Blackrock College

CCTV Policy

April 2025

Summary of Policy Changes

Revision History

Version Number/ Revision Number	Revision Date	Summary of Changes
1.0	10 May 2018	Policy created and approved by the Board of Management
2.0	30 July 2019	Updated and revised
3.0	April 2025	Updated as revised as per JMB CCTV Policy Template 2025

CONTENTS

1 SCOPE

1.1 The purpose of this CCTV Policy (the "Policy") is to regulate the use of CCTV within Blackrock College (the "College"). The Principal will ensure that a copy of this Policy is available to staff, students, parents and visitors to the College.

1.2 The Board of Management is required to maintain a secure, safe and operational environment for the College community and its visitors. This Policy is designed to assist the College with this responsibility in addition to the achievement of other important objectives such as the protection of College property and assets.

1.3 This Policy applies to teaching staff, non-teaching staff, volunteers, students, parents/carers, contractors and visitors to the College, including members of the public.

1.4 The provision of CCTV within a College 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.

1.5 The College's Data Protection Policy governs all processing of personal data associated with the operation of CCTV system within the College.

1.6 Use of the CCTV system must be consistent with all other policies implemented by the College, including, for example the Anti-Bullying Policy, the Harassment and Sexual Harassment Policy, and the Code of Behaviour.

1.7 As a workplace and as a learning environment, the College 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 College's implementation and day to day operation of CCTV.

1.8 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 PURPOSES OF CCTV

2.1 "The purpose of this policy is to regulate the use of Closed Circuit Television and its associated technology in the monitoring of both the internal and external environs of the premises under the remit of Blackrock College."

2.2 CCTV systems are installed (both internally and externally) in premises for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation within and/or in the external environs of the premises during both the daylight and night hours each day. CCTV surveillance at the Blackrock College is intended for the purposes of:

(i) To secure and protect its premises and assets.

(ii) To deter crime and anti-social behaviour, and to assist in the investigation, detection, and prosecution of criminal offenses and/or anti-social behaviour.

(iii) To provide a safe environment for all staff and students, and to deter bullying and/or harassment.

(iv) To maintain good order and compliance with the College's Code of Behaviour.

(v) To assist the College in the conduct of any legal proceedings brought by or against the College.

(vi) 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.

(vii) Promoting the health and safety of staff, students, and visitors.

(viii) Discouraging actions such as physical altercations or any other inappropriate physical behaviour.

(ix) Establishing facts and identifying evidence in the course of workplace investigations regarding alleged serious (gross) misconduct incidents or complaints for the purpose of disciplinary action if there has been a breach of College policies or procedures, or any other serious (gross) misconduct.

(x) Reducing the incidence of crime and anti-social behaviour (including theft and vandalism).

(xi) Protecting the College buildings and College assets, both during and after College hours.

(xii) Assisting in identifying, apprehending, and prosecuting offenders.

(xiii) Monitoring of Access Control Systems: Monitor and record restricted access areas at entrances to buildings and other areas.

(xiv) Verification of Security Alarms: Intrusion alarms, exit door controls, external alarms.

(xv) Criminal Investigations (carried out by An Garda Síochána): Robbery, burglary, and theft surveillance.

2.3 Any use for purposes, other than those listed above, is prohibited by this Policy. For example, the use of CCTV to routinely monitor employee performance is forbidden by this Policy.

2.4 Information obtained in violation of this Policy may not be used in a College disciplinary proceeding against any member of the College community.

3 OPERATION AND MANAGEMENT

3.1 Cameras

(i) The System will operate 24 hours each day, 365 days of the year, except for periods of breakdown or scheduled maintenance.

(ii) The location of CCTV cameras will be known to the Principal and will have been approved by the Board of Management.

(iii) Cameras recording external areas are positioned to prevent or minimise any recording of passers-by or of another person's private property.

(iv) CCTV Monitoring and Recording may include the following areas within the College:

- External Areas: Main entrance/exit gates, vehicular and pedestrian routes, parking areas, building perimeters, storage areas, receiving areas for goods/services;
- Access areas: entrances to buildings, security alarms and access control systems;
- Building interiors: designated congregation areas, lobbies and corridors, locker and storage areas, cashier and service locations;

(v) Due care is taken to uphold reasonable privacy expectations and it is the presumption that cameras will not be located so as to intrude in areas such as:

- Offices;
- Meeting rooms;
- Classrooms;
- Changing rooms; and
- Toilets.

(vi) 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.

(vii) 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 College.

(viii) The College does not use CCTV to process biometric data for the purposes of identifying individuals, such as through the use of facial recognition software.

3.2 Signage

(i) CCTV Signage is placed at the entrances and at prominent locations within the College.

(ii) The signage at the entrances provides the following information:

- identity and contact details of the Data Controller (i.e. the College);
- specific purposes for which the CCTV system is being used;
- instructions as to how data subjects can access further information.

WARNING

IMAGES ARE BEING MONITORED AND RECORDED FOR THE PURPOSE OF THE SAFETY OF OUR STAFF AND STUDENTS, THE PREVENTION OF BULLYING, THE PREVENTION OF ANTI-SOCIAL BEHAVIOUR, THE PROTECTION OF BLACKROCK COLLEGE AND ITS PROPERTY AND CRIME PREVENTION.

THIS SYSTEM IS IN OPERATION 24 HOURS A DAY, EVERYDAY.

THESE IMAGES MY BE PASSED ON TO AN GARDA SIOCHANA.

THIS SCHEME IS CONTROLLED BY THE PRINCIPAL OF BLACKROCK COLLEGE.

(iii) The signage at other locations within the College is used to indicate that CCTV is in operation. Such signage might consist, for example, of an image of a CCTV camera.

3.3 Controls

(i) 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.

(ii) 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.

(iii) There is a remote (i.e. off-site) access allowed to either live or recorded CCTV footage.

(iv) A log of all access to images will be maintained. This log will note key details of any and all access to the live or recorded data, including at least the following information: data and time of access; user names; purpose for accessing. It is recommended that this log should also document the copying of any data or material stored in the system.

(v) Any recorded footage and monitoring equipment are stored securely in a restricted area. Unauthorised access to that area will not be permitted at any time. Monitors, especially when they are in open office areas, will be positioned appropriately so as to protect the rights of those whose images may be displayed.

(vi) Other than the Principal and Deputy Principal(s), staff designated to view CCTV images for the purposes outlined in this Policy include Maintenance Manager, Head of Security and Year Deans.

(vii) The Principal may, from time to time, authorise staff, other than those designated above, to view recorded images where this is considered necessary. Such staff should be accompanied on these occasions by another designated member of staff.

(viii) CCTV will not be used as an indiscriminate live monitoring tool.

(ix) Any use of temporary cameras (for example, during special events that have particular security and/or health and safety requirements) will be approved in advance by the Principal.

4 RESPONSIBILITIES

The Principal and the Maintenance Manager will:

(i) Ensure that the use of CCTV systems is implemented in accordance with the policy set down by Blackrock College.

(ii) Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within Blackrock College.

(iii) Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy

(iv) Ensure that the CCTV monitoring at Blackrock College is consistent with the highest standards and protections

(v) Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy

(vi) Maintain a record of access (e.g. an access log) to or the release of tapes or any material recorded or stored in the system

(vii) Ensure that monitoring recorded tapes are not duplicated for release

(viii) Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally

(ix) 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 do not include mobile video equipment or hidden surveillance cameras used for authorised criminal investigations by An Garda Síochána].*

(x) Give consideration to both students and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment

(xi) Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the College and be mindful that no such infringement is likely to take place

(xii) Co-operate with the Health & Safety Officer of Blackrock College in reporting on the CCTV system in operation in the College

(xiii) Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy"

(xiv) Ensure that monitoring digital recordings are stored in a secure place with access by authorised personnel only

(xv) Ensure that images recorded on digital recordings are stored for a period not longer than 60 days and are then automatically erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by the Chairperson of the Board

(xvi) Ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy

(xvii) Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics

(xviii) Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas

(xix) Ensure that where An Garda Síochána request to set up mobile video equipment for criminal investigations, legal advice has been obtained and such activities have the approval of the Chairperson of the Board.

5 DATA PROTECTION

5.1 General

All video images that contain personal data must be processed in accordance with the College's Data Protection Policy. This requires the College to ensure that all CCTV data is:

(i) processed lawfully, fairly and in a transparent manner;

(ii) collected for specified, explicit and legitimate purposes;

(iii) adequate, relevant and limited to what is necessary;

(iv) accurate and, where necessary, kept up to date;

(v) kept for no longer than is necessary;

(vi) processed in a manner that ensures appropriate security.

Additionally, the College must be ready to demonstrate its compliance (accountability) with the 6 data processing principles, set out above. The Board of Management is the accountable data controller and as such is responsible for oversight of the College's CCTV system ensuring that it is deployed in a manner that is professional, ethical and lawful.

5.2 Legal Basis

The processing of CCTV by the College is reliant upon one or both of the following lawful bases:

(i) Article 6 (1) (f) legitimate interest,

(ii) Article 6 (1) (e) necessity to perform a task carried out in the public interest or in the exercise of official authority.

5.3 Retention

(i) The images captured by the CCTV system are retained for a maximum of 28 days, except where the image identifies an issue and which necessitates a longer period specifically in the context of an investigation/prosecution of that issue.

(ii) In some circumstances a longer retention period may be justifiable for a particular section of video footage. For example, an extended retention period could be justifiable as part of an investigation in to a serious incident or an accident or where footage might need to be retained as evidence for potential criminal proceedings. Such footage will be isolated from the general recordings and kept securely for the purposes that have arisen.

5.4 Requests for Disclosure

(i) 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.

(ii) Recipients to whom the College may allow disclosure of CCTV recordings in specific circumstances include the following:

a) The College's insurance company.
b) Social Workers, HSE and/or TUSLA: in respect of any child protection and/or child safeguarding and/or child welfare matters.
c) Department of Education and Skills and/or any Section 29 Appeals Committee: in relation to any Code of Behaviour, suspension and/or expulsion process.
d) Teaching Council: where legally required in relation to any process under the Teaching Council Acts 2001 – 2015, including fitness to teach investigation.
e) individuals (or their legal representatives) subject to a court order.

(iii) In certain limited circumstances the College 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:

a) where the College 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 College property, or
b) where An Garda Síochána provide a warrant or a court order which imposes a legal obligation on the College to comply with the disclosure request.
c) where An Garda Síochána approach the College 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 College must satisfy itself that there is another appropriate lawful basis that allows legitimate disclosure. Additionally, the College 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.

6 DATA SUBJECT RIGHTS

6.1 General

(i) This section highlights certain rights that are viewed as particularly relevant to the operation of the College's CCTV system. A full list of data subject rights is set out in the College's Data Protection Policy.

(ii) The College will be conscious of the need to respond without undue delay and within the advised timeframes. A response will be provided within one month of receipt of any request.

(iii) While the College will always respect and facilitate the exercise of these rights, it needs to be understood that they are not unconditional and that the College may need to give consideration to other obligations.

6.2 Right to Object

(i) Data subjects have the right to object when data processing is based on the College's legitimate interests or relates to a task carried out in the public interest, both of which usually legitimise the College's operation of CCTV.

(ii) In the event of such an objection the College must demonstrate compelling legitimate grounds if such processing is to continue.

(iii) Regardless of the outcome of any assessment of the College's right to continue its processing of CCTV data in the face of an objection, the College will ensure that it gives appropriate consideration to feedback or concerns shared by students (or their parents/guardians) and staff or others regarding any possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or any aspect of the College's operation of its CCTV system.

6.3 Right of Access

(i) Any person whose image has been recorded can request a copy of the information which relates to them, and the College is obliged to act on that request provided that an exemption or prohibition does not apply to the release.

(ii) A person should provide all the necessary information to assist the College in locating the CCTV recorded data, such as the date, time and location of the recording. If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data and therefore its supply may not be required.

(iii) Where the image/recording identifies a third party (i.e. an individual other than the one making the access request), the College may be precluded from providing a copy where it is adjudged that the release may interfere with the rights of those third parties.

(iv) In such circumstances the College will examine whether the redaction or anonymisation of the images will allow for their release. The College in responding to a right of access must ensure that it does not adversely affect the rights of others.

6.4 Right to Complain

(i) If you are concerned about how your personal data is being processed, then please address these concerns in the first instance to the Principal who is responsible for the day-to-day application of this Policy.

(ii) A matter that remains unresolved may be referred to the Board of Management by writing to the Chairperson c/o College. The Board of Management is designated as the data controller for the College and as such is responsible and accountable for oversight of this Policy.

(iii) Should you feel dissatisfied with how the College has addressed a complaint or concern that you have raised, you have the right, as data subject, to bring the matter to the attention of the Data Protection Commission.

Telephone	(01) 765 01 00
	1 800 437 737
E-mail	info@dataprotection.ie
Post	Data Protection Commission
	21 Fitzwilliam Square South
	Dublin 2
	D02 RD28
Website	www.dataprotection.ie

7 IMPLEMENTATION AND 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 College), 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 College.

This policy was reviewed by the Board of Management on _____.

Signed: _____

Chairperson, Board of Management

Signed: _____

Secretary, Board of Management