CCTV Policy
February 2020

Scoil Mhuire
St. Patrick's Street, Trim,
Co. Meath, C15 FF67.

T: (046) 94 31439
E: info@scoilmhuiretrim.ie

CIRCULATION SHEET

Client	Scoil Mhuire
Project Title	Scoil Mhuire GDPR Project 2020
Document Title	CCTV Policy

Revisions				
Rev	**Status**	**Approved By**	**Office of Origin**	**Issue Date**
R01	Release	Ark Services W: www.arkservices.ie	Cork	February 2020

Circulation			
Name	**Organisation**	**Issue Date**	**Method**
Principal	Scoil Mhuire	February 2020	Email

TABLE OF CONTENTS

1 Introduction 4

2 Data Protection Policy 4

2.1 GDPR Awareness 4
2.2 Balance of Rights 4
2.3 Lawful Processing Criteria 4

3 Responsible Person Contact Details 4

4 GDPR Principles 5

4.1 Principle 1: Lawfulness, fairness and transparency 5
4.2 Principle 2: Purpose Limitation 5
4.3 Principle 3: Data Minimisation 5
4.4 Principle 4: Data Accuracy 5
4.5 Principle 5: Storage Limitation 5
4.6 Principle 6: Integrity & Confidentiality 5
4.7 Principle 7: Accountability 5

5 Responsibilities 6

5.1 Board of Management 6
5.2 Principal 6
5.3 Deputy Principal 6

6 Data Protection Impact Assessment (DPIA) 7

7 Justification for the use of CCTV 7

8 Location of CCTV Cameras 7

9 Covert Surveillance 8

10 Notification and Signage 8

11 Management, Control and Access 8

12 Requests by An Garda Síochána: 9

13 Retention of Recordings 9

14 Security Companies 9

15 Review 9

1 Introduction

This CCTV Policy has been prepared for the use of CCTV at Scoil Mhuire. The purpose of the Policy is to ensure that data subject's rights and freedoms are not overridden by the use of CCTV at the school.

2 Data Protection Policy

2.1 GDPR Awareness

The Data Protection Policy & the Data Privacy Impact Assessment should be referred to when consulting this document. Scoil Mhuire will ensure that management and staff are aware of GDPR and are trained appropriately to their duties in respect of processing of personal data as per this data protection policy. The training and awareness programme will consist of:

- Briefing to all staff;
- A general email to all staff with the Data Protection Policy;

2.2 Balance of Rights

In using personal data for the operation of the school, we will ensure that we will only use a subject's data if the subject's rights do not outweigh our lawful basis in using that data.

The balance will be assessed by first checking that we have a lawful basis for using the data, and then evaluating whether disproportionate financial, reputational or social harm could be caused to the individual through our use of their data. We will achieve this on an ongoing basis via the Data Protection Policy and Record of Processing methods already explained in the Data Protection Policy.

2.3 Lawful Processing Criteria

Scoil Mhuire processes personal data in the pursuance of several lawful processing criteria. In all cases we examine the balance of rights with respect to the use of personal data. It is our objective to align our activities with the rights of the data subject, such that our use of their data is beneficial to the data subject and that any inconvenience or risk to the data subject is minimal in comparison with the benefits there from. We have established our lawful processing criteria in the Data Map & Processing Activities outlined in the Data Protection Policy.

3 Responsible Person Contact Details

Below are the contact details of the person most qualified to respond to questions regarding this Privacy Impact Assessment.

Title: Principal
Address: Scoil Mhuire, St. Patrick's Street, Trim, Co. Meath, C15 FF67.
Telephone: (046) 94 31439

4 GDPR Principles

4.1 Principle 1: Lawfulness, fairness and transparency

Scoil Mhuire believes in operating our school fairly and ethically and this will extend to all personal data held for those purposes. Subjects will be informed when data is being collected, and at the same time informed what we will use that data for. We will ensure that appropriate technical and organisational measures are in place to secure that data.

Collection and processing of data will be transparent. Advisory notices and privacy statements relating to data rights will be published as appropriate in plain English and will be structured where relevant to improve accessibility of this information to data subjects. Persons will be clearly advised of their rights also.

4.2 Principle 2: Purpose Limitation

Personal data collected by Scoil Mhuire will be processed only for the purpose for which it was collected. In the event that this purpose should change, data subjects will be informed within the 30-day regulatory period and consent sought for the change.

4.3 Principle 3: Data Minimisation

Scoil Mhuire will collect only the minimum quantity of personal data to carry out a particular task. Where appropriate, potential data subjects will be requested not to provide unwanted or inappropriately sensitive personal information.

4.4 Principle 4: Data Accuracy

Scoil Mhuire will make every effort to ensure that subjects' information is accurate and up to date. Scoil Mhuire will endeavour to ensure via appropriate levels of staff training that it is transcribed accurately. If it is not possible for subjects to correct their data personally, data can be corrected by contacting Reception.

4.5 Principle 5: Storage Limitation

Scoil Mhuire will store and retain personal data only while there is a valid and lawful basis to do so. Personal information will be deleted when it is no longer required for the purposes for which it was collected.

Where systems do not allow deletion of all records relating to an individual, records will be anonymised by replacing personal information fields with substituted generic text.

4.6 Principle 6: Integrity & Confidentiality

Personal Data shall be processed securely i.e. in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage. Scoil Mhuire will use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

4.7 Principle 7: Accountability

Scoil Mhuire is responsible for, and is able to demonstrate compliance with GDPR. This means Scoil Mhuire will demonstrate that these Data Protection Principles (as outlined here) are met for all Personal Data for which it is responsible.

5 Responsibilities

5.1 Board of Management

- Approve the CCTV Policy;
- Provide adequate resources to ensure that an appropriate CCTV system can be procured, operated and maintained;

5.2 Principal

- Ensure that the use of CCTV systems is implemented in accordance with the policy set down by Scoil Mhuire;
- Oversee and coordinate the use of CCTV monitoring for safety and security purposes within the school;
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy;
- Ensure that the CCTV monitoring at the school is consistent with the highest standards and protections;
- Review camera locations and be responsible for the release of any information or material stored in video tapes in compliance with this policy;
- Maintain a record of the release of tapes or any material recorded or stored in the system;
- Ensure that monitoring recorded tapes are not duplicated for release;
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally;
- Provide a list of the CCTV cameras and the associated monitoring equipment, and the capabilities of such equipment, located in the School, to the Board of Management for formal approval;
- Approve the location of temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events. NOTE: (Temporary Cameras does not include mobile video equipment or hidden surveillance cameras used for criminal investigations.);
- Give consideration to both pupils and staff petitions regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment;
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the centre and be mindful that no such infringement is likely to take place;
- Ensure that adequate signage, at appropriate and prominent locations is displayed.
- Ensure that on receipt of a valid subject access request, that still images are provided that redact the faces of other others (not involved directly in the incident) to protect their identity.

5.3 Deputy Principal

- Ensure that the use of CCTV systems is implemented in accordance with the policy set down by Scoil Mhuire;
- Assist the Principal and coordinate the use of CCTV monitoring for safety and security purposes within the school;
- Review camera locations and be responsible for the release of any information or material stored in video tapes in compliance with this policy;
- Maintain a record of the release of tapes or any material recorded or stored in the system;
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the centre and be mindful that no such infringement is likely to take place;
- Ensure that on receipt of a valid subject access request, that still images are provided that redact the faces of other others (not involved directly in the incident) to protect their identity.

6 Data Protection Impact Assessment (DPIA)

Article 35.1 of the General Data Protection Regulations makes reference to the mandatory requirement for a Data Protection Impact Assessment (DPIA):

"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."

CCTV systems are considered 'high risk' particularly in Article 35.1(c): "a systematic monitoring of a publicly accessible area on a large scale"

The appropriate time to carry out a CCTV Data Protection Impact Assessment (DPIA) is prior to the procurement of, or installation of the CCTV system or camera(s). Prior to the introduction of the GDPR, DPIA's were discretionary, however from 25th May 2018, it is mandatory to carry out a DPIA on all installations.

Readers should refer to the school's DPIA where we have demonstrated:

- strong justification for the installation of the CCTV system/camera(s);
- consideration has been given to the privacy rights of the data subject with regard to the proposed location of the camera(s);
- consideration has been given to other appropriate security measures e.g. alarm systems, coded entry or swipe cards;
- the data subjects occupying the building have been notified of the proposed system/camera and given an opportunity to voice any concerns;
- careful consideration has been given to the security and management of the system within the School and externally if a contracted company is used.

7 Justification for the use of CCTV

The school is obliged under the GDPR, to ensure that data collected by CCTV systems is adequate, relevant, not excessive and only used for the purposes for which the data was collected. As per the General Data Protection Regulations, the school is able to justify the installation of CCTV systems and cameras on our premises. The justifiable reason for installation does indeed outweigh any consideration given to other less intrusive methods of managing any ongoing issue.

8 Location of CCTV Cameras

The school has endeavoured to select locations which are the least intrusive to the data subjects occupying the building. The installation of CCTV cameras in areas where individuals would have a reasonable expectation of privacy have also been considered e.g. CCTV camera have not been installed in changing facilities, toilets etc.

CCTV systems will not normally be used to monitor day-to-day staff/student classroom activity.

External cameras have been positioned in such a way as to prevent or minimise the recording of passers-by or the privacy rights of neighbouring private properties. The CCTV cameras will only capture images within the perimeter of the school premises.

9 Covert Surveillance

The school will not engage in covert surveillance of data subjects. Data subjects will be informed at all times through policies, privacy notices and signage on the sound legal basis for the CCTV monitoring.

Where An Garda Síochána requests to carry out covert surveillance on the school premises, such covert surveillance may require the consent of a Judge. Accordingly, any such request should be made in writing and the school will seek legal advice where necessary.

10 Notification and Signage

The Principal will provide a copy of CCTV Policy and CCTV Privacy Notice on request to staff, students, parents and visitors to the school premises. The CCTV Policy and CCTV Privacy Notice describes the purpose of the CCTV monitoring, the rights of the Data Subject with regard to the monitoring, and contact details for those wishing to access more information.

Signage shall be placed internally in each premises near to where CCTV cameras are sited to inform data subjects that CCTV is in operation in that area. More extensive external signage shall also be prominently displayed on entrance to the school property. This signage shall include a statement that CCTV is in operation as well as a contact (such as a phone number) for persons wishing to discuss this processing, the specific purpose for the CCTV should also be displayed.

Appropriate locations for signage will include:

- Entrances to premises e.g. external doors, walls and school gates or any highly visible appropriate area;
- Reception area;
- Close to each internal camera;

11 Management, Control and Access

The CCTV system is located in the Principal's Office - a secure office where monitoring screens and recorded footage is securely held.

- The office is locked when not occupied by authorised personnel;
- Unauthorised access to the monitoring screens or footage is not permitted;

In relevant circumstances, CCTV footage may be shared with certain other bodies/agencies where the school is required to do so.

Under the GDPR, the school - as part of a valid Subject Access Request, is obliged to provide data subjects with a copy of their personal data on request. If the requested data are CCTV recordings, the school reserves the right to release this either (a) in soft copy footage, or (b) in still images (photos) at a rate of one photograph per second of video.

If the CCTV footage includes images of other people, their images will be pixilated or otherwise blanked out. Data Access Requests for CCTV footage should be notified immediately to the Principal who will examine the content of the request, and advise on any further steps e.g. the requirement for pixilation of the footage.

12 Requests by An Garda Síochána:

Information obtained through video monitoring may only be released when authorised by the Principal, following consultation with the Board of Management.

If An Garda Síochána request CCTV images for a specific investigation, An Garda Síochána may require a warrant and accordingly any such request made by An Garda Síochána should be made in writing and the school will immediately seek legal advice.

There is a distinction between a request by An Garda Síochána to view CCTV footage and to obtain/download copies of CCTV footage. In general, An Garda Síochána making a request to simply view footage on the premises would not raise any specific concerns from a data protection perspective.

13 Retention of Recordings

The retention period for CCTV footage is 28 days. Footage will not be retained by the school for longer than 28 days, unless it is required as part of an ongoing investigation or Data Access Request.

14 Security Companies

Security companies that install and service cameras on behalf of the school are considered to be "Data Processors". As data processors, they operate under the instruction of data controllers (the school).

The school is required to have a Data Processing Agreement in place with any CCTV security company contracted to manage the CCTV systems in place in the school.

This agreement details the areas to be monitored, how long data is to be stored, what the security company may do with the data; what security standards should be in place and what verification procedures may apply.

The written contract also states that the security company will give the school all reasonable assistance to deal with any data access request made under the GDPR which may be received by the school within the statutory time-frame (generally one month).

Under GDPR, Contracted CCTV companies, as data processors, are required to have appropriate security measures in place to prevent the unauthorised access, alteration, disclosure, or destruction of the data, and secure technical measures in place to protect against any unlawful forms of processing. Employees of the CCTV security company must be made aware of their data protection obligations when processing the data.

15 Review

The policy will be reviewed and evaluated from time to time. On-going review and evaluation will take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, An Garda Síochána, Department of Education and Skills, Audit units (internal and external to the school), national management bodies, legislation and feedback from parents/guardians, students, staff and others.

Adopted at the Board of Management meeting on the 26th June 2020. Implementation of the policy will be monitored by the Principal of the school.