ST BARTHOLOMEW'S SCHOOL

CCTV System Policy & Procedure

September 2024

INTRODUCTION

Closed Circuit Television Systems (CCTV) are installed in St Bartholomew's School (the School) premises and grounds; the use of CCTV and its compliance with Data Protection and other legislation is governed by this Policy. Recognisable images and any related documents and recordings captured by CCTV systems are "personal data" and are therefore subject to the provisions of the GDPR and the 2018 Data Protection Act.

1. PURPOSE OF POLICY

The purpose of this Policy is to regulate the use of Closed Circuit Television and its associated technology in the monitoring of both the internal and external environs of the premises under the remit of St Bartholomew's School.

2. SCOPE

This Policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material.

CCTV systems are installed (both internally and externally) in premises for the purpose of enhancing security of the building and its associated equipment, as well as creating a mindfulness among the occupants that a surveillance security system is in operation within and/or in the external environs of the premises during both the daylight and night hours every day of the year.

CCTV surveillance at the School is intended for the purposes of:

- Promoting the safeguarding of students and the health and safety of staff, students and visitors.
- Protecting the School buildings and School assets, both during and after School hours.
- Helping reduce the incidence of crime and anti-social behaviour (including theft and vandalism).
- Supporting a Police investigation in the event of a suspected crime.
- Ensuring that the School rules are respected so that the School can be properly managed.

The School does not operate any other forms of surveillance technology.

Definitions within this Policy are as per the Data Protection Policy.

3. RESPONSIBILITIES

The Headteacher is responsible for the overall implementation of this Policy.

The Data Protection Officer (DPO) is responsible for the privacy and data security of personal data as covered by this Policy.

The Estate Manager is responsible for the operational management of the system, including the functionality and efficiency of all cameras.

The ICT Manager is responsible for any technical support required for the operation of the system.

4. GENERAL PRINCIPLES

The School has a statutory responsibility for the protection of its property, equipment and other plant as well providing a sense of security to its employees, students and all visitors to its premises. The School owes a duty of care 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 by integrating the best practices governing the public and private surveillance of its premises.

The use of the CCTV system will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies for other purposes is prohibited by this Policy e.g. CCTV will not be used for monitoring employee performance; CCTV will not be used to monitor normal student/teacher classroom activity; nor will CCTV be used in areas where people expect privacy.

Information obtained through the CCTV system may only be released when authorised by the Headteacher and may be used in staff and student disciplinary processes

Any requests for CCTV recordings/images from the Police will be fully recorded and legal advice will be sought, as appropriate, if any such request is made. (See "Access" below). If a law enforcement authority, such as the Police, is seeking a recording for a specific investigation, the Police may require a warrant and accordingly any such request made by the Police should be requested in writing and the School will immediately seek legal advice, as appropriate.

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the School, including Equality, Anti-Bullying and Disciplinary Policies and the Concerns & Complaints Policy and Procedures.

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 School premises is limited to uses that do not violate the individual's reasonable expectation to privacy, for example, offices, the gym, changing rooms etc.

All CCTV systems and associated equipment will be required to be compliant with this Policy following its adoption by the School.

5. JUSTIFICATION FOR USE OF CCTV

The use of CCTV to control the perimeter of the School buildings for security purposes is justified as a legitimate interest (for the health and safety of individuals and for the prevention and detection of crime).

In other areas of the School where CCTV has been installed [such as the Hub, hallways, stairwells], the Data Protection Officer has demonstrated through a Data Protection Impact Assessment 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.

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

6. LOCATION OF CAMERAS

The School has selected locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals. Cameras placed so as to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

CCTV monitoring and recording of Public Areas in St Bartholomew's may include:

- The protection of School buildings and property (for example, the building's perimeter, entrances and exits, lobbies and corridors, special storage areas, receiving areas for goods/services).
- Monitoring of Access Control Systems (for example, monitor and record restricted access areas at entrances to buildings and other areas).
- Verification of Security Alarms (for example, Intrusion alarms, exit door controls, external alarms).
- Video Patrol of Public Areas (for example, parking areas, main entrance/exit gates, Traffic Control).
- Criminal Investigations as carried out by the Police (for example, as relating to burglary and theft surveillance or alleged assault).

CCTV Video Monitoring and Recording of Public Areas in St Bartholomew's does not include:

- The monitoring of an individual, their property or a specific group of individuals (unless an immediate response to events is required and in accordance with the Regulation of Investigatory Power Act 2000).
- Any observation on adjacent private homes, gardens and other areas of private property.

7. COVERT SURVEILLANCE

St Bartholomew's will not engage in covert surveillance.

Where the Police requests to carry out covert surveillance on School premises, such covert surveillance may require the consent of a judge. Accordingly, any such request made by the Police will be requested in writing and the School will seek legal advice.

8. NOTIFICATION – SIGNAGE

This Policy is made available to staff, students and visitors to the School in the shared area, on the School website or from the DPO.

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.

Adequate and compliant CCTV signage will:

- Be prominently displayed at the entrance to the School property.
- Include the name and contact details of the School as the data controller as well as the specific purpose(s) for which the CCTV camera is in place in each location.

9. STORAGE & RETENTION

The images/recordings will be held on a secure networked area; any media storing the recorded footage and the monitoring equipment will be securely stored in a restricted area.

Access to the system is controlled via a separate VPN and individual log ins, all devices with access to the CCTV VPN are located in locked offices.

Access to the system is controlled with a log of access on a secure and restricted google sheet. All access to CCTV images must be recorded on the google sheet. Access to this sheet is managed by the DPO who also determines the access permissions granted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the Headteacher.

Images are retained for the duration of one month (28 days); after this retention period, recordings are automatically over-written or deleted.

Where the images identify an issue (such as a staff or student disciplinary issue, break-in or theft) those particular images/recordings are retained specifically in the context of an investigation/student or staff disciplinary process/prosecution of that issue. It is then deleted upon resolution.

Images held in excess of their retention period will be reviewed on a three monthly basis by the DPO and any not required for evidential purposes will be deleted.

Access to retained CCTV images is restricted to the DPO and other persons authorised by the Headteacher or DPO.

10. VIEWING OF CCTV RECORDINGS

Access to the CCTV system and stored images will be restricted to authorised personnel only i.e. Headteacher, the Data Protection Officer, Leadership Team, the Estate Manager, the ICT Manager, and House Heads, Investigating Officers for staff or student disciplinary processes, the HR Manager when accompanying an Investigating Officer, Governors and the Clerk to Governors involved in or managing staff or student disciplinary processes. The Headteacher or DPO can authorise other individuals to view footage following a written request.

In relevant circumstances and following necessary authorisation, CCTV footage may be disclosed to other third parties:

- To the Police where the School (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 the School property.
- To any statutory body charged with child safeguarding.
- Where a suspicion of misconduct arises and at the formal request of the Investigating Officer or HR Manager, the DPO may provide access to CCTV images for use in staff disciplinary cases.
- To assist the Headteacher in establishing facts in cases of unacceptable student behaviour, in which case, the parents/guardians will be informed.
- To data subjects (or their legal representatives), pursuant to a Subject Access Request where the time, date and location of the recordings is furnished to the School. This is as documented in the Schools Rights and Requests Policy.
- To individuals (or their legal representatives) subject to a court order.
- To the School's insurance company where the insurance company requires same in order to pursue a claim for damage done to the insured property.

The Headteacher, Deputy Headteacher: Safeguarding & Inclusion, Assistant Headteachers for KS3 and KS4 are authorised to show students and parents CCTV footage of their children as part of a student disciplinary process as long any other individuals in the footage can be anonymised through blurring or other appropriate method.

Any authorised access request will be carried out:

- When access is logged on the restricted google sheet, including details from the data disclosure form and time/date/duration of access and images viewed.
- Viewed in a secure monitoring area and environment.

11. DOWNLOADING OF CCTV RECORDING

On occasion, and in exceptional circumstances, there is requirement to download footage.

In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings) any download media used to record events from the hard drive must be prepared in accordance with the following procedures: -

i. The completion of an authorised data disclosure form signed by the Data Protection Officer.
ii. Each download media and file must be identified by a unique reference number in the file name
iii. In exceptional circumstances, such as for legal proceedings, download media such as USB sticks, may be used. The download media must be brand new to avoid the potential for corruption or a data breach by other data still being accessible.
iv. The Data Protection Officer in conjunction with the Estate Manager will register the date and time of on, including its reference, if it is needed by an external organisation. If the download is for an internal staff or student process, the footage must be saved to a secure network area such as NewTopics or a GoogleDrive in order to share with permissions to view kept to a minimum.
v. Download media required for evidential purposes must be sealed, witnessed and signed by the Data Protection Officer, then dated and stored in a separate secure evidence store. If a download media is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed and signed by the Data Protection Officer, then dated and returned to the evidence store.
vi. If download media is archived the reference must be noted.
vii. Footage retained for an internal process must be deleted as soon as it is no longer needed.

12. ASSESSMENT OF THE SYSTEM

Performance monitoring, including random operating checks, may be carried out by the Estate Manager and the Data Protection Officer or specifically delegated personnel.

Where systems are already in operation, their operation will be reviewed regularly by the Estate Manager.

New CCTV systems will be introduced only after following a Data Protection Impact Assessment.

13. SECURITY COMPANIES

The School CCTV system is controlled by a security company contracted by the School.

The School has a written contract with the security company in place which details the areas to be monitored, how long data is to be stored, what the security company may do with the data, what security standards should be in place and what verification procedures apply.

The School remains the Controller of all personal data.

14. COMPLAINTS

Any complaints in relation to the School's CCTV system should be addressed to the Data Protection Officer or Headteacher.

15. POLICY MANAGEMENT

Publication - This Policy shall be available from the DPO, on the shared network and the School website.

Revisions - The DPO is responsible for the maintenance and accuracy of this Policy. This Policy will be reviewed every 3 years.

Other Documents and Policies

This Policy supplements St Bartholomew's School other policies relating to personal information, including but not limited to:

- Information Security Policy
- Data Protection Policy
- Rights and Requests Policy

Reference is made to the Information Commissioner's Office Guidance:
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/