



CCTV Policy - Ballinteer Community School

INTRODUCTION

Ballinteer Community School installed an internal Closed Circuit Television System (CCTVS) during the scholastic year 2012-2013, which supplemented an existing external CCTV system installed in the new school building at the time of its completion in 2008. There has not been a CCTV School Policy to-date.

This CCTV Policy is drawn-up in consultation with staff, the Parent's Association and the Board of Management. The Board of Management of Ballinteer Community School will review the operation of this CCTV system biannually in consultation with staff, and the Parent's Association.

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 Ballinteer Community School.

The CCTV system in Ballinteer Community School is installed on the premises (both internally and externally) to enhance the security of the building and its associated equipment. CCTV surveillance at Ballinteer Community School is exclusively and specifically for the purpose 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 Gardaí in a bid to deter and detect crime;
 - Assisting in identifying, apprehending and prosecuting offenders; and ▪
- Ensuring that there is respect for the school rules.

2. SCOPE

This policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material. The Board of Management of Ballinteer Community School will ensure that it operates its CCTV system, only in a way that is compatible with the provisions of this policy.

3. GENERAL PRINCIPLES

Ballinteer Community School has a statutory responsibility for the protection of its property, equipment and other plant as well as providing a sense of security to its employees, students and visitors to its premises. As such, Ballinteer Community School has a duty of care under the provisions of the 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 best practice governing the public and private surveillance of its premises.

The use of the CCTV system will, at all times, 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 the policy e.g. CCTV will not be used for monitoring employee performance.

Information, obtained through the CCTV system, may only be released after authorisation by the Principal and following consultation with the Chairperson of the Board of Management. Any requests for CCTV recordings/images from An Garda Síochána will be fully chronicled by the Principal, and legal advice will be sought if any such request is made. (See “Access” below). If a law enforcement authority, such as An Garda Síochána, is seeking a recording for a specific investigation, An Garda Síochána may require a warrant and accordingly any such request made by An Garda Síochána must be requested in writing at which time the school will immediately seek legal advice on the matter.

Any CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all other existing school policies and be cognisant of policies yet to be adopted by the school, including the Equality & Diversity Policy, Dignity at Work Policy, Codes of Practice for dealing with complaints of Bullying & Harassment and Sexual Harassment and other relevant policies, and include 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 will not be used in a disciplinary proceeding against an employee of the school or a student attending the school. All CCTV systems and associated equipment within the school campus will be required to be compliant with this policy following its ratification by the Board of Management of Ballinteer Community School. Recognisable images captured by CCTV systems are “personal data.” They are therefore subject to the provisions of the Data Protection Acts 1988 and 2003.

4. JUSTIFICATION FOR USE OF CCTV

Section 2(1) (c) (iii) of the Data Protection Acts requires that data is "adequate, relevant and not excessive" for the purpose for which it is collected. This means that Ballinteer Community School must 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 the purpose of security, is justified by the Board of Management on the basis that the system is intended to capture images of intruders or individuals damaging property or removing goods without authorisation.

The CCTV system will not be used to monitor normal teacher/student classroom activity in school.

In other areas of the school, where CCTV is currently installed, e.g. hallways, stairwells, locker areas, the Principal has established that there is a proven risk to security and health & safety of the school community and that the installation of CCTV is proportionate in addressing such issues that have arisen prior to the installation of the system. The decision to place internal cameras in Ballinteer Community School resulted directly from repeated student interference with the Fire Alarm system and the inherent health and safety implications resulting in such interference.

5. LOCATION OF CAMERAS

The location of cameras is a key consideration of this policy. The location of CCTV to monitor areas where individuals would have a reasonable expectation of privacy cannot be justified. Ballinteer Community School has endeavoured to select locations in which the installation of CCTV cameras are least intrusive in order to protect the privacy of individuals. The placement of cameras to record external areas are located in such a way as to prevent or minimise the recording of passersby or of another person's private property.

CCTV Video Monitoring and Recording of Public Areas in Ballinteer Community School 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, school grounds and Traffic Control
 - ***Criminal Investigations (carried out by An Garda Síochána):*** Robbery, burglary and theft surveillance
-

6. COVERT SURVEILLANCE

Ballinteer Community School will not engage in covert surveillance.

Where An Garda Síochána makes a 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 An Garda Síochána will be requested in writing and the school will seek legal advice prior to consent.

7. NOTIFICATION – SIGNAGE

The Principal 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. The location of CCTV cameras will also be indicated to the Board of Management. Adequate signage will be placed at each location in which a CCTV camera is sited to indicate that CCTV is in operation. Adequate signage will also be prominently displayed at the entrance to **Ballinteer Community**

School campus. 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, the prevention of bullying, for the safety of our staff and students and for the protection of Ballinteer Community School and its property. This system will be in operation 24 hours a day, every day. These images may be passed on to An Garda Síochána.

This CCTV system is controlled and operated by the Principal/Deputy Principal of Ballinteer Community School.

For more information contact: 01 2988195

8. STORAGE & RETENTION

Section 2(1)(c)(iv) of the Data Protection Acts 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, images captured by the CCTV system installed in Ballinteer Community School will be retained for a maximum of 28 days, except where an image/s 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 ONLY. Supervising the access and maintenance of the CCTV System is the responsibility of the Principal. The Principal may delegate the administration of the CCTV System to the Deputy Principal. 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 Gardaí, the Deputy Principal, 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 ONLY on a need-to-know basis. All viewings will be recorded and logged accordingly, with logged signatures of the relevant parties.

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

9. 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 under any circumstances or at any time. The area will be secured when not occupied by authorised personnel. A register of instances of access to recorded images will be maintained by the controller.

Access to the CCTV system and stored images will be restricted to authorised personnel ONLY i.e. the Principal of the school or the Deputy Principal in the Principal's absence .

In relevant circumstances, CCTV footage may be accessed:

- By An Garda Síochána where Ballinteer Community School are required by law to make a report regarding the commission of a suspected crime; or
- Following a request by An Garda Síochána when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on Ballinteer Community School property.
- 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 authorized access request where the time, date and location of the recordings is furnished to Ballinteer Community School, or
- To individuals (or their legal representatives) subject to a court order.
- By the school's insurance company where the insurance company requires same in order to pursue a claim for damage done to the insured property.

An access register will be kept by the Principal, stating who accessed the recordings/images, on what dates and times, and for what purposes the recordings/images were accessed.

Requests by An Garda Síochána: Information obtained through video monitoring will only be released when authorised by the Principal following consultation with the Chairperson of the Board of Management. If An Garda Síochána request CCTV images for a specific investigation, An Garda Síochána may need to furnish a warrant, and accordingly any such request made by An Garda Síochána to Ballinteer Community School should be made formally 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 application in writing to the school Principal. The school may charge up to €6.35 for responding to such a request and must respond **within 40 days, by registered post.**

Access requests may be made in writing to... Mr David O'Connell, The Principal, Ballinteer Community School, Ballinteer, Dublin 16.

A person should provide all the necessary information to assist Ballinteer Community 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 as such 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.

10. RESPONSIBILITIES

The Principal will:

- Ensure that the use of CCTV systems is implemented in accordance with the policy set down by the Board of Management of Ballinteer Community School
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within Ballinteer Community School
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy
- Ensure that the CCTV monitoring at Ballinteer Community 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 register) 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 An Garda Síochána].*
- 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 (locations must be justified)
- 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 Ballinteer Community 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 28 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 of Management of Ballinteer Community School
- 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 An Garda Síochána request to set up mobile video equipment for criminal investigations, legal advice is obtained and such activities have the approval of the Chairperson of the Board of Management of Ballinteer Community School

11. SECURITY COMPANIES

If the CCTV system in operation in Ballinteer Community School, is controlled by a security company contracted by the school, the following will apply:

The school will put **a written contract with the security company in place**, which details the areas to be monitored, the length of time the 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 Section 4 Data Protection Acts 1988 and 2003 and which may be received by the school within the statutory timeframe (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). Sections 2(2) and 2C of the Data Protection Acts 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. See [Content of the Service Agreement](#) for further guidance.

12. IMPLEMENTATION & REVIEW

The policy will be reviewed and evaluated from time to time. On-going review and evaluation will take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, An Garda Síochána, 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.

The date from which the policy will apply is the date of adoption by the Board of Management. Implementation of the policy will be monitored by the Principal of the school.

**Ratified by the Board of Management of Ballinteer Community School on 8th
June 2017**

Mr David Dwyer Chairperson

Mr David O'Connell Principal

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 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. All requests should be made formally, in writing.

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 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 1988 & 2003. This is an important procedure to adopt as a

contravention may result in action being taken against a school by the Office of the Data Protection Commissioner, or may expose a school to a claim for damages from a student, staff member or visitor.

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 intended 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 that 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 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 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, and has the policy 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 (40) 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?

APPENDIX 3 - ROLES

Data Controller: Mr David O'Connell, Principal, Ballinteer Community School, Ballinteer, Dublin 16

Telephone: 01 298 8196. Email:

Data Processor: Gallant Security Systems Limited

Unit 715, Northwest Business Park, Phase 4, Kilshane Drive, Blanchardstown, Dublin 15.

Telephone: 01 861 2770, Fax: 01 861 2764

Emergency No: 087 266 6782. Email: info@gallantsecurity.com

APPENDIX 4 - The Data Protection Commissioners Guidelines for the use of CCTV in schools

It is recommended that where CCTV systems are not already installed in school grounds, and an actual need for CCTV monitoring has been identified, the CCTV system should only be introduced following consultation by the Board of Management with staff, students and parents and following a privacy impact

assessment being carried out (see the template Privacy Impact Assessment at Appendix 2 of the [CCTV Policy Template](#). Where CCTV systems are already in place, their use will be reviewed periodically, in consultation by the Board of Management with staff, students, and parents.

Where CCTV is in operation, the school should have a CCTV Policy in place.

Template CCTV policy for Schools: Download [CCTV Policy Template](#). For assistance in developing a CCTV policy, and operating a CCTV system in compliance with data protection, see Guidelines on the use of CCTV Footage (Extract from the Office of the Data Protection Commissioner – Guidelines for CCTV footage)

The principle rationale for the installation of such systems can primarily be for security purposes. The Data Protection Commissioner recognises that CCTV recording may be justified for securing the perimeter of school property. However it may not be justifiable for day-to-day monitoring of staff and students. The Data Protection Commissioner advises that CCTV cameras should not enter the classroom itself. The Commissioner also advises that it would be difficult to justify the use of CCTV in offices. Indeed, any use beyond monitoring the perimeter of the school/ETB premises would need to be fully justifiable and evidence-based, with a very high threshold for such evidence. For example, it may not be justified or proportionate to continually monitor staff and students through the CCTV system, and such monitoring could be highly intrusive and in breach of the Data Protection Acts. In addition, if the CCTV recording is being used to tackle and prevent criminal/anti-social behaviour/theft/vandalism in known trouble spots, the school/ETB may have to demonstrate that monitoring/patrolling the area periodically by staff was not working and that the criminal/anti-social behaviour was continuing or the cost of monitoring was prohibitive. In order to justify the erecting of CCTV cameras in an area, the school/ETB may have to show that the location was a proven trouble-spot which had generated significant problems in the past (including a risk to security, and/or to the health and safety of staff and students) and therefore constituted a security/safety concern which the CCTV monitoring was designed to address. For example, see the Data Protection Commissioner's case study 8 of 2010, in which it

is stated that using CCTV for a non-security related matter (i.e. to address a workperformance issue) could be in breach of the data protection acts. The school/ETB will therefore have to ensure that the CCTV recording is justified, necessary, reasonable and proportionate in all the circumstances.

It is important to note that the location of the CCTV cameras should be chosen with great care and should not be erected in places where individuals would have a reasonable expectation of privacy (such as changing rooms and bathrooms). In general, CCTV cameras on school/ETB premises will be erected in a fixed place and should not be rotated/trained on certain individuals or events. Schools/ETBs should ensure to the greatest extent possible that there is no (or only minimal) recording of passers-by or another person's private property. See in particular, the Data Protection Commissioner's case study 8 of 2005 ("CCTV Cameras on the Luas Line").

Schools should be aware that the images captured on CCTV might have to be handed over to An Garda Síochána as part of inquiries into criminal activity (see ["What if a school is asked by a law enforcement authority for access to the recordings?"](#) set out below). The images may also have to be handed over to the individuals captured on the CCTV, who will each be considered a "data subject" and has the right to make a data access request under section 4 Data Protection Acts. See [Section 3 and 4 access requests](#), and see also [Requests for CCTV footage held](#).

The school/ETB will have to ensure that it can provide data subjects with copies of that subject's images captured by the CCTV system, pursuant to a data access request. In the access request, the data subject should provide the date, time and location of the recording to assist the school/ETB in locating images relating to that particular person. In giving the person a copy of their data, the school/ETB may provide a still/series of still pictures, a tape or disk with relevant images. However, the images of any other person appearing on the data should be obscured before the data is released to the applicant.

The CCTV system should only be accessible by the Principal or other authorised school employees who need to have access to the data (such as the Deputy Principal in the Principal's absence). An access log should be maintained by the school/ETB, stating who accessed the recordings/images, on what dates and times and for what purposes. It is important that the recordings are securely stored in a locked location and that the images are safely deleted at regular intervals. The school will need to develop a retention period that can be justified. The Data Protection Commissioner states that, "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 is retained specifically in the context of an investigation of that issue" - see [Data Protection CCTV](#). Accordingly, the retention period for CCTV images/recordings should be a maximum of 28 days, unless where the CCTV images/recordings capture issues (such as criminal behaviour or a risk to health and safety) and the CCTV images/recordings are retained to investigate that issue.

A notice informing people that CCTV is in operation should be displayed in a prominent position in areas where CCTV recordings are being made and also at the entrance to the school/ETB property. The sign should be clear and legible. The Data Protection Commissioner sets out requirements for these notices and the school's notice could state:



Warning: CCTV in operation Images are being monitored and recorded for the purposes of crime prevention, the prevention of anti-social behaviour, for the safety of our staff and students and for the

protection of school property. The system will be in operation 24 hours a day, every day. These images may be passed to An Garda Síochána. This system is controlled by [insert name of school/third party company name]. For more information, call [insert telephone number of school/third party company].”

Where the CCTV is operated or controlled by a third party (such as a commercial security company), the school must put a written data processing agreement in place with that security company. For further advice and guidance, see also [Content of Service Agreements](#).

APPENDIX 5 – CCTV Camera Locations

