William Booth
Primary School
CCTV Policy
June 2019

Closed Circuit Television (CCTV) Policy

At our school we take our responsibility towards the safety of staff, visitors (including visiting children and property) very seriously. To that end, we use CCTV to monitor security and will actively seek instances of aggression or physical damage to our offices and its members.

The purpose of this policy is to manage and regulate the use of the CCTV system at our school and ensure that:

- We comply with the General Data Protection Regulation and the Data Protection Act 2018.
- The images that are captured are useable for the purposes we require them for.
- We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

This policy covers the use of CCTV which capture moving and still images of property and people who could be identified, as well as information relating to individuals for any of the following purposes:

- Observing what an individual is doing
- Taking action to prevent or detect a crime
- Using images of individuals that could affect their privacy

Legal framework

This policy has due regard to legislation including, but not limited to, the following:

- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The General Data Protection Regulation (GDRP May 2018)
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Equality Act 2010

This policy has been created with regard to the following statutory and non-statutory guidance:

- Home Office (2013) 'The Surveillance Camera Code of Practice'
- ICO (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'.

This policy operates in conjunction with the following Trust policies:

- Data Protection
- Freedom of Information Policy

Definitions

For the purpose of this policy a set of definitions will be outlined, in accordance with the surveillance code of conduct:

- **Surveillance** – monitoring the property and the movements and behaviour of individuals; this can include video, audio or live footage. For the purpose of this policy only video and audio footage will be applicable.
- **Overt surveillance** – any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000.
- **Covert surveillance** – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.

We do not condone the use of covert surveillance when monitoring staff or any of its visitors. Covert surveillance will only be operable in extreme circumstances.

Any overt surveillance footage will be clearly signposted around the school.

Roles and responsibilities

The role of the data protection officer (DPO) includes:

- Dealing with freedom of information requests and personal information requests (formerly known as subject access requests) in line with legislation, including the Freedom of Information Act 2000.
- Ensuring that all data controllers at the school handle and process surveillance and CCTV footage in accordance with data protection legislation.
- Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
- Ensuring consent is clear, positive and unambiguous. Pre-ticked boxes and answers inferred from silence are non-compliant with the GDPR.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Keeping comprehensive and accurate records 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 and if needed the Trust, e.g. the Trustees.

- Abiding by confidentiality requirements in relation to the duties undertaken while in the role.
- Monitoring the performance of the school's data protection impact assessment (DPIA) and providing advice where requested.
- Presenting reports regarding data processing at the school to the senior leadership team and the Governing Body; and where requested to the Trust.

*William Booth Schoo*l, as the corporate body, is the Data Controller. The Governing Body therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

The School Business Manager deals with the day-to-day matters relating to CCTV and for the benefit of this policy will act as the Data Controller.

The role of the Data Controller includes:

- Processing CCTV footage legally and fairly.
- Collecting CCTV footage for legitimate reasons and ensuring that it is used accordingly.
- Collecting CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection.
- Ensuring that any CCTV footage identifying an individual is not kept for longer than is necessary.
- Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure – especially when processing over networks.

Purpose and justification

The school will only use CCTV for the safety and security of the school and its staff and visitors.

CCTV is used as a deterrent for violent behaviour and damage to the school.

If the CCTV systems are no longer required the school will deactivate them.

The Data Protection principles

Data collected from CCTV will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- Accurate and, where necessary, kept up-to-date; every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Objectives

The surveillance system will be used to:

- Maintain a safe environment.
- Ensure the welfare of staff and visitors.
- Deter criminal acts against persons and property.
- Assist the police in identifying persons who have committed an offence.

Protocols

The CCTV system will be registered with the ICO in line with data protection legislation.

CCTV is a closed digital system which does **not** record audio.

Warning signs have been placed throughout the premises where CCTV is active, as mandated by the ICO's Code of Practice.

The system has been designed for maximum effectiveness and efficiency; however, the school cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

CCTV will not be trained on individuals, private vehicles or property unless an immediate response to an incident is required.

Security

Access to the CCTV, software and data will be strictly limited to authorised operators and will be password protected.

The school's authorised CCTV system operators are:

- AIT

The main control facility is kept secure and locked when not in use.

If, in exceptional circumstances, covert surveillance is planned, or has taken place, copies of the Home Office's authorisation forms will be completed and retained.

Our system will be tested for security flaws to ensure that they are being properly maintained at all times.

Our CCTV system will not be intrusive.

The CCTV Data Controller will decide when to record footage, e.g. a continuous loop outside the school grounds to deter intruders.

Any cameras that present faults will be repaired immediately as to avoid any risk of a data breach.

Privacy by Design

The use of CCTV will be critically analysed using a DPIA, in consultation with the DPO.

A DPIA will be carried out prior to any further installation of any surveillance and CCTV system.

If the DPIA reveals any potential security risks or other data protection issues, the school will ensure they have provisions in place to overcome these issues.

Where the school identifies a high risk to an individual's interests, and it cannot be overcome, the school will consult the Trust and or ICO before they use CCTV. The Trust will act on the ICO's advice.

The school will ensure that any further installation of CCTV will always justify its means.

Code of Practice

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 notifies all staff and visitors of the purpose for collecting surveillance data via notice boards, letters and emails.

CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All surveillance footage will be kept for **30** days for security purposes; the CCTV Data Controller is responsible for keeping the records secure and allowing access.

The school has a surveillance system for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of children, staff and visitors.

The CCTV **is owned by AIT** and images from the system are strictly controlled and monitored by authorised personnel only.

The school will ensure that CCTV is used to create a safer environment for children, staff and visitors to the school, and to ensure that its operation is consistent with the obligations outlined in data protection legislation. The policy is available from the school's website.

The 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 Data Controller, 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 which are communicated throughout the school.
- Only keep images and information for as long as required.
- 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 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.

Access

Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed.

All servers containing images belong to, and remain the property of AIT.

Individuals have the right to submit a personal information request to gain access to their personal data in order to verify the lawfulness of the processing.

The school will verify the identity of the person making the request before any information is supplied, requiring two forms of ID.

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 personal information request has been made electronically, the information will be provided in a commonly used electronic format.

Requests by persons outside the school for viewing or obtaining digital recordings, will be assessed by the CCTV Data Controller who will consult the DPO on a case-by-case basis with close regard to data protection and freedom of information legislation.

It is important that access to, and disclosure of, the images recorded by 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 lawyers 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 Freedom of Information Act 2000

Requests for access or disclosure will be recorded and the CCTV Data Controller will make the final decision as to whether recorded images may be released to persons other than the police.

Monitoring and Review of the Policy

This Policy may be amended at any time to take account of changes in legislation. The normal cycle of review for this policy will be two years.