

CCTV System Policy

1 Introduction

- 1.1 The purpose of the CCTV System Policy of Dundalk Grammar School (“the Policy”) is to regulate the management, operation and use of the closed-circuit television (CCTV) system (“the System”) at Dundalk Grammar School (“the School”). This Policy should be read in accordance with the schools’ Data Protection Policy 2024.
- 1.2 The system comprises a number of fixed and dome cameras located around the school site.
- ~~1.3~~ The Policy follows Data Protection Commissioner Guidelines and is drafted in conformity with the Data Protection Acts 1988-2003 and Data Protection Act 2018 (“the Acts”).
- 1.4 Comments from interested parties are welcome and will be considered when the policy is reviewed.
- 1.5 The System is wholly owned by the School and is not accessible remotely.

2 Objectives of the System

- (a) To protect the school properties and associated assets, including two ICT rooms;
- (b) To increase personal safety of staff, pupils and visitors and reduce the fear and incidence of crime;
- (c) To assist the school in dealing with serious breaches of school discipline¹;
- (d) To protect members of the public and private property;
- (e) To assist in identifying, apprehending and prosecuting offenders;
- (f) To support the Gardaí in a bid to deter and detect crime.

(Note: The System will not be used to monitor staff conduct or performance except where required to investigate the alleged perpetration 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 GDPR/ the Acts.
- 3.2 Cameras will be used to monitor activities within the school circulation areas and its car parks, ICT rooms and other public areas as an adequate, relevant and proportionate response to the achievement of the objectives identified under paragraph 2 above.
- 3.3 Static cameras are not to focus on private homes, gardens and other areas of private property.
- 3.4 Materials or knowledge secured as a result of the use of the System will not be used for any commercial purpose. The recorded images stored will only be released for use in the investigation of a specific crime by the Garda Síochána. Recorded images containing personal data will never be released to any third parties for any purpose that is not permitted under the Policy.
- 3.5 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.
- 3.6 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 CCTVs to inform all persons who may be deemed Data Subjects, of the operation of the System.

¹ These are defined (in school’s Code of Behaviour) as follows: (i) serious disruption or abusive behaviour to staff or other pupils (ii) violent behaviour (iii) not attending classes or leaving school premises without permission (iv) bullying of staff or pupils (v) abuse/destruction of property (vi) theft, smoking/ vaping, drinking or substance abuse.

4 Operation of the system

- 4.1 For the purposes of the Data Protection Acts 1988, 2018 the Data Controller will be the Board of Management of Dundalk Grammar School. In practice, the System will be overseen by the Headmaster, 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.
- 4.3 The Deputy Principal (or in his/her absence another designated member of staff) will ensure that the CCTV system is operational at all times.
- 4.4 Other than the Headmaster and Deputy Principal, staff designated to view recorded images for the purposes outlined in this policy include all Assistant Principals and the School Facilities Manager. This can only take place with the permission of the Headmaster or the Deputy Principal.
- 4.5 The Headmaster or the Deputy Principal may authorise staff, other than those designated above, to view recorded images where this is considered necessary to achieve the system objectives outlined above (Section 2). However such staff must be accompanied by another designated member of staff.
- 4.6 The Deputy Principal will ensure that authorised staff viewing recorded images enter a written record in the CCTV log-book. At the beginning of each academic year a report will be presented to the Board of Management outlining the number of occasions that the CCTV has been accessed and for what purpose.
- 4.7 The System will be operated 24 hours each day, every day of the year, except periods of breakdown or necessary maintenance.

5 Location of System

- 5.1 The Deputy Principal's office is where the system is installed and from where it is controlled.
- 5.2 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.
- 5.3 Access to the Deputy Principal's office will be limited to the authorised people while recorded data is being viewed.
- 5.4 During the working day when the office is not manned the system is password protected and the visual display is switched off.

6 Monitoring procedures

- 6.1 Camera operation will be maintained at all times.
- 6.2 The Monitor is installed in the Deputy Principal's office. The visual display, which is password protected, will be switched off unless it is being accessed for the purposes outlined in section 2 of this policy. The monitor will also be switched off outside office hours.
- 6.3 The Monitor shall not be used to display the image from a single camera unless the video footage is being reviewed by an authorised member of staff. The default display setting for the monitor is multiple images once accessed using a password (i.e. the simultaneous display of 16 camera images).

7 Video recording procedures

- 7.1 Recordings are initially made to a hard disk. The equipment is programmed to delete images after 28 days automatically. Data can be recorded on to a storage device (such as a USB) for specific purposes in accordance with this policy and with the authorisation of the Headmaster. Such recordings will be stored in a locked cabinet.
- 7.2 In order to maintain and preserve the integrity of the USBs used to record events from the hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:

- (i) Each USB must be identified by a unique mark.
- (ii) Before use each USB must be cleaned of any previous recording.
- (iii) The school records shall register the date and time of USB insert, including USB reference.
- (iv) A USB required for evidential purposes must be sealed, witnessed, signed by the Headmaster or delegated representative, dated and stored in a separate and secure container.
- (v) If the USB is archived the reference must be noted.

- 7.3 Following submission of a warrant or a formal written request (from a Garda of senior rank) USBs may be viewed by the Gardaí for the prevention and detection of crime. Gardaí access may be provided without such notice if this is adjudged to be warranted and in such circumstances, written official confirmation should follow on afterwards. Such access must be recorded in the CCTV Log.
- 7.4 A record will be maintained of the release or viewing of USBs to the Gardaí or other authorised persons. A register will be maintained for this purpose.
- 7.5 In respect of USBs not required to be retained for security, crime detection or other legitimate purposes, the School will ensure its best endeavours are used to dispose safely and properly of the contents of the USBs after 28 days.
- 7.6 Applications received from outside bodies (e.g. solicitors) to view or release personal data stored on USBs and held by the School will be referred to the Headmaster. In these circumstances a copy of the request will be provided as an appropriate data access request (section 11).

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 Headmaster, and may lead to disciplinary action where appropriate.
- 8.2 Any serious breach of the Policy will be immediately investigated and this may include an independent investigation to be carried out by nominees of the Headmaster.

9 Assessment of the System

- 9.1 Performance monitoring, including random operating checks, will be carried out by the Deputy Principal. A documentary record of such checks shall be maintained in the CCTV Log Book.
- 9.2 A report on the operation of the system will be presented annually to the Board of Management.

10 Complaints

- 10.1 Any complaints about the School's CCTV system should be addressed to the Headmaster.
- 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 Commission, Canal House, Station Road, Portarlington, Co. Laois, R32 AP23.

11 Access by the Data Subject

- 11.1 The Acts/ GDPR 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).
- 11.2 Requests by Data Subjects for such access should be made in writing to the Headmaster. The Board of Management may be informed of requests for access where this is deemed to be appropriate.²

² In order to facilitate the processing of access requests Data subjects are asked to provide specific details of time and location.

- 11.3 The form of access granted may consist of facilities being offered at the School premises to view the relevant personal data, in original or copy form, or the release of a copy USB storing the relevant personal data.³

12 Public information

- 12.1 Copies of the Policy will be available to the public from the School Administration Office and the School Website (<http://www.dgs.ie>).

13 Summary of Key Points

- The CCTV system is owned and operated by the school.
- The recording system will be secured at all times and not remotely accessible.
- Recording USBs will be used properly and in accordance with the Acts and indexed, stored and destroyed within a reasonable period when it is no longer reasonably necessary to retain such data.
- USBs may only be viewed by Authorised School staff, and the Gardaí.
- USBs required as evidence will be properly maintained and preserved and witnessed and packaged before copies are released to the Gardaí.
- USBs will not be made available to the media or third parties generally for commercial or entertainment use.
- USBs will be disposed of securely and content deleted.
- Any breaches of the Policy will be investigated by the Headmaster. An independent investigation will be carried out for serious breaches.
- Breaches of the Policy and remedies will be reported to the Headmaster.

³ No Data Subject can be given access to an image which includes any other Data Subject. Consequently all images which show third parties must be treated to prevent identification of any other party. Access may also be delayed where there is an ongoing investigation within the School. In any event the School will endeavour to respond to, and facilitate as appropriate, any access request within one calendar month of the date of receipt.

Signage:

CCTV signage prominently displayed round the school campus at main entrances and around the school, and ICT rooms.

