CCTV Policy and Procedures

Version 1.2

Policy Author	Geoffrey Tanti	**Designation**	Senior Manager IT	**Dept.**	IT Dept.
Policy Reviewer	Anthony Satariano	**Designation**	Head QA	**Dept.**	QA Dept
Policy Approver	N/A	**Effective Date**	08/5/2018		

1 Scope

The Institute for Education (IfE) 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 of the IfE falls is the Chief Executive Officer.

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 IfE, Martin Luther King Road, Pembroke. Cameras are used to monitor activities around the IfE's perimeter, for the purpose of securing the safety and well-being of both the IfE's building and its staff / visitors.

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

3.3 The system comprises a number of fixed and fully functional cameras located around the IfE's building perimeter. These are monitored by the Senior Manager IT and Security.

3.4 The IfE's use of CCTV complies with the requirements of Data Protection Legislation.

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 IfE.

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 IfE's property.
- Ensure a safer environment within the IfE.
- 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 IfE.

5.1.2 The day-to-day management will be the responsibility of the 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 IfE'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 Security, the CEO and the Senior Manager IT. 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.

5.2.4 Recording is carried out on digital data apparatus.

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

5.2.6 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.

5.2.7 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 Retention and disposal of material:

5.3.1 Data disks will be disposed of by a secure method.

5.3.2 Footage will be stored on data recorder hard drives for up to 7 days.

5.3.4 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.

6.1.5 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 IfE, the other a Copy which can be released to competent authorities on presentation of a signed data access request form.

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

6.1.7 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.

6.1.8 The record sheet should then be completed, and the Copy disk signed for and counter signed by an IfE'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.

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 IfE's Data Protection Officer. Requests by the Police can only be actioned under Subsidiary Legislation 586.08 of the Data Protection Act.

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 586.08. Disks will only be released to the Police on the clear understanding that the disk remains the property of the IfE, and both the disk and information contained on it are to be treated in accordance with this policy.

6.2.5 The IfE 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 IfE 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 IfE'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.

7.3 Any data breaches arising from breaches to this policy, will be notified to the Data Protection Supervisory Authority (the Information and Data Protection Commissioner) as indicated in terms of Article 33 of the General Data Protection Regulation.

8 Assessment Of The Scheme

8.1 Performance monitoring of the CCTV system, including random operating checks, may be carried out from time to time.

9 Complaints

9.1 Any complaints about the IfE's CCTV system should be addressed to the Data Protection Officer, Institute for Education, Martin Luther King Road, Pembroke; PBK1990 or by sending an email on ife.dp@ilearn.edu.mt .

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 Legislation 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 IfE 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
ife.dp@ilearn.edu.mt

10.3 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.

10.4 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

- Data Protection Act (CAP 586)
- General Data Protection Regulation (GDPR) (EU) 2016/679

12 Version history

Originator	Version	Date	Changes Done
IT Dept.	1.0	08/05/2018	Initial Release
QA Dept.	1.1	09/11/2020	Revised after feedback from IDPC
QA Dept	1.2	18/04/2023	Updated articles 1, 2, 5.2 and 10.