management of the surveillance and/or CCTV system will be the responsibility of both the leadership team and the School Business Manager.

The surveillance and/or CCTV system will only be operated and monitored by approved staff as directed by the Headteacher and the School Business Manager.

The CCTV system will be operated 24 hours each day, every day of the year, typically by motion detection.

Control units

The School Business Manager will check and confirm the efficiency of the surveillance and/or CCTV system daily and in particular that the equipment is properly recording and that cameras are functional.

Access to the CCTV control Units will be strictly limited to those staff as approved by the Headteacher or the School Business Manager.

Visitors and other contractors wishing to view the control units will be subject to particular arrangement as outlined below:

- Control unit operators must satisfy themselves over the identity of any other visitors wishing to view the control cabinet and the purpose of the visit.
- Where any doubt exists, access will be refused.
- Details of all visits and visitors will be endorsed in the control unit file.
- The surveillance and/or CCTV system may generate a certain amount of interest. It is vital that operations are managed with the minimum of disruption. Casual visits will not be permitted.
- Visitors must first obtain permission from the Headteacher or School Business Manager and must be accompanied throughout the visit.
- Any visit may be immediately curtailed if prevailing operational requirements make this necessary.
- If out of hours emergency maintenance arises, the control unit operators must be satisfied of the identity and purpose of contractors before allowing entry.
- A visitor's log will be maintained in the School Business Manager's office in the control unit file. Full details of visitors including time/data of entry and exit will be recorded.
- The control units are located in the main office and the Premises Officer's office, which are only accessible to authorised personnel and are locked during out of hours.
- Other administrative functions will include maintaining hard disc space, filing and maintaining occurrence and system maintenance logs.

- Emergency procedures will be used in appropriate cases to call the Emergency Services.

Captured Imagery Procedures

Adherence to data protection legislation

The School understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles. The School will notify all students, staff and visitors of the purpose for collecting CCTV data via notice boards, letters and emails.

Key considerations

The surveillance and/or CCTV system will:

- Be designed to take into account its effect on individuals and their privacy and Personal Data.
- Be transparent and include a contact point, the DPO, through which people can access information and submit complaints.
- Have clear responsibility and accountability procedures for images and information collected, held and used.
- Have defined policies and procedures in place that are communicated throughout the School.
- Restrict access to retained images and information with clear rules on who can gain access. Consider all operational, technical and competency standards, relevant to the surveillance and/or CCTV system and its purpose, and work to meet and maintain those standards in accordance with the law.
- Be subject to stringent security measures to safeguard against unauthorised access.
- Be regularly reviewed and audited to ensure that policies and standards are maintained.
- Only be used for the purposes for which it is intended, including supporting public safety, the protection of pupils, staff and volunteers, and law enforcement.
- Be accurate and well maintained to ensure information is up-to-date

Covert Monitoring

It is not the School's policy to conduct 'Covert Monitoring' unless there are 'exceptional reasons' for doing so. The school may, in exceptional circumstances, determine a sound reason to 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.

The following must be adhered to when initiating covert monitoring:

- In the circumstances above authorisation must be obtained from the Headteacher and advised by the ICO before any commencement of such covert monitoring.
- Covert monitoring must cease following completion of an investigation.
- Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilet cubicles, changing areas etc.
- Storage and Retention of CCTV images, recorded data will not be retained for longer than is necessary.

Retention of imagery/Data

In order to maintain and preserve the integrity of the imagery used to record events from the hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:

- Each CD/DVD will be identified by a unique mark.
- The Data Controller shall register the date and time of the event and date of CD/DVD manufacture.
- Each frame of the captured image shall be watermarked with the date and time of the event/activity.

The CD/DVD required for evidential purposes must be sealed, witnessed, signed by the Headteacher, dated and stored in a separate and secure evidence tape store. This would be in the fire proof, lockable cupboard in the School Office.

- If a CD/DVD is not manufactured for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the Headteacher, dated and returned to the evidence tape store.
- If the CD/DVD is to be archived the reference must be noted.
- Imagery may be viewed by the Police for the prevention and detection of crime, authorised officers of the local County Council for supervisory purposes, authorised demonstration and training.
- A record will be maintained of the release of all CD/DVD imagery given to the Police or other authorised applicants. A register will be available for this purpose.
- Viewing of CD/DVD imagery by the Police must be recorded in writing and in the log book. Police will usually view the CCTV footage on the premises and this would not warrant any concerns for the data to be leaked.
- Should CD/DVD imagery be required as evidence, a copy may be released to the Police under the procedures described in this Policy. CD/DVD imagery will only be released to the Police on the clear understanding that the CD/DVD remains the property of the School, and both the CD/DVD and information contained on it are to be treated in accordance with this Policy.

- The School also retains the right to refuse permission for the Police to pass to any other person the CD/DVD or any part of the information contained thereon. On occasions when a Court requires the release of an original tape this will be produced from the secure evidence CD/DVD store, complete in its sealed bag.
- The Police may require the School to retain the stored CD/DVD imagery for possible use as evidence in the future. Such CD/DVD's will be properly indexed and properly and securely stored until they are needed by the Police.
- Applications received from outside bodies (e.g. solicitors) to view or release tapes will be referred to the Headteacher. In these circumstances the CD/DVD imagery will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. A fee can be charged in such circumstances: £50 for subject access requests; a sum not exceeding the cost of materials in other cases.

Access

Under the GDPR, individuals (to whom "Personal Data" relate) have the right to obtain confirmation that their personal information is being processed, including those obtained by CCTV.

Subject access request

In relation to Subject Access Requests ("**SAR**"):

- Individuals have the right to submit a SAR to gain access to their Personal Data in order to verify the lawfulness of the processing.
- SAR should be made on an application form available from the
- Headteacher.
- The School will verify the identity of the person making the request before any information is supplied.
- A copy of the information will be supplied to the individual free of charge; however, the School may impose a 'reasonable fee' to comply with requests for further copies of the same information.
- Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
- Requests by persons outside the School for viewing or copying disks, or obtaining digital recordings, will be assessed by the Headteacher, who will consult with the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.
- Where a request is manifestly unfounded, excessive or repetitive, the School holds the right to refuse to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one

month of the refusal. Alternatively, the School may charge a reasonable fee if the request is accepted by the School.

- All fees will be based on the administrative cost of providing the information.
- All requests will be responded to without delay and at the latest, within one month of receipt.
- In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.
- In the event that a large quantity of information is being processed about an individual, the School will ask the individual to specify the information the request is in relation to.
- It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.
- Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:
 - The Police – where the images recorded would assist in a specific criminal inquiry.
 - Prosecution agencies – such as the Crown Prosecution Service (CPS).
 - Relevant legal representatives – such as solicitors and barristers.
 - Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the FOA.

Requests for access or disclosure will be recorded and the Headteacher together with the DPO will make the final decision as to whether recorded images may be released to persons other than the Police.

Breaches of the code (including breaches of security)

Any breach of this Policy by the School staff will be initially investigated by the Headteacher with the assistance of the DPO, in order for him/her to take the appropriate disciplinary action.

Any serious breach of this Policy will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach. Following investigation, a breach of this Policy may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

Assessment of the Policy

Performance monitoring, including random operating checks, may be carried out by the School Business Manager to ensure compliance with this Policy.

Complaints

Any complaints about the School's CCTV system should be addressed to the Headteacher.

Monitoring and review

This Policy will be monitored and reviewed on a two-year basis by the DPO and the Headteacher to ensure that it meets legal requirements, relevant guidance published by the ICO and industry standards.

We may amend this Policy (at any time). The Headteacher will communicate changes to this Policy to all members of staff.

The scheduled review date for this Policy is located on the first page.

Public information

Copies of this Policy will be available to the public from the School office and the school website.

Summary of Key Points:

- This Policy will be reviewed every two years.
- The CCTV system is owned and operated by the School.
- The Control unit will not be manned out of school hours.
- The Control unit is not open to visitors except by prior arrangement and good reason.
- Liaison meetings may be held with the Police and other bodies.
- Recording hard drives and compact discs will be used properly indexed, stored and destroyed after appropriate use.
- Tapes may only be viewed by authorised school officers, control unit staff and the Police.
- CD/DVD imagery required as evidence will be properly recorded witnessed and packaged before copies are released to the police.
- CDs will be disposed of securely by incineration.
- Any breaches of this Policy will be investigated by the Headteacher. An independent investigation will be carried out for serious breaches.
- Breaches of the Policy and remedies will be reported to the Headteacher.

Appendix A- CCTV locations

- Camera -1 Car Park
- Camera-2 Old Building to New Building
- Camera-3 Nursery Playground
- Camera-4 Reception Playground
- Camera-5 Junior Playground Bottom
- Camera-6 Junior Playground Westside
- Camera-7 Junior Playground Topside
- Camera-8 Infant Playground
- Camera-9 Back of Old Building
- Camera-10 Front of Old Building
- Camera-11 Infants Playground Eastside
- Camera-12 Main Entrance Gate
- Camera-13 Prayer Garden
- Camera-14 Side Walkway to Junior playground.

Appendix B – Checklist

This CCTV system and the images produced by it are controlled by the School Business Manager who is responsible for how the system is used. The school notifies the Information Commissioner about the CCTV system, including any modifications of use and/or its purpose (which is a legal requirement of the GDPR).

The School has considered the need for using CCTV and have decided it is required for the prevention and detection of crime and for protecting the safety of the school's community. It will not be used for other purposes. The school will conduct regular reviews of our use of CCTV.

CCTV Review actions	Checked (Date if appropriate)	By	Date of next review
Notification has been submitted to the Information Commissioner and the next renewal date recorded.	May 2018	Matthew Bulpitt	Sep 2024
There is a named individual who is responsible for the operation of the system.	May 2018	Matthew Bulpitt	Sep 2024
A system had been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.	May 2018	Matthew Bulpitt	Sep 2024

Staff and members of the school community will be consulted about any proposal to install / amend CCTV equipment or its use as appropriate.	May 2018	Matthew Bulpitt	Sep 2024
Cameras have been sited so that they provide clear images.	May 2018	Matthew Bulpitt	Sep 2024
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.	May 2018	Matthew Bulpitt	Sep 2024
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).	May 2018	Matthew Bulpitt	Sep 2024
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.	May 2018	Matthew Bulpitt	Sep 2024
The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.	May 2018	Matthew Bulpitt	Sep 2024
Except for law enforcement bodies, images will not be provided to third parties.	May 2018	Matthew Bulpitt	Sep 2024
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the data controller knows to seek advice from the Information Commissioner as soon as such a request is made.	May 2018	Matthew Bulpitt	Sep 2024
Regular checks are carried out to ensure that the system is working properly and produces high quality images.	May 2018	Matthew Bulpitt	Sep 2024

Appendix C – CCTV Signage

It is a requirement of the GDPR to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The school is to ensure that this requirement is fulfilled.

The CCTV sign should include the following:

- That the area is covered by CCTV surveillance and pictures are recorded
- The purpose of using CCTV
- The name of the school
- The contact telephone number or address for any enquiries

Example sign.

