# CCTV POLICY & PROCEDURES

INSTITUTE FOR EDUCATION,
MARTIN LUTHER KING ROAD,
PEMBROKE PBK 1990

## 1. Scope

The Institute for Education within the Ministry for Education and Employment deals with personal data by means of CCTV camera/s and abides by this policy with regards to the data processed by this means.

## 2. Background information

The data controller for the Ministry for Education and Employment under which the Institute for Education falls is the Ministry's Permanent Secretary.

## 3. Introduction

3.1 The purpose of this Policy is to regulate the management, operation and use of the Closed-Circuit Television (CCTV) system at the Institute for Education, Martin Luther King Road, Pembroke. Cameras are used to monitor activities within the Institute building and on its site, to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of the Institute, together with its staff and visitors.

3.2 CCTV monitoring and recording systems will only be installed in or on the Institute's property after that this has been reviewed and approved by the Institute's Administration.

3.3 The system comprises a number of fixed and fully functional cameras located in the building and externally around the Institute's perimeter. These are monitored by the Manager – System Administrator.

3.4 The Institute's use of CCTV complies with the requirements of the Data Protection Act 2001 - PART III – Requirements and Criteria for Processing.

3.5 This policy document will be subject to review bi-annually to include consultation as appropriate with interested parties.

3.6 The CCTV system is owned by the Institute for Education.

3.7 Independently installed and operated CCTV systems will not be permitted and where found, actions will be taken to close these systems down.

## 4. Objectives of the CCTV policy

### 4.1 The objectives of the CCTV Policy are to:

- Protect the Institute's property.
- Ensure a safer environment within the Institute.
- Support the Police in a bid to deter and detect crime, by providing evidence in support of an enquiry or prosecution.

## 5. Operation of the CCTV system

### 5.1 Management of the system

5.1.1 The CCTV operating system will be administered and managed by the Institute.

5.1.2 The day-to-day management will be the responsibility of the Institute for Education (IfE) during the working week, outside normal hours and at weekends.

5.1.3 All cameras are monitored on the respective site where they operate, through the NVR which is found in the administration building.

5.1.4 The CCTV system will be operated 24 hours a day, 365 days of the year.

5.1.5 Emergency procedures will be used when it becomes necessary to call the Emergency Services.

5.1.6 Warning signs will be prominently placed in all areas covered by the Institute's CCTV cameras.

### 5.2. System control - Monitoring procedures:

5.2.1 On a regular basis the system will be checked by the Manager – System Administrator to confirm the efficiency of the system, ensuring that:

- The cameras are functional
- The equipment is properly recording

5.2.2 Access to the CCTV System will be strictly limited to the Manager – System Administrator and the IfE Data Protection Officer. Unauthorised persons are not permitted to view live or pre-recorded footage.

5.2.3 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

Recording is carried out on digital data apparatus which is located within the Administration Building.

Recorded data will only be released to the competent authorities in respect to the investigation of a specific crime. Recorded data will never be released for other intents or purposes.

Processing for a distinct activity that is not compatible with the original reason for which cameras were installed will only be done if prior notice is given to the data subjects.

In view of Chapter II (Article 5) of the GDPR , the Data Controller justifies the use of a CCTV Surveillance Camera system for the above-mentioned purpose. The

recognisable images captured by the cameras will be processed adequately, and in a relevant manner and shall be necessary in relation to the purposes of the processing as per Chapter II Article 6 of the GDPR.

### 5.3 Exemptions:

5.1 The CCTV system is designed to ensure maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

### 5.4 Retention and disposal of material:

Data disks will be disposed of by a secure method.

Footage will be stored on data recorder hard drives for up to 15 days.

Footage will only be stored on data disks if footage is requested by competent authorities in the process of detecting crime and in the prosecution of offenders.

## 6. DIGITAL RECORDING PROCEDURES

### 6.1 Rules for retention of data

6.1.1 In order to maintain and preserve the integrity of the Network Video Recorder (NVR), hard disks used to record events from the CCTV cameras and the facility to use them in any future proceedings, the following procedures for their use and retention of data must be strictly adhered to:

6.1.2 The NVR must be identified by a unique mark or serial number.

6.1.3 The NVR must be kept in a secure location with access restricted to authorised staff.

6.1.4 The system needs to be checked daily to ensure the system is operational.

A disk required for evidential purposes must be of the CD-R type only, disks will be provided in pairs each carrying an identical identification number, one a Master Disk to be retained by the Institute, the other a Copy which can be released to competent authorities on presentation of a signed data access request form.

The disk should be loaded with the required CCTV data and viewer programme; identical information should be loaded on both Master and Copy disks.

Each disk should be sealed in its own case, the Master Copy should be kept securely. The Copy disk could be handed to the authority making the request on production of some legal document, such as an ID card.

The record sheet should then be completed and the Copy disk signed for and counter signed by an Institute's representative.

### 6.2 Dealing with official requests: use of CCTV in relation to criminal investigations:

6.2.1 CCTV recorded images may be viewed by the Police for the prevention and detection of crime, authorised staff at the Institute for Education, for supervisory purposes, discipline reasons or authorised demonstration and training.

6.2.2 A record will be maintained of the release of Data on Disk to the Police or other authorities. A register will be available for this purpose.

6.2.3 Viewing of CCTV images by the Police must be recorded in writing and entered in the log book. This will be under the management of an Institute's Data Protection Officer. Requests by the Police can only be actioned under Subsidiary Legislation 440.06 of the Data Protection Act 2001 - Chapter 440.

6.2.4 Should a disk be required as evidence; a copy may be released to the Police under the procedures described in the Subsidiary Legislation 440.06. Disks will only be released to the Police on the clear understanding that the disk remains the property of the Institute, and both the disk and information contained on it are to be treated in accordance with this policy.

6.2.5 The Institute retains the right to refuse permission for the Police to pass to any other person the disk or any part of the information contained therein.

6.2.6 The Police may require the Institute to retain the stored disk(s) for possible use as evidence in the future. Such disk(s) will be properly indexed and securely stored until they are needed by the Police.

## 7. BREACHES OF THE POLICY (INCLUDING BREACHES OF SECURITY)

7.1 Any breach of the Policy by authorised staff, will be initially investigated by the Institute's top-level management, in order for them to initiate the appropriate disciplinary action.

7.2 Any serious breach of this policy will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

## 8. ASSESSMENT OF THE SCHEME

8.1 Performance monitoring, including random operating checks, may be carried out.

## 9. COMPLAINTS

9.1 Any complaints about the Institute's CCTV system should be addressed to the Data Protection Officer, Institute for Education, Martin Luther King Road, Pembroke; PBK1990.

9.2 Complaints will be investigated in accordance with Section 5 of this policy.

## 10. ACCESS BY THE DATA SUBJECT

10.1 The Data Protection Act provides Data Subjects (individuals to whom "personal data" relate) with a right to access data held about themselves, including that obtained by CCTV.

10.2 The data protection officer representing the Institute for Education may be contacted as follows for any requests for information, including Data Subject Access Requests:

**ADDRESS**
The Data Protection Officer
Institute for Education
Martin Luther King Road
Pembroke.
PBK1990

**Telephone**
(+356) 2598 2003

**Email**
anthony.satariano@ilearn.edu.mt

Data subjects will have a right of access to data being processed as per Chapter II (Article 15) of the General Data Protection Regulation. (Please refer to section relating to Access, below). Data subjects are also hereby informed of their right to lodge a complaint with the Information and Data Protection Commissioner.

The Information and Data Protection Commissioner may be contacted as follows:

**ADDRESS**
Information and Data Protection Commissioner
Level 2, Airways House
High Street
Sliema. SLM 1549

Malta

**Telephone**
(+356) 2328 7100

**Email**
idpc.info@gov.mt

## 11. Related Policies

- General Data Protection Regulation (GDPR) (EU) 2016/679
- Data Protection Act (CAP 440)

## 12. Version history

| Version | Date | Changes Done |
|---|---|---|
| 1.0 | 08/05/2018 | Initial Release |
| | | |