




Erne Integrated College

CCTV Policy

February 2024

Signature of Chairperson of the Board of Governors	
Date Adopted by the Board of Governors	28 February 2024
Policy Review Date	February 2025

1 Introduction

1.1 Erne Integrated College recognises that CCTV systems can be privacy intrusive.

1.2 This policy shall be reviewed regularly and approved by the School's Board of Governors.

2 Objectives

2.1 The purpose of the CCTV system is to assist the school in reaching these objectives:

- To protect students, staff and visitors against harm to their person and/ or property;
- To protect the school buildings and assets;
- To assist in establishing cause of accidents and other adverse incidents and prevent reoccurrence.

3 Purpose

3.1 The purpose of this policy is to regulate the management, operation and use of the CCTV systems (closed circuit television) by the school.

3.2 CCTV cameras will not be installed in areas in which individuals would have an expectation of privacy such as toilets or changing facilities.

3.3 CCTV cameras are installed in such a way that they are not hidden from view. Signs are displayed where relevant, so that staff, students, visitors and other members of the public are made aware that they are entering an area covered by CCTV. The signs also contain contact details as well as a statement of purposes for which CCTV is used.

4 Statement of intent

4.1 The CCTV system will comply with the requirements both of the Data Protection Act 2018 and General Data Protection Regulations (GDPR).

- 4.2 The school will treat the systems, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Data Protection Act and GDPR.
- 4.3 Cameras have been set so far as possible to deny observation on adjacent private homes, gardens and other areas of private property.
- 4.4 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.
- 4.5 The CCTV system have been deployed to give maximum effectiveness and efficiency however it is not possible to guarantee that the systems will cover or detect every single incident taking place in the areas of coverage.
- 4.6 Signs will be clearly visible on the site and make clear who is responsible for the equipment.
- 4.7 CCTV images are not retained for longer than necessary, taking into account the purposes for which they are processed. Data stored is automatically overwritten by the system after a period of 28 days.

4 System Management

- 5.1 Access to the CCTV systems and data shall be password protected and will be kept in a secure area.
- 5.2 The CCTV systems are administered and managed by the school C2k manager who acts as Systems Manager and is responsible for restricting access, in accordance with the principles and objectives expressed in this policy. The Systems Manager will be assisted by the Building Supervisor and ICT technician in the management and operations of the systems.
- 5.3 The system and the data collected will only be available to the System Manager and designated assistants.
- 5.4 The CCTV systems are designed to be in operation 24 hours each day, every day of the year, though the school does not guarantee that it will be working during these hours.
- 5.5 Where a person, requests access to the CCTV data or system, the Principal must satisfy him/ herself of the identity and legitimacy of purpose of any person making such request. Where any doubt exists access will be refused. A third

party making a request will be liable to any costs incurred if access to the data is approved by the Principal.

6 Downloading captured data onto other media

6.1 In order to maintain and preserve the integrity of the data (and to ensure its admissibility in any legal proceedings) any download target device used to record data from the CCTV storage device must be prepared in accordance with the following procedures:

- (a) Each downloaded data must be identified by a unique mark recorded in the CCTV storage device;
- (b) Before downloading data from the CCTV system storage device, the download target device must be cleaned of any previous recording;
- (c) Downloaded data required for evidential purposes must be sealed, witnessed and signed by the System Manager, then dated and stored in the school safe. If downloaded data is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed and signed by the System Manager, then dated and returned to the school safe;
- (d) If downloaded data is put onto a storage device, the device will be encrypted and password protected.

6.2 Images may be viewed by the police for the prevention and detection of crime and by the Systems Manager and their assistants, the Principal and other authorised senior leaders.

6.3 A record will be maintained and held in the school safe of the release of any downloaded data to the police or other authorised applicants.

6.4 Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the downloaded data (and any images contained thereon) remains the property of the school, and downloaded data (and any images contained thereon) are to be treated in accordance with data protection legislation.

6.5 The school also retains the right to refuse permission for the police to pass the downloaded media (and any images contained thereon) to any other person.

On occasions when a court requires the release of downloaded data this will be produced from the school safe.

- 6.6 The police may require the school to retain the downloaded data for possible use as evidence in the future. Such downloaded data will be securely stored in the school safe until they are needed by the police.
- 6.7 Applications received from third parties (e.g. solicitors or parents) to view or release images will be referred to the school's Principal and a decision made in consultation with the school's C2k Manager.

7 Complaints about the use of CCTV

- 7.1 Any complaints in relation to a school's CCTV system should be addressed to the Principal.
- 7.2 The Principal will assess the complaint and advise the complainant accordingly.

8 Request for access by the data subject

- 8.1 The Data Protection Act 2018 provides data subjects – those whose image has been captured by the CCTV system and can be identified - with a right to access such data held about themselves.
- 8.2 Requests for such data should be made to the School Principal.