



## 1 Introduction

- 1.1 The purpose of the CCTV System Policy in Monaghan Collegiate School is to regulate the management, operation and use of the closed circuit television (CCTV) system in the school environs.
- 1.2 The system comprises a number of fixed cameras located around the school site. The policy follows Data Protection Commissioner guidelines and is drafted in conformity with the Data Protection Acts 1988-2003.
- 1.3 The policy is drafted in consultation with all the education partners within the school community and is subject to review.
- 1.4 The system is wholly owned and operated by the school.

## 2 Objectives of the System

- 2.1 To protect the school buildings and their assets
- 2.2 To increase personal safety of staff, pupils and visitors and reduce the fear and incidence of crime.
- 2.3 To protect members of the public and private property.
- 2.4 To assist in managing the school.
- 2.5 To assist in relation to matters other than security, namely the promotion of and compliance with Health and Safety standards and the taking of appropriate disciplinary measures, where so required.
- 2.6 The system will not be used to monitor staff conduct or performance, except where required to investigate the alleged commission of a crime.

## 3 Statement of intent

- 3.1 The school will treat the system and all information, documents and recordings obtained and used there from as data which may be deemed personal data requiring protection under the Acts.
- 3.2 Cameras will be used to monitor activities within the school circulation areas, student areas, its car parks and other public areas as an adequate, relevant and proportionate response to the achievement of the objectives identified at paragraph 2.1.
- 3.3 The cameras used by the school are fixed position cameras and cannot be zoomed or remotely altered.
- 3.4 Materials or knowledge secured as a result of the use of the System will not be used for any commercial purpose.
- 3.5 The recorded images shall be stored on Zip Discs which will only be released to the Gardai or other third parties for use in the investigation of a specific crime with the written authority of the Garda Síochána. Zip Discs containing personal data will never be released to the media or other third parties for any purpose that is not permitted under the Policy without the Data Subject's consent.
- 3.6 The planning and design of the System has endeavoured to ensure that it will give maximum effectiveness and efficiency insofar as is reasonably practicable but it is not possible to guarantee that the System will cover or detect every single incident taking place in the areas of coverage.

3.7 Warning signs, as required by the Code of Practice of the Data Protection Commissioner have been placed at all access routes to areas covered by the school CCTV's to inform all persons who may be deemed Data Subjects, of the operation of the System.

#### 4 Operation of the system

4.1 For the purposes of the Data Protection Acts 1988-2003 the Data Controller will be Monaghan Collegiate School. In practice, the System will be managed by the Principal, in accordance with the principles and objectives expressed in the Policy.

4.2 The day-to-day management will be the responsibility of the Deputy-Principal as approved by the Principal. Other personnel may also be authorised by the Principal to view recorded images for the purposes outlined in this policy.

4.3 There should always be two persons involved in reviewing recordings.

4.4 The Control panel will be located on the sidewall of the Administration Office, screened from public view.

4.5 The system will be operated 24 hours each day, every day of the year, except for periods of breakdown or necessary maintenance.

4.6 Recordings will remain on the system for 28 days, and will then be replaced by new recordings.

#### 5 Control Panel

5.1 The Administration Office is where the system is installed and from where it is controlled. The Deputy-Principal will check and confirm the efficiency of the system regularly and in particular that the equipment is properly recording and that cameras are functional. The recording equipment password is protected.

5.2 Access to the Control Panel will be limited to the authorised people while recorded data is being viewed.

5.3 If out of hours emergency maintenance arises, the caretaking staff must be satisfied of the identity and purpose of maintenance before allowing access to the control room.

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

#### 6 6. Monitoring procedures:

6.1 Camera surveillance will be maintained at all times will be used only in accordance with this policy:

6.2 Cameras are installed in the following areas

6.2.1 Entrance to school buildings

6.2.2 Stairs

6.2.3 External of building

6.2.4 Car parking areas

6.2.5 Study/Dining hall

#### 7 Video recording procedures:

7.1 Recordings are initially made to a hard disc, which is located in the Control Panel in the Administration Office. The equipment is programmed to delete images after 28 days automatically. Data can be recorded on to zip discs for specific purposes of legitimate investigation in accordance with this policy and with the authorisation of the Principal. Such zip discs will be stored in the school safe adjacent to the Principal's office.

7.2 In order to maintain and preserve the integrity of the zip discs used to record events from the hard drive and the facility to use them in any further investigations, the following procedures for their use and retention must be strictly adhered to:

7.2.1 Each zip disc must be identified by a unique mark.

7.2.2 Before use each zip disc must be cleaned of any previous recording.

- 7.2.3 The authorised person shall register the date and time of the zip disc insert, including zip disc reference.
- 7.2.4 A zip disc required for evidential purposes must be sealed, witnessed, signed by the Authorised person, dated and stored in the school safe.
- 7.2.5 If the zip disc is archived the reference must be noted.
- 7.2.6 Zip discs may be viewed by the Gardai for the prevention and detection of crime on receipt of a warrant from a senior officer.
- 7.2.7 A record will be maintained of the release or viewing of zip discs to the Gardai or other authorised persons. A register will be maintained by the Deputy Principal for this purpose.
- 7.2.8 Should a zip disc be required as evidence, a copy may be released to the Gardai. Zip discs will only be released to the Gardai on the clear understanding that the recording remains the property of the school, and both the zip disc and information contained on it are to be treated in accordance with this code. The school also retains the right to refuse permission for the Gardai to pass to any other person the zip disc or any part of the information contained thereon. On occasions when a Court requires the release of an original zip disc this will be produced from the secure evidence zip disc store, complete in its sealed bag.
- 7.2.9 The Gardai may require the school to retain the stored zip discs for possible use as evidence in the future. Such zip discs will be properly indexed and properly securely stored until they are needed by the Gardai
- 7.3 In respect of zip discs not required to be retained for security, crime detection or other legitimate purposes.
  - 7.3.1 The School will ensure its best endeavours are used to safely and properly dispose of the contents of the zip discs after 28 days.
  - 7.3.2 Applications received from outside bodies (e.g. solicitors) to view or release personal data stored on zip discs and held by the School will be referred to the Principal. In these circumstances a copy of the relevant zip disc will normally be made available for viewing or 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 may be charged in such circumstances.
- 8 Breaches of the Policy (including breaches of security).
  - 8.1 Any breach of the Policy by the school staff or any other person with responsibility under the Policy will be initially investigated by the Principal, in order for him/her to take the appropriate disciplinary action.
  - 8.2 Any serious breach of the policy will be immediately investigated and an independent investigation carried out by nominees of the Principal to make recommendations on how to remedy the breach.
- 9 Assessment of the System.
  - 9.1 Performance monitoring, including random operating checks, will routinely be carried out.
- 10 Complaints
  - 10.1 Any complaints about the School's CCTV system should be addressed to the Principal.
  - 10.2 Complaints will be investigated in accordance with paragraphs 8.1 and 8.2 of the Policy.
  - 10.3 Any person who might be deemed a Data Subject in relation to the System shall be at liberty to make a complaint directly to the office of the Data Protection Commissioner, Canal House, Station Road, Portarlinton, Co. Laois.

11 Access by the Data Subject:

- 11.1 The Acts provide Data Subjects (individuals to whom “personal data relate”) with a right of access to personal data held about themselves (including images recorded by the System and stored on zip discs), under the terms of the Acts.
- 11.2 Requests by Data Subjects for such access should be made in writing to the Principal.
- 11.3 The form of access granted may consist of facilities being offered at the School premises to view the relevant personal data or the release of a copy zip disc storing the relevant personal data.

12 Public information:

- 12.1 Copies of the Policy will be available to the public from the School Office and the Principal.

This policy has been tabled, discussed and approved by the Board of Management of Monaghan Collegiate School

#### **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 1988 and 2003 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All school/ETB 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.

**Access Request** – this is where a person makes a request to the organisation for the disclosure of their personal data under Section 3 and/or section 4 of the Data Protection Acts.

**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

Before a school/ETB installs a new CCTV system, it is recommended that a documented privacy impact assessment is carried out. A school/ETB which properly conducts such an assessment is less likely to introduce a system that contravenes the provisions of the Data Protection Acts 1988 & 2003. This is an important procedure to adopt as a contravention may result in action being taken against a school/ETB by the Office of the Data Protection Commissioner, or may expose a school/ETB 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/ETB's 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/ETB 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/ETB, 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/ETB satisfied that it complies with the Data Protection Acts 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/ETB'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/ETB 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/ETB 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//ETB have a data protection policy? Has it been updated to take account of the introduction of a CCTV system?
- Does the school/ETB 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/ETB 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?



**Images are being monitored and recorded for the purpose of:**

- **crime-prevention,**
- **the prevention of anti-social behaviour,**
- **the prevention of bullying,**
- **for the safety of our staff and students,**
- **and for the protection of Monaghan Collegiate School and its property.**

This system will be in operation 24 hours a day, every day.

These images may be passed to An Garda Síochána. This scheme is controlled by Monaghan Collegiate School.

For more information phone 04782060

Principal