CCTV Policy

1. Introduction

Closed Circuit Television (CCTV) Systems are installed in St John the Evangelist Church School.

CCTV operation will be reviewed regularly in consultation with staff, the board of management.

2. 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 school.

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, 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 the school 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);
- supporting the Police in a bid to deter and detect crime;
- assisting in identifying, apprehending and prosecuting offenders; and
- ensuring that the school rules are respected so that the school can be properly managed.

3. Scope

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

4. General Principles

The school as the corporate body 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 invitees to its premises. The school owes a duty of care under the provisions of Safety, Health and Welfare at Work Act 2005 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 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 monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the school, 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.

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.

Information obtained in violation of this policy may not be used in a disciplinary proceeding against an employee of the school 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 the school. Recognisable images captured by CCTV systems are "personal data." They are therefore subject to the provisions of the Data Protection Act 2018.

5. Justification for use of CCTV

The Data Protection Act requires that data 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 control the perimeter of the school buildings for security purposes has been deemed to be justified Bath & Wells Multi Academy Trust. 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 teacher/student classroom activity in school.

6. Location of cameras

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 school has endeavoured to select locations for the installation of CCTCV 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 Video Monitoring and Recording of Public Areas in the school may include the following:

- ***Protection of school buildings and property:*** The building's perimeter, entrances and exits, lobbies and corridors, special storage areas, cashier locations, receiving areas for goods/services
- ***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

7. Covert surveillance

The school will not engage in covert surveillance.

Where the police may request 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. Informing / fairness – signage

The school will provide a copy of this CCTV Policy on request to staff, students, parents and visitors to the school. 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, and referenced in all the schools Privacy Notices.

Adequate signage will be displayed at the entrance to the school propertyat or close to each internal camera.

9. Storage & Retention

The Data Protection Act states that data "shall not be kept for longer than is necessary for" the purposes for which it was obtained. A data controller needs to be able to justify this retention period. For a normal CCTV security system, it would be difficult to justify retention 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 60 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 with a log of access kept. Access will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the Headteacher. The school may delegate the administration of the CCTV System to another staff member. In certain circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out above (such individuals may include the Police, the Business manager, the relevant Year Head, other members of the teaching staff, representatives of the Department of Education and Skills, representatives of the HSE and/or the parent of a recorded student). When CCTV

recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

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.

10. Access

Tapes/DVDs storing the recorded footage and the monitoring equipment will be securely stored in a restricted area. Unauthorised access to that area will not be permitted at any time. The area will be locked when not occupied by authorised personnel. A log of access to tapes/images will be maintained.

Access to the CCTV system and stored images will be restricted to authorised personnel only.

In relevant circumstances, CCTV footage may be accessed:

- By the police where the 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 the school property, or
- To the HSE and/or any other statutory body charged with child safeguarding; or
- To assist the Principal in establishing facts in cases of unacceptable student behaviour, in which case, the parents/guardians will be informed; or
- To data subjects (or their legal representatives), pursuant to an access request where the time, date and location of the recordings is furnished to the school or
- 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.

Requests by the police: Information obtained through video monitoring will only be released when authorised by the Head teacher following consultation with the Chairperson of the Board of Management. If the police request CCTV images for a specific investigation, the police may require a warrant and accordingly any such request made by the police should be made in writing and the school should immediately seek legal advice.

Access requests: On written request, any person whose image has been recorded has a right to be given a copy of the information recorded which relates to them, provided always that such an image/recording exists i.e. has not been deleted and provided also that an exemption/prohibition does not apply to the release. Where the image/recording identifies another individual, those images may only be released where they can be redacted/anonymised so that the other person is not identified or identifiable. To exercise their right of access, a data subject must make an SAR in writing to the school Business manager.

Access requests can be made to the following: School Business Manager

A person should provide all the necessary information to assist the school in locating the CCTV recorded data, such as the date, time and location of the recording. If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data and may not be handed over by the school.

In giving a person a copy of their data, the school may provide a still/series of still pictures, a tape or a disk with relevant images. However, other images of other individuals will be obscured before the data is released.

11. Responsibilities

The Business Manager will:

- Ensure that the use of CCTV systems is implemented in accordance with the policy set down by the school
- 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 in 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) 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 perimeter of view from fixed location 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].*
- 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 is likely to take place
- Co-operate with the Health & Safety Officer of the school in reporting on the CCTV system in operation in the school
- Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing 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 60 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by the Chairperson of the Board
- 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 monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics
- 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 the Chairperson of the Board

SECURITY COMPANIES

The school CCTV system is controlled by a security company contracted by the school
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 the Data Protection Act 2018 which may be received by the school within the statutory time-frame (generally 40 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). The Data Protection Act 2018 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 has been made aware of their obligations relating to the security of data.

12. Implementation & Review

The policy will be reviewed and evaluated every 3 years. On-going review and evaluation will take cognisance of changing information or guidelines (e.g. from the ICO, the police, Department of Education and Skills, Audit units (internal and external to the school/) national management bodies, legislation and feedback from parents/guardians, students, staff and others).

Date Implemented:	September 2021

APPENDIX 1 – DEFINITIONS

Definitions of words/phrases used in relation to the protection of personal data and referred to in the text of the policy;
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.
The Data Protection Acts – The Data Protection Acts 2018 rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All school staff must comply with the provisions of the Data Protection Acts 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 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).
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 the Data Protection Act 2018.
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 who (either alone or with others) controls the contents and use of personal data.
Data Processor - a person 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. The Data Protection Acts place responsibilities on such entities in relation to their processing of the data.

APPENDIX 2 - PRIVACY IMPACT ASSESSMENT

It is a statutory requirement that any activity involving a high risk to the data protection rights of the individual when processing personal data be assessed by the Data Protection Impact Assessment. Prior to the assumption of any such activity the school will consult with its Data Protection Officer assess risks based on an initial screening process. The DPIA will:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

Upon completion of a DPIA the regulator (ICO) maintains the right to cease the proposed processing should it remain high risk.

Before a school installs a new CCTV system, it is recommended that a documented privacy impact assessment is carried out. A school which properly conducts such an assessment is less likely to introduce a system that contravenes the provisions of the Data Protection Acts 2018. This is an important procedure to adopt as a contravention may result in action being taking against a school by the ICO, or may expose a school to a claim for damages from a student.

Some of the points that might be included in a Privacy Impact Assessment are:

- What is the school purpose for using CCTV images? What are the issues/problems it is meant to address?
- Is the system necessary to address a pressing need, such as staff and student safety or crime prevention?
- Are the CCTV cameras intended to operate on the outside of the premises only?
- Is it justified under the circumstances?
- Is it proportionate to the problem it is designed to deal with?
- Is it intended that CCTV cameras will operate inside of the building?
- Are internal CCTV cameras justified under the circumstances?
- Are internal CCTV cameras proportionate to the problem they are designed to deal with?
- What are the benefits to be gained from its use?
- Can CCTV systems realistically deliver these benefits? Can less privacy-intrusive solutions, such as improved lighting, achieve the same objectives?
- Does the school need images of identifiable individuals, or could the system use other images which are not capable of identifying the individual?
- Will the system being considered deliver the desired benefits now and remain suitable in the future?
- What future demands may arise for wider use of images and how will they be addressed?
- Is the school, the data controller for the entire CCTV system (bearing in mind that some schools under the PPP are managed for operational purposes by management companies, in which case specific legal advice may need to be sought)?.
- Where a management company is in place, is the school satisfied that it complies with the Data Protection Act with regard to the processing of images of staff, students and visitors to your school captured on any CCTV systems under its management?
- What are the views of those who will be under CCTV surveillance?

- What could be done to minimise intrusion for those whose images may be captured, particularly if specific concerns have been expressed?
- How have staff, students and visitors been assured by the School that they will not be monitored and that the CCTV system will be used only for the stated purposes?
- Does the school's policy on the use of CCTV make it clear that staff (teaching and non-teaching) will not be monitored for performance or conduct purposes?
- Have the views of staff & students regarding the location of cameras been taken into account?
- Can the location of each internal camera be justified in accordance with the overall purpose for the use of the CCTV system?
- Has appropriate signage been erected at the location of each internal camera indicating that recording is taking place and outlining the purpose of such recording?
- Who will have access to the system and recordings/images?
- What security measures are in place to protect the CCTV system and recordings/images?
- Are those who will have authorised access to the system and recordings/images clear about their responsibilities?
- Are the camera monitors kept out of view of staff, students and visitors and is access to the camera monitors restricted to a limited number of staff on a 'need to know' basis?
- Is the room(s) which houses the camera monitors and the CCTV system securely locked when unattended?
- Does the school have a procedure in place to ensure that recordings/images are erased or deleted as soon as the retention period (28 days) has expired?
- Does the school have a procedure in place for handling requests for access to recordings/images from An Garda Síochána?
- Will appropriate notices be in place to ensure that individuals know that they are being monitored?
- Does the school have a data protection policy? Has is been updated to take account of the introduction of a CCTV system?
- Does the school have a procedure in place to handle access requests seeking a copy of images recorded by the CCTV system (within the statutory timeframe of forty days)?
- Has the right of access been communicated to staff, students and visitors?
- Has the school communicated its policy on the use of CCTV to staff, students and visitors and how has this been done?
- How are new students and new staff informed of the school's policy on the use of CCTV?