CCTV Policy

Contents

Introduction 2
Definitions 2
Purpose 3
Scope 3
Principles of Use 3
Justification for use of CCTV 4
Data Protection Impact Assessment 4
Location of cameras 5
Covert surveillance 5
Notification, Signage and Awareness 6
Storage & Retention 6
Access 7
Responsibilities 7
Implementation and Review 9

Version	Date	Summary of changes	Author
V1.0	June 2019	Initial	One West
V1.1	Dec 2022	Refresh	One West
V2.0	Aug 2023	School and Town Council CCTV policies consolidated	One West
V2.1	Oct 2023	Formatting changes	One West

CCTV Policy

Introduction

Closed Circuit Television (CCTV) Systems are installed in Bathampton Primary School. Bathampton Primary School will adhere to the Surveillance Camera Commissioner's Code of Practice and its 12 principles in addition, relevant parts of data protection legislation covering the processing of personal data.

Definitions

CCTV – Closed-circuit television is the use of video cameras to transmit a signal to a specific place on a limited set of monitors. The images may then be recorded on video tape or DVD or other digital recording mechanism.

Data Protection Laws – The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 give rights to individuals as well as placing responsibilities on those persons handling, processing, managing, and controlling personal data. All staff must comply with the provisions of data protection laws when collecting and storing personal information. This applies to personal information relating both to employees of the organisation and individuals who interact with the organisation.

Data - information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on a computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system).

Directed Surveillance - covert surveillance in places other than residential premises or private vehicles.

Personal Data – Data relating 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 - this is where a person makes a request to the organisation for the disclosure of their personal data under data protection law.

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 Subject – an individual who is the subject of personal data.

Data Controller - a person/organisation who (either alone or with others) controls the contents and use of personal data.

Data Processor - a person/organisation who processes personal information on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of their employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. Data protection laws place responsibilities on such entities in relation to their processing of the data.

CCTV Policy

Purpose

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 Bathampton Primary School.

CCTV systems are installed on the premises for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the occupants, at any one time, 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 each day.

CCTV at Bathampton Primary School is intended for the purposes of:

- Protecting buildings and assets, both during and after working hours.
- Promoting the health and safety of staff, pupils, residents, and visitors.
- 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.

Scope

This Policy will determine the siting of CCTV equipment and define the approach to assessing the appropriateness of such locations to be used. It will specify the effective governance of CCTV equipment and the related processing activities. The Policy will ensure that Data Protection by Design is incorporated into Bathampton Primary School CCTV process and that the rights of data subjects are properly observed.

Principles of Use

Bathampton Primary School as the corporate body has a statutory responsibility for the protection of its property and equipment as well providing security to its employees, pupils and visitors to its premises. Bathampton Primary School owes a duty of care under the Health and Safety at Work etc. Act 1974 provisions of and associated legislation and utilises CCTV systems and their associated monitoring and recording equipment as an added mode of security and surveillance for those purposes.

The use of a CCTV system by Bathampton Primary School will observe the 12 principles of the Surveillance Camera Code of Practice.

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 take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the Banes, including Equality & Diversity Policy, Dignity at Work Policy, Codes of Practice for dealing with complaints of Bullying & Harassment and Sexual Harassment and other relevant policies, including the provisions set down in equality and other educational and related legislation.

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.

Information obtained in violation of this policy may not be used in a disciplinary proceeding against an employee of the school, member of the public, or a student attending one of its schools/centres.

All CCTV systems and associated equipment will be required to be compliant with this policy following its adoption by Bathampton Primary School. Recognisable images captured by CCTV systems are “personal data.” They are therefore subject to the provisions of the Data Protection Act 2018.

Justification for use of CCTV

Data Protection Laws requires that personal data is "adequate, relevant and not excessive" for the purpose for which it is collected. This means that Bathampton Primary 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 control the perimeter of the Bathampton Primary School for security purposes has been deemed to be justified by the Headteacher and Govenors.The system is intended to capture images of intruders or of individuals damaging property or removing goods without authorisation.

CCTV systems will not be used to monitor normal staff activity on site.

In other areas where CCTV has been installed, Bathampton Primary School 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.

Data Protection Impact Assessment

Prior to the adoption of any new CCTV system or where an existing system is identified as not having been assessed, a comprehensive DPIA must be undertaken. This will include a review of the purpose

or purposes for the use of CCTV; establish any impact it may have upon individuals; and any risks that may be involved with the system.

The Head Teacher will be responsible for completing the DPIA in collaboration with the DPO. Should a third party be used to deliver CCTV the person from the School responsible for its implementation will work alongside the third party and the DPO to ensure that the DPIA is completed.

Location of cameras

Bathampton Primary School has endeavoured to select locations for the installation of CCTV cameras where there will be a maximum effect, whilst having a minimum impact upon people's privacy. 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.

The following locations may be subject to CCTV Video Monitoring and Recording.

- The building's perimeter, entrances and exits, lobbies and corridors, special storage areas, cashier locations, receiving areas for goods/services for the purpose of ***protecting school buildings and property.***
- 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 verifying such alarms.
- Parking areas, main entrance/exit gates, traffic control for the purpose of video patrolling in the event that an incident occurs involving the wellbeing of pupils, staff or individuals associated with the school.

Covert surveillance

Bathampton Primary School will not engage in covert surveillance.

The police may request to carry out covert surveillance using school equipment, such covert surveillance will require the consent of a Justice of the Peace or Magistrate. Accordingly, any such request made by the police will be requested in writing and the school may seek legal advice.

CCTV Policy

Notification, Signage and Awareness

Adequate signage will be placed at each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation. Adequate signage will also be prominently displayed at the entrance to Bathampton Primary School property. Signage shall include the name and contact details of the data controller as well as the specific purpose(s) for which the CCTV camera is in place in each location.



WARNING

CCTV cameras in operation

Images are being monitored and recorded for the purpose of crime-prevention, the prevention of anti-social behaviour, for the safety of our staff and pupils and for the protection of Bathampton Primary School and its property. This system will be in operation 24 hours a day, every day.

These images may be passed to the police.

This scheme is controlled by Bathampton Primary School and operated by Select Security

For more information contact 01179 664881

Appropriate locations for signage will be at entrances to premises i.e. external doors, school gates.

Storage & Retention

In accordance with the sixth Data Protection Principle, which states that data "shall not be kept for longer than is necessary for" the purposes for which it was obtained the CCTV security system should not retain general footage beyond a month (28 days), except where the images identify an issue – such as a break-in or theft and those particular images/recordings are retained specifically in the context of an investigation/prosecution of that issue.

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.

The images/recordings will be stored in a secure environment. A log of access will be maintained that will show who accessed the system at what time and for what purpose. Access will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of Bathampton Primary School. Bathampton Primary School may delegate the administration of the CCTV system to another staff member.

Tapes/DVDs will be stored in a secure environment with a log of access to tapes kept. Access will be restricted to authorised personnel. Similar measures will be employed when using disk storage, with automatic logs of access to the images created.

Access

Unauthorised access to live feeds, equipment used to store images and any additional equipment that is used to support the system will not be permitted at any time. Such areas will be appropriately secured when not in use by authorised personnel. A log of access to tapes/images will be maintained.

CCTV footage may be accessed for the purposes defined in part 2 of this policy:

- By the police where Bathampton Primary School (or its agents) are required by law to make a report regarding the commission of a suspected crime; or
- 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 Bathampton Primary School property, or
- To the HSE and/or any other statutory body with the powers of investigation.
- To individuals (or their legal representatives) subject to a court order.

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.

Any person whose image has been recorded has a right to access the footage which relates to them as part of a Subject Access Request (SAR). Where the image/recording identifies another individual, those images may only be released where they can be redacted/anonymised or with the explicit consent of the other people identifiable in the footage. The SAR policy and guidance should be referred to if such a request is made.

A person should provide all the necessary information to assist Bathampton Primary School in locating the CCTV recorded data, such as the date, time, and location of the recording.

In giving a person a copy of their data, the Bathampton Primary School may provide a still/series of still pictures, a tape, or a disk with relevant images. However, other images of other individuals must be redacted before the data is released unless they have provided explicit consent for its disclosure.

Responsibilities

The Head Teacher will:

- In collaboration with the DPO 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.
- Ensure that the use of CCTV systems is implemented and controlled in accordance with the policy set down by Bathampton Primary School
- Complete a Data Protection Impact Assessment (DPIA) for any CCTV system/s and carry out a review of the DPIA/s on an annual basis.
- 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) to or the release of tapes or any material recorded or stored in the system.

- Ensure that monitoring recorded tapes are not duplicated for release.
- Ensure that the field of view of cameras conforms to this policy both internally and externally.
- Approve the location of temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events. *NOTE: [Temporary cameras do not include mobile video equipment or hidden surveillance cameras used for authorised criminal investigations by the police].*
- Consider both pupils and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment.
- Co-operate with the Health & Safety Officer of Bathampton Primary School in reporting on the CCTV system operation.
- Ensure that external cameras are non-intrusive in terms of their positions and views and comply with the principle of "Reasonable Expectation of Privacy."
- Ensure that monitoring tapes are stored in a secure place with access by authorised personnel only.
- Ensure that images recorded on tapes/DVDs/digital recordings are stored for a period not longer than 28 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other use as approved by senior management in consultation with the DPO.
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas.
- Ensure that where the police request to set up mobile video equipment for criminal investigations, legal advice has been obtained and such activities have the approval of senior management.

SECURITY COMPANIES

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

The following applies:

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 written contract also states that the security company will give the **school** all reasonable assistance to deal with any subject access request made under data protection laws which may be received by the **school** within the statutory time-frame (generally 30 days).

Security companies that place and operate cameras on behalf of clients are considered to be "Data Processors." As data processors, they operate under the instruction of data controllers (their clients).

Data protection laws place a number of obligations on data processors. These include having appropriate security measures in place to prevent unauthorised access to, or unauthorised alteration, disclosure, or destruction of, the data, in particular where the processing involves the transmission of data over a network and against all unlawful forms of processing.

This obligation can be met by having appropriate access controls to image storage or having robust encryption where remote access to live recording is permitted. Staff of the security company have been made aware of their obligations relating to the security of data.

CCTV Policy

Implementation and Review

The policy will be reviewed on an annual basis or in the event of significant change to the system, national guidance, best practice of legislation relating to the capture of images by CCTV.

This policy was approved by the Board of Govenor's on October 2026.

Approver:

Komilla Datta
Headteacher