

# **CCTV Policy St. Louis Community School**

## **1. POLICY STATEMENT**

1.1 Closed Circuit Television (CCTV) is an increasing feature of our everyday lives. It can, and is, used for a variety of reasons and has been regulated in accordance with the Data Protection Acts 1988 – 2018.

1.2 This policy is designed to inform staff, students and the public about the safeguards in place with regard to the operation of and access to the CCTV systems and the resultant images in the school.

## **2. PURPOSE**

2.1 The CCTV systems within and on the grounds of St. Louis Community School will monitor the interior/exterior of buildings, car parks, and specific school locations.

2.2 Areas covered by surveillance cameras will be those most susceptible to unauthorised activities or inappropriate behaviours. The cameras are there for the deterrence of inappropriate behaviours or crime against an individual's safety, individual's and school property, in vehicles and on the premises.

2.3 CCTV in itself does not offer protection but rather deterrence.

## **3. SCOPE**

3.1 This Policy applies to the premises and grounds of St. Louis Community School.

## **4. LEGISLATION/OTHER RELATED POLICIES**

A. Data Protection Acts 1988-2018

B. School Data Protection Policy

C. School Data Subject Access Request Procedure contained in Appendix 4 of the School Data Protection Policy.

## **5. ROLES AND RESPONSIBILITIES**

- 5.1 It is the responsibility of the school principal to monitor this policy and ensure it is implemented in the school.
- 5.2 The school principal and Deputy Principal will be the responsible persons for the management of CCTV equipment and the availability of recordings/images. The school principal cannot release/access CCTV footage except on the expressed request of a data subject captured in the footage.
- 5.3 All employees must adhere to the relevant parts of this policy.
- 5.4 Data Subject Access Requests for access to recordings/images will be dealt with by the school principal who will coordinate with the Clerical Officer.

## **6. SITING OF CAMERAS AND SIGNAGE**

### 6.1 Siting

- 6.1.1 It is essential that the surveillance equipment is sited in such a way that it only monitors those areas intended to be covered by the equipment.
- 6.1.2 If it is not possible to restrict coverage, the owner of the property or space being overlooked should be consulted. If cameras are adjustable by the operators, this should be restricted so that it is not possible to manipulate them to overlook areas not intended to be covered. Operators should be trained in recognising privacy implications.

## 6.2 Signage

6.2.1 It is essential that legible “CCTV RECORDING IN USE” signs are displayed in a prominent place where they will be clearly seen by staff, students and the public. The signs should contain the following information:

- A. Identity of the organisation responsible for the surveillance
- B. Purpose for the surveillance
- C. Contact details

## 7. QUALITY OF THE IMAGES

7.1 It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose/s for which they are intended.

7.2 The equipment and recording media should be maintained on a regular basis to ensure the quality of the images is upheld.

## 8. RETAINING INFORMATION AND PROCESSING IMAGES

8.1 It is important that images are not retained for longer than is considered necessary for the purpose for which they were processed. While images are retained, it is essential that their integrity is maintained, for both evidential purposes and to protect the rights of those individuals captured in the images.

8.2 Images should not be retained for longer than 28 days unless they are required for evidential purposes in legal proceedings. Under these circumstances, the information should be retained securely and clearly marked as to why it is being retained for a period exceeding 28 days.

## 9. ACCESS TO THE IMAGES

9.1 It is important that access to, and the disclosure of, images to third parties is strictly controlled and documented. This is to ensure that the rights of the individual are maintained and that the chain of evidence remains intact should the images be required for evidential purposes.

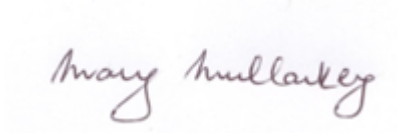
## 9.2 Data Subject Access Requests

- 9.2.1 Under Data Protection legislation, an individual has the right to view personal information held about them by an organisation. The school principal will coordinate with the Clerical Officer, or other relevant professional, to arrange for the copying of or on site viewing of the recording, to satisfy the request. The images of identifiable 3rd party individuals also captured in the CCTV footage may have to be redacted to protect the data protection rights of those individuals. The School Data Subject Access Request Procedure shall apply.
- 9.2.2 In addition, the following should be logged:
- A. Details of the image disclosed i.e. the date, time and location of the image the reason for the disclosure
  - B. Whether any images were disguised/blurred to prevent identification of individuals other than the data subject
- 9.2.3 If it is not possible to disguise images, an external company or other relevant professional may be called in to facilitate this. This will need to be logged.
- 9.2.4 Requests will not be complied with if insufficient details are supplied relating to the date and time of the recording. A letter must be sent to the requester advising them of this.
- 9.2.5 If the data subject wishes to view the images on site, as opposed to a copy being sent, the viewing should take place in a closed office with only the relevant individuals present.

## 9.3 Garda Requests

- 9.3.1 In line with the Data Protection Acts 1988- 2018, An Garda Síochána are entitled to view personal information about individuals if it is for the following purposes:
- A. For the prevention or detection of crime
  - B. The apprehension or prosecution of offenders
  - C. Required urgently to prevent injury or other damage to the health of a person or serious loss of or damage to property,
  - D. Required by or under any enactment or by a rule of law or order of a court
- 9.3.2 Requests must be made on the official Garda Data Protection form and passed to the Principal.
- 9.3.3 Actions will be logged as per the Subject Access guidance in Section 9.2 above. Should information be required to be retained for evidential purposes, procedures detailed in Section 8.2 should be followed.

**Signed: Chairperson, Board of Management**

A handwritten signature in cursive script, reading "Mary Hurlankey". The signature is written in a dark ink on a light-colored background.

**Date: 3.5.2023**