CCTV Policy

Of

Jesus & Mary Secondary School,

Gortnor Abbey

School Patrons: Le Chéile Schools Trust clg.

Signed: _____
(Chairperson of Board of Management)

Signed: _____
(Principal)

Date: 8/6/26

Reviewed January 2025
Reviewed June 2026

CCTV Policy

Jesus & Mary Secondary School, Gortnor Abbey
Gortnor Abbey, Crossmolina, Co. Mayo.
T: 096 31194
E: office@gortnorabbey.ie

Issued By
The Ark HQ™

Date Issued
January 2025

CCTV Policy

Document Title

CCTV Policy

Revisions

No.	Status	Author(s)	Office	Issue Date
Rev 01	Release	The Ark HQ™	Cork	January 2025

Circulation

Position	Office	Issue Date	Method
Senior Management	Jesus & Mary Secondary School, Gortnor Abbey	January 2025	Email
Board of Management	Jesus & Mary Secondary School, Gortnor Abbey	January 2025	Email
Staff	Jesus & Mary Secondary School, Gortnor Abbey	January 2025	Email

Table of Contents

1. Scope 4
2. GDPR Awareness 4
3. Balance of Rights 5
4. Lawful Processing Criteria 5
5. Responsible Person Contact Details 5
6. Data Protection Impact Assessments 6
7. GDPR Principles 7
8. Responsibilities – Board of Management 8
9. Responsibilities – Senior Management 8
10. Purpose of CCTV 9
11. Justification for the use of CCTV 9
12. CCTV Cameras 10
13. Covert Surveillance 10
14. Notification & Signage 11
15. Management, Control & Access 11
16. Access Requests by Third Parties 12
17. Retention of Recordings 13
18. Security Companies 13
19. Review 14
21. CCTV Policy Acknowledgement 15

1. Scope

This CCTV Policy has been prepared for the use of CCTV at Jesus & Mary Secondary School, Gortnor Abbey. 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.

- The Board of Management is required to maintain a secure, safe and operational environment for the school community and its visitors. This Policy is designed to assist the school with this responsibility in addition to the achievement of other important objectives such as the protection of school property and assets.
- This Policy applies to teaching staff, non-teaching staff, volunteers, students, parents/carers, contractors and visitors to the School, including members of the public.
- The provision of CCTV within a school must respect the highest legal and ethical standards. Recognisable images captured by CCTV systems constitute personal data and are subject to the provisions of all relevant data protection legislation, including the General Data Protection regulation (GDPR) and the Data Protection Act 2018, as well as the provisions of other relevant regulations and legislation.
- The School's Data Protection Policy governs all processing of personal data associated with the operation of CCTV system within the School.
- Use of the CCTV system must be consistent with all other policies implemented by the School, including, for example the Anti-Bullying Policy, the Harassment and Sexual Harassment Policy, and the Code of Behaviour.
- As a workplace and as a learning environment, the school must offer an appropriate level of privacy and safety to employees, students and the wider community. This means, for example, that any intrusion upon normal staff and student activities should be minimal. A set of robust standards and safeguards inform the school's implementation and day to day operation of CCTV.
- This Policy will be reviewed and evaluated from time to time. Such review and evaluation will take cognisance of information and guidelines issued by relevant bodies (such as the Data Protection Commission, An Garda Síochána, Department of Education, national management bodies etc) as well as feedback received from parents/guardians, students, staff and others.

2. GDPR Awareness

The Data Protection Policy & the Data Privacy Impact Assessment should be referred to when consulting this document. Jesus & Mary Secondary School, Gortnor Abbey 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 policy.

3. 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 CCTV Policy and Record of Processing methods already explained in this policy.

4. Lawful Processing Criteria

Jesus & Mary Secondary School, Gortnor Abbey 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 Processing Map & Retention Schedule outlined in our Data Protection Policy.

5. Responsible Person Contact Details

Below are the contact details of the person most qualified to respond to questions regarding the CCTV Policy:

- Title: Principal.
- Address: Gortnor Abbey, Crossmolina, Co. Mayo.
- Telephone: 096 31194.
- Email: office@gortnorabbey.ie

6. Data Protection Impact Assessments

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. GDPR Principles

Principle 1: Lawfulness, fairness and transparency
Jesus & Mary Secondary School, Gortnor Abbey 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 notices 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.

Principle 2: Purpose Limitation
Personal data collected by Jesus & Mary Secondary School, Gortnor Abbey 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.

Principle 3: Data Minimisation
Jesus & Mary Secondary School, Gortnor Abbey 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.

Principle 4: Data Accuracy
Jesus & Mary Secondary School, Gortnor Abbey will make every effort to ensure that subjects' information is accurate and up to date. Jesus & Mary Secondary School, Gortnor Abbey 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.

Principle 5: Storage Limitation
Jesus & Mary Secondary School, Gortnor Abbey 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.

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. Jesus & Mary Secondary School, Gortnor Abbey will use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

Principle 7: Accountability
Jesus & Mary Secondary School, Gortnor Abbey is responsible for and is able to demonstrate compliance with GDPR. This means Jesus & Mary Secondary School, Gortnor Abbey will demonstrate that these Data Protection Principles (as outlined here) are met for all Personal Data for which it is responsible.

8. Responsibilities – Board of Management

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

9. Responsibilities – Senior Management

- Ensure that the use of CCTV systems is implemented in accordance with the policy set down by Jesus & Mary Secondary School, Gortnor Abbey.
- 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 recordings in compliance with this policy.
- Maintain a record of the release of recordings or any material recorded or stored in the system.
- Ensure that monitoring recordings 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 students 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 school and be mindful that no such infringement is likely to take place.
- Ensure that adequate signage is posted at appropriate and prominent locations.
- Ensure that on receipt of a valid subject access request, that recordings / images are provided that redact the faces of other others (not involved directly in the incident) to protect their identity.

10. Purpose of CCTV

The School uses CCTV for the following purposes:

- To secure and protect its premises and assets.
- To deter crime and anti-social behaviour. and to assist in the investigation, detection, and prosecution of criminal offences and/or anti-social behaviour.
- To provide a safe environment for all staff and students. to deter bullying and/or harassment.
- To maintain good order and compliance with the school's code of behaviour.
- To assist the school in the conduct of any legal proceedings brought by or against the school.
- For verification purposes and for dispute-resolution, particularly in circumstances where there is a dispute as to facts and where the recordings may be capable of resolving that dispute.

11. 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.
- CCTV is used proportionately in accordance with the GDPR for the purpose of crime-prevention, the prevention of anti-social behaviour, the prevention of bullying, for the safety of our staff and students and for the protection of personal and school property.
- The justifiable reason for installation does indeed outweigh any consideration given to other less intrusive methods of managing any ongoing issue.

12. CCTV Cameras

- The System will operate 24 hours each day, 365 days of the year, except for periods of breakdown or scheduled maintenance.
- The location of CCTV cameras will be known to the Principal and will have been approved by the Board of Management.
- Cameras recording external areas are positioned to prevent or minimise any recording of passers-by or of another person's private property.
- The CCTV system comprises of external and internal (common areas) cameras located in strategic areas around the school.
- 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.
- However, there may be exceptional circumstances where placing CCTV in such areas could be justified subject to a Data Protection Impact Assessment (DPIA).
- Any area where CCTV recording is taking place must always be clearly identified through appropriate signage.
- No processing of audio data, such as audio monitoring or audio recording, is in operation. Nor will there be any deployment of covert surveillance within the School.

13. 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.

14. Notification & Signage

- The Principal will provide a copy of CCTV Policy on request to staff, students, parents and visitors to the school premises.
- The CCTV Policy 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 area 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.
- 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.

15. Management, Control & Access

- Access is restricted to the following persons:
  - Principal.
  - Deputy Principal.
  - Principal Approved Staff.
  - Approved Contractors.
- Supervising the operation and maintenance of the CCTV System is the responsibility of the Principal. The Principal may delegate the administration of the CCTV System to another staff member.
- Access to CCTV systems and footage will be strictly controlled and protected by appropriate security measures. Such access will be limited to relevant personnel on a need-to know basis only.
- There is no remote (i.e. off-site) access allowed to either live or recorded CCTV footage.
- The CCTV system can be accessed by those with access in the Principal's Office.
- 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.
- Subject 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.

16. Access Requests by Third Parties

- Information obtained through the CCTV system can only be released on the authorisation of the Principal and where there is believed to be an appropriate lawful basis allowing disclosure to a third party. Where necessary there will also be consultation with the Chairperson of the Board of Management and/or the seeking of legal advice.
- Recipients to whom the School may allow disclosure of CCTV recordings in specific circumstances include the following:
    - The school's insurance company.
    - Social Workers, HSE and/or TUSLA: in respect of any child protection and/or child safeguarding and/or child welfare matters.
    - Department of Education and Skills and/or any Section 29 Appeals Committee: in relation to any Code of Behaviour, suspension and/or expulsion process.
    - Teaching Council: where legally required in relation to any process under the Teaching Council Acts 2001 – 2015, including fitness to teach investigation.
    - Individuals (or their legal representatives) subject to a court order.
- In certain limited circumstances the School may disclose CCTV footage to An Garda Síochána (or another law enforcement authority). Any such disclosure will be fully documented and limited to what is necessary and proportionate in the circumstances. Such circumstances may include the following:
    - Where the school is required to make a report regarding the commission of a suspected crime. or following a request by An Garda Síochána when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on school property, or
    - Where An Garda Síochána provide a warrant or a court order which imposes a legal obligation on the school to comply with the disclosure request.
    - Where An Garda Síochána approach the school believing that CCTV footage may be of assistance for the investigation, detection and prevention of offences. In the absence of a court order /warrant the school must satisfy itself that there is another appropriate lawful basis that allows legitimate disclosure. Additionally, the school must ensure that the request:
    - Is received in writing on official Garda letterheaded paper - this can be sent by post or as an attachment to an email,
    - States that it is made pursuant to section 41(b) of the Data Protection Act 2018, confirming that it is necessary for the prevention, detection, investigation or prosecution of a criminal offence,
    - Includes such other information as is necessary to confirm its official status. This may include the requesting Garda's name and badge number, the investigation pulse number, signature of Garda of the rank of Superintendent, or above.

17. 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 Subject access request.
- The signals received from the cameras on the campus system and the internal building system are recorded, 24 hours a day, motion activated. This recorded footage is stored digitally on a school site based server. Data from the CCTV System is retained for up to 28 days but will be permanently deleted once there is no reason to retain the recording information
- Where relevant images are produced and are required in relation to an incident, the recording shall be downloaded and saved and retained securely by those will access rights
- At the end of their useful life, all images stored in whatever format will be erased permanently and securely. Any physical matter such as tapes or discs will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.

18. 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 subject 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.

19. 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.
- The date from which the policy will apply is the date of adoption by the Board of Management.
- Implementation of the policy will be monitored by the Principal of the school.

21. CCTV Policy Acknowledgement

Print Name	Signed	Date