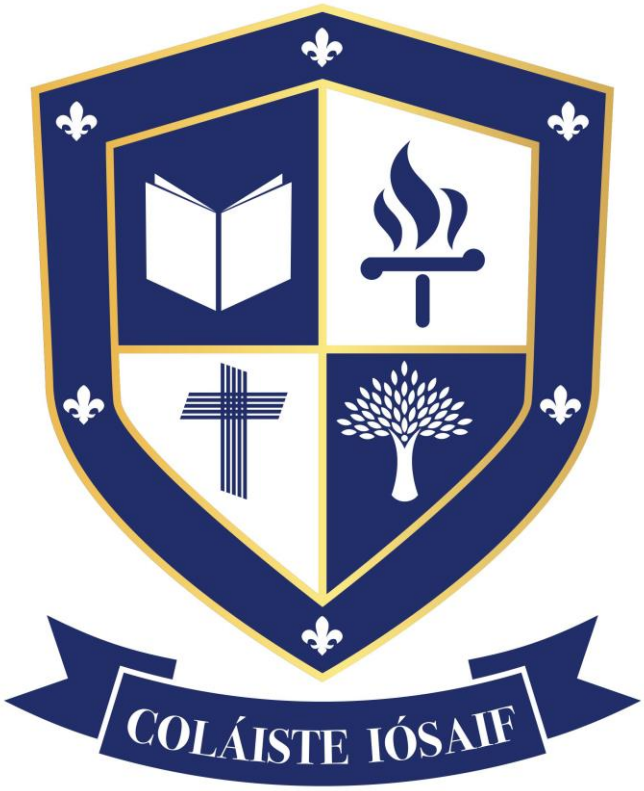
CCTV Policy



St. Joseph's, Fairview

This document is intended to provide details of the main policies of Coláiste Iósaif an Fhionnradharc in relation to anti-bullying. It is intended to help parents and guardians understand the environment and approach of the school. This document is regularly reviewed. All feedback is encouraged and welcome.

Version	Description	Authors
2021	Existing policy	Board of Management
Oct 2023	Revised version of policy	Board of Management

School Contact Details

Principal: Seán Stack

Board of Management Chairperson: James Rogan

School Phone Number: 01-8339779

Address: Coláiste Iósaif an Fhionnradharc, Fairview,
Dublin 3

CCTV System

1. Introduction

1.1 The purpose of the CCTV System Policy in Coláiste Iósaif 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 and PiR 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 and GDPR 2018.
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 (a) To protect the school buildings and their assets. (b) To increase personal safety of staff, pupils and visitors and reduce the fear and incidence of crime. (c) To protect members of the public and private property. (d) To assist in managing the school. (e) 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. (f) 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 Unless an immediate response to events is reasonably required staff must not directly focus cameras singularly at an individual, their property or a specific group of individuals, without an authorisation being obtained using the school's forms for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000.
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 shall be stored on the system's hard drive, 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 Siochana. 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.
3.5 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 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 GDPR (2018) the Data Controller will be Coláiste Iósaif. 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-today 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 The Control room will be located in the Deputy Principal's office, and may be extended at the Principal's discretion.
4.4 The system will be operated 24 hours each day, every day of the year, except for periods of breakdown or necessary maintenance.

5. Control Room

5.1 The system is situated in the DP's office. 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 Room 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 contractors before allowing access to the control room.
5.4 Emergency procedures will be used in appropriate cases to call the Emergency Services.

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 and (a) Assembly Areas (b) Corridors and Social Areas (c) Entrance doors of main school building. (d) Car park, School Driveway and other external public areas.

7. Video recording procedures:

7.1 Recordings are initially made to a drive which is located in the Control Room in the server room. The equipment is programmed to delete images after a set period of time. Data can be recorded on to zip discs for specific purposes in accordance with this policy and with the authorisation of the Principal.
7.2 In order to maintain and preserve the integrity of the drives 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 drive must be identified by a unique mark. (ii)Before use each drive must be cleaned of any previous recording. (iii)The authorised person shall register the date and time of the drive. (iv)A drive required evidential purposes must be witnessed, signed by the Authorised person, dated and stored in a separate and secure location. If a drive is not copied for the Gardai before it is transferred, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the Authorised person, dated and returned to the secure zip disc store. (v)If the drive is archived the reference must be noted.
(vi)A phone may be used to record the screen in less serious situations
7.3 Video recordings may be viewed by the Gardai for the prevention and detection of crime.

7.4 A record will be maintained of the release or viewing of drive to the Gardai or other authorised persons. A register will be maintained for this purpose.
7.5 Should a drive be required as evidence, a copy may be released to the Gardai under the procedures described in paragraph 7.1(iv) of the Policy. Drives will only be released to the Gardai on the clear understanding that the recording remains the property of the school, and both the drive 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 drive this will be produced where still available.
7.6 The Gardai may require the school to retain the stored drive for possible use as evidence in the future. Such drive will be properly indexed and properly securely stored until they are needed by the Gardai.
7.7 In respect of drive not required to be retained for security, crime detection or other legitimate purposes, the School will ensure its best endeavours are used to safely and properly dispose of the contents of the drive after 28 days, or recording period of server.
7.8 Applications received from outside bodies (e.g. solicitors) to view or release personal data stored on drive and held by the School will be referred to the Principal. In these circumstances a copy of the relevant drive 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 will be 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, Portarlington, 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 drive), 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:

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