St Gerald's DLS College
Policy on CCTV

Table of Contents

1.0: Introduction

Closed Circuit Television Systems (CCTVS) are installed in a number of areas around the School campus.

2.0: 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 premises under the remit of St Gerald's DLS College"

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.

3.0: Scope

This policy applies to all personnel, Schools/colleges and other education and administrative centres under the remit of St Gerald's College and relates directly to the location and use of CCTV, the monitoring, recording and subsequent use of such recorded material.

4.0: 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 visitors to its premises. The School owes a duty of care under the provisions of Health Safety and Welfare 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 particular School/centre community by integrating the best practices governing the public and private surveillance of its premises.

The primary aim of CCTV monitoring of School premises is to deter crime and vandalism and to assist in the protection and safety of the staff, students and visitors, School property

and its associated equipment and materials.

Monitoring, for security purposes 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 monitoring of political or religious activities, or employee and/or student evaluations would undermine the acceptability of the resources for use regarding critical safety and security objectives and is therefore prohibited by this policy. Information obtained through video monitoring may only be released when authorised by the Principal, following consultation with the Chairperson of the Board of Management and/or the Trustees.

CCTV monitoring of public areas, for security purposes will be conducted in a manner consistent with all existing policies adopted by the School including, Dignity at Work Policy, Codes of Practice for dealing with complaints of Bullying & Harassment and Sexual Harassment in the School, 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 the School premises, is limited to uses that do not violate the reasonable expectation to privacy as defined by law.

Information obtained in violation of this policy may not be used in a disciplinary proceeding against an employee of the School or a student.

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 Article 15 of the General Data Protection Regulation (GDPR)

5.0: Justification for Use of CCTV

General Data Protection Regulation (GDPR) require that personal date is adequate, relevant and not excessive for the purpose for which they are collected. This means that the Principal/Chairperson needs to be able to justify the obtaining and use of personal data by means of a CCTV system. A system used to control the perimeter of a building for security purposes will usually be easy to justify. Such a system will typically be intended to capture images of intruders or of individuals damaging property or removing goods without authorisation.

The use of CCTV systems in other circumstances – for example, to constantly monitor students or staff can be more difficult to justify and could involve a breach of the Data Protection Acts.

Before considering the installation of CCTV systems to other areas of the School/centre e.g. hallways, stairwells, locker areas, the Principal must demonstrate 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.

6.0: 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. Cameras placed so as to record external areas should be positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

Examples of CCTV Video Monitoring and Recording of Public Areas:

- Protection of School/College/Education & administrative centre and property building perimeter, entrances and exits, lobbies and corridors, special storage areas, laboratories, 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 gates and traffic control

- Protection of pedestrians, monitoring pedestrian and vehicle traffic activity
- Criminal investigations such as assault, robbery, burglary and theft.

7.0: Covert Surveillance

The use of recording mechanisms to obtain data without an individual's knowledge is generally unlawful. Covert surveillance is normally only permitted on a case by case basis where the data are kept for the purposes of preventing, detecting or investigating offences, or apprehending or prosecuting offenders. This provision automatically implies an actual involvement of An Garda Síochána or an intention to involve An Garda Síochána.

Covert surveillance must be focused and of short duration. Only specific (and relevant) individuals/locations should be recorded. If no evidence is obtained within a reasonable period, the surveillance should cease.

If the surveillance is intended to prevent crime, overt cameras may be considered to be a more appropriate measure, and less invasive of individual privacy. Permission of Chairperson of the Board must be obtained before considering covert surveillance.

8.0: Notification and Signage

The Principal will provide written notifications describing 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 and the Patron. Adequate signage will be placed at appropriate and prominent locations and will include wording indicating the distinct purpose the information will be used for. Appropriate locations for signage will include:

- At entrances to premises i.e. external doors and school gates
- Reception area
- At or close to each internal camera
- Under each camera indicating the purpose of:
    - To maintain good order,
    - To prevent bullying,

- To ensure the health and safety of the students and staff

9.0: Storage & Retention

The General Data Protection Regulation (GDPR) and the Data Proteciton Act 2018 states that data shall not be kept for longer than is necessary for the purposes for which they were obtained. A data controller needs to be able to justify this retention period. For a normal security system, it would be difficult to justify retention beyond a month, except where the images identify an issue – such as a forced entry situation or theft - and is retained specifically in the context of an investigation of that issue. Please see the school's data retention policy.

The storage medium should be stored in a secure environment with a log of access kept. Access should be restricted to authorised personnel. The images captured by the CCTV system should 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 of that issue. Tapes/DVDs should be stored in a secure environment with a log of access to tapes kept. Access should be restricted to authorised personnel. Similar measures should be employed when using disk storage, with automatic logs of access to the images created.

9.1: Access

Access to the CCTV system and stored images must be restricted to authorised personnel only i.e. Principal. The tapes storing the recorded footage and the monitoring equipment must be securely stored in a restricted area. Unauthorised access to that area must not be permitted at any time. The area should be locked when not occupied by authorised personnel. A log of access to tapes/images must be maintained.

9.2: Requests by An Garda Síochána

Information obtained through video monitoring may only be released when authorised by the Principal, following consultation with the Chairperson of the Board. If An Garda Síochána request CCTV images for a specific investigation, the Principal must satisfy him/herself that there is a genuine investigation underway. A request from An Garda Síochána should be in

writing on Garda headed notepaper however, for practical purposes pending receipt of the written request, a phone call to the requesting Garda's station may be sufficient, provided that he/she speaks to a member in the District Office, the station sergeant or a higher ranking officer, as all may be assumed to be acting with the authority of a District/Divisional officer in confirming that an investigation is authorised.

9.3: Access requests.

Any person whose image has been recorded has a right to be given a copy of the information recorded on request, provided such an image/recording exists i.e. has not been deleted. To exercise that right, a person must make an application in writing to the School. In certain circumstances, it will be possible to charge a "reasonable fee" to the data subject to cover administrative charges where the request involves the gathering of large amounts of data.

The school must respond to your request within one month/30days. Where the school is extending the period for replying to your request, it must inform you of any extension, and the reason(s) for the delay in responding, within one month of receiving the request.

Access requests can be made to the following address: The Principal, St Gerald's DLS College, Newport Road, Castlebar, Co. Mayo or dataprotection@geralds.ie. The School will have some grounds for refusing to grant an access request. Where a request is deemed manifestly unfounded or excessive, it can be refused.

Practically, a person should provide necessary information, 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.

In giving a person a copy of his/her data, the School may provide a still/series of still pictures, a tape or a disk with relevant images. However, other people's images will be obscured before the data are released.

10.0: RESPONSIBILITIES

The Principal of the school 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 at the school is consistent with the highest standards and protections
- review camera locations and be responsible for the release of any information or material stored in video tapes in compliance with this policy
- maintain a record of access 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
- provide a list of the CCTV cameras and the associated monitoring equipment, and the capabilities of such equipment, located in the Centre, to the BOM for formal approval
- 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 does not include mobile video equipment or hidden surveillance cameras used for authorised criminal investigations.)
- give consideration to both students and staff petitions 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/centre 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
- advise the BOM that adequate signage, at appropriate and prominent locations is

displayed as detailed above

- 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 period not longer than 28 days and will then be 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 on behalf of the BOM.
- ensure that camera control is solely to monitor suspicious behaviour and not individual characteristics
- ensure that camera control is not in breach of the intrusion on intimate behaviour by persons in public areas
- ensure that mobile video equipment will only be used for criminal investigations and with the approval of the Chairperson and the local Garda Authorities

11.0 Security Companies

Where a School CCTV system is controlled by a Security Company contracted by the School, the following applies: The School will have 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 may apply.

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 must be made aware of their obligations relating to the security of data.

12: Definitions

Definitions of words/phrases used in relation to the protection of personal data and referred to in the text of the policy;

12.1: 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.

12.2: The Data Protection Acts

The Data Protection Acts 2018 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.

12.3: 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).

12.4: 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.

12.5: Access Request

This is where a person makes a request to the organisation for the disclosure of their personal data under section 4 of the Acts.

12.6: 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.

12.7: 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.

12.8: 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 his/her employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Act places responsibilities on such entities in relation to their processing of the data.

13.0: Review

This policy is operative from September 2018. It will be reviewed by the Board of Management for subsequent years.

14.0: Ratification

This policy was ratified by the Board of Management on _____

Signed:_ Brendan Forde

Brendan Forde

Chairperson of BoM

Signed: Daniel Hyland

Daniel Hyland

Secretary of BoM

Date of next review:_____