

CBS Thurles

CCTV POLICY

CONTENTS

1 SCOPE 3
2 PURPOSES OF CCTV 3
3 OPERATION AND MANAGEMENT 4
3.1 Cameras 4
3.2 Signage 5
3.3 Controls 5
4 DATA PROTECTION 6
4.1 General 6
4.2 Legal Basis 6
4.3 Retention 7
4.4 Use of a Processor (CCTV/Security Company) 7
4.5 Requests for Disclosure 8
5 DATA SUBJECT RIGHTS 9
5.1 General 9
5.2 Right to Object 9
5.3 Right of Access 9
5.4 Right to Complain 10

1 SCOPE

1.1 The purpose of this CCTV Policy (the "Policy") is to regulate the use of CCTV within CBS Thurles[1] . The Principal will ensure that a copy of this Policy is available to staff, students, parents and visitors to the School.

1.2 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.

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

1.4 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.

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

1.6 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.

1.7 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.

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 School uses CCTV for the following purposes:

(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 offences and/or anti-social behaviour;

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

(iv) to maintain good order and compliance with the School's Code of Behaviour;

(v) to assist the School in the conduct of any legal proceedings brought by or against the School;

(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.

2.2 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.

[1] Where school classes and activities are carried out in temporary premises, the school will endeavour to ensure that any relevant CCTV system is operated in a manner that is compatible with the provisions of this policy.

2.3 Information obtained in violation of this Policy may not be used in a School disciplinary proceeding against any member of the School 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 school:

- 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[2]:

- Offices;
- Meeting rooms;
- Classrooms;
- Changing rooms; and
- Toilets[3].

(vi) However, there may be exceptional circumstances where placing CCTV in such areas could be justified subject to a Data Protection Impact Assessment (DPIA).[4] 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 School.[5]

---

[2] Any CCTV installation must be deemed necessary and proportionate and be undertaken in circumstances where no other less intrusive means of achieving the same objective is available to the school. It should be preceded by a comprehensive examination of its impact on privacy, which will usually take the form of a data protection impact assessment (GDPR Article 35). This DPIA should take appropriate account of the views of the data subjects and may also involve consultation with school advisory bodies and/or the Gardai and/or Data Protection Commission as appropriate. The CCTV installation should not proceed where its impact on privacy is considered unacceptable.

[3] Using CCTV to monitor individuals in toilets or changing rooms will likely contravene the GDPR in nearly all circumstances.

[4] Completion of a DPIA is strongly recommended where a school is implementing a new CCTV system, or making changes, such as additions to or reconfiguration of, an already existing CCTV system. Indeed, a statutory requirement to complete a DPIA in defined circumstances came in to effect in May 2018 (with the coming in to force of GDPR). The DPC advises that "An example of a scenario that would likely trigger the need for a DPIA is the implementation of a CCTV system in a school, covering more than just public areas". Comprehensive guidance on Data Protection Impact Assessments, including a DPIA template, is available on the DPC website. The *DPC Toolkit for Schools* includes an appendix (p64-76) that addresses how a school should carry out a DPIA.

[5] The use of recording mechanisms to obtain data without an individual's knowledge is generally unlawful. Covert surveillance is normally only permitted on an exceptional case-by-case basis where the data are kept for the purposes of preventing, detecting or investigating offences, or apprehending or prosecuting offenders. This provision automatically implies that a written specific policy be put in place detailing the purpose, justification, procedure, measures and safeguards that will be implemented with the final objective being, an actual involvement of An Garda Síochána or other prosecution authorities for potential criminal investigation or civil legal proceedings being issued, arising as a consequence of an alleged committal of a criminal offence(s).

(viii) The school does not use CCTV to process biometric data for the purposes of identifying individuals, such as through the use of facial recognition software.[6]

(ix) 'Dummy' cameras fall outside the scope of this Policy as they do not record data subjects.

3.2 Signage

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

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

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

WARNING CCTV cameras in operation 24 hours a day, every day. These images may be passed to An Garda Síochána. This system is controlled by <name of school> [and operated by <insert name of commercial security company where deemed appropriate>] for the following purposes: (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 offences and/or anti-social behaviour; (iii) to provide a safe environment for all staff and students; to deter bullying and/or harassment; (iv) to maintain good order and compliance with the School's Code of Behaviour; (v) to assist the School in the conduct of any legal proceedings brought by or against the School; (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. For further information see the school Data Protection Policy and CCTV Policy at www.cbsthurles.ie

(iii) The signage at other locations within the school is used to indicate that CCTV is in operation.[7] 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 no remote (i.e. off-site) access allowed to either live or recorded CCTV footage.[8]

[6] Facial recognition processing is considered biometric processing and accordingly the relevant personal data is categorised as "special category" data. Any processing of biometric data should be considered separately to the regular usage of the CCTV system and a data controller engaging in such processing must take all steps to ensure that it is compliant with the data protection legislative frameworks.

[7] The information should be positioned in such a way that the data subject can easily recognise the circumstances of the surveillance before entering the monitored area. It is not necessary to reveal the precise position of the camera as long as there is no doubt as to which areas are subject to monitoring.

[8] Remote access to CCTV cameras, by whatever means, is becoming more frequent with advances in technology. For example, some CCTV systems allow footage to be accessed remotely, via mobile phone. Such technology can be helpful in terms of providing security monitoring of an empty building at night time or at weekends. However, controllers utilising remote access must consider any additional risk of unauthorised disclosure which may arise from such functionality.

(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.[9] 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 <insert list of staff identified by their role e.g. Assistant Principals>.

(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.[10]

4 DATA PROTECTION[11]

4.1 General

All video images that contain personal data must be processed in accordance with the School's Data Protection Policy. This requires the School 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 School 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 school's CCTV system ensuring that it is deployed in a manner that is professional, ethical and lawful.

4.2 Legal Basis

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

[9] This is particularly important given the widespread availability of camera phones, where copies of footage could easily be made without authorisation. Signage prohibiting such filming should be considered. The area should be locked when not occupied by authorised personnel. Alternatively access to the CCTV system may be protected by password/PIN, ideally with a unique password/PIN issued to each user.

[10] Temporary cameras do not include mobile video equipment or hidden surveillance cameras used for authorised criminal investigations by An Garda Síochána.

[11] In order to demonstrate that its use of CCTV is GDPR compliant, a school must be able to demonstrate the following: (i) CCTV is being used for a legitimate purpose; and (ii) the data protection principles are being respected; (iii) CCTV use is necessary and proportionate taking account of data subjects rights and interests; and (iv) All risks associated with the processing of personal data have been identified, assessed and minimised to an acceptable level.

(i) Article 6 (1) (f) legitimate interest[12],

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

4.3 Retention

(i) The images captured by the CCTV system are retained for a maximum of 30 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.

4.4 Use of a Processor (CCTV/Security Company)

Where the School CCTV system is operated by a security company contracted by the Board of Management, the following applies[13]:

(i) Prior to agreeing to the engagement of any security company as a service provider to the school, an appropriate assessment of their suitability will have been undertaken. This assessment will include guarantees of their capacity to implement sufficient technical and organisational measures to protect the rights of the school community.[14]

(ii) The School will have a written contract, known as a Service Level Agreement (SLA), in place with the security company which outlines the terms and conditions that relate to the CCTV service that is being provided.

(iii) Staff of the security company will be aware of their obligations relating to the security of personal data, and be bound by a strict duty of confidentiality.

(iv) Where the security company (Hall Alarms) has access to the recorded images of individuals, it is classified as a "data processor" and this imposes certain statutory requirements under the GDPR.[15] In these circumstances the School and the security company must have a written Data Processing Agreement (DPA) in place.[16]

(v) The Data Processing Agreement provides a description of the CCTV processing as well as a number of binding commitments on behalf of the processor (the security company) to the controller (the School) including, inter alia[17]:

- to act only on the School's instructions
- to implement appropriate technical and organisational measures
- to ensure confidentiality of persons authorised to process data
- not to engage another processor without written authorisation

[12] The legitimate interest needs to be real and current (i.e. it must not be fictional or speculative). In light of the principle of accountability, controllers are advised to document relevant incidents (date, description, impact etc). Those documented incidents can be a strong evidence for the existence of a legitimate interest. This interest as well as the necessity of the monitoring should be reassessed at periodic intervals.

[13] Security companies that operate cameras on behalf of clients are considered to be 'Data Processors'. As processors, they operate under the instruction of data controllers i.e. the school's Board of Management.

[14] The Private Security Authority (PSA) is the statutory body with responsibility for licensing and regulating the private security industry in Ireland. Although it is not a data protection requirement, any contractor who installs, maintains, repairs or services CCTV systems as part of a business, trade or profession must hold a PSA license. Licensing applies to CCTV systems used solely or partially for security purposes.

[15] The CCTV company should be identified (by name/function) as a "recipient" in the school's main Data Protection Policy.

[16] This Data Processing Agreement is set out in writing, typically as an addendum to the Service Level Agreement.

[17] GDPR Article 28 sets out the full list of requirements. See also *Guidance on Data Processing Agreements* on the DPC website.

- to inform the School without undue delay in the event of a data breach
- to assist the School to comply with its obligations under GDPR.

4.5 **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 School may allow disclosure of CCTV recordings in specific circumstances include the following[18]:

a) The school'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/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 – 2024, including fitness to teach investigation.

e) individuals (or their legal representatives) subject to a court order.

(iii) 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:

a) 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

b) 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.

c) 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.[19] 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.

[18] The inclusion of a body on this list does not, of itself, justify the sharing of CCTV footage with that body. Each case must be examined to ensure that an appropriate lawful basis exists to legitimise the sharing of specific data in the applicable circumstances.

[19] The school must be able to demonstrate that the data was necessary and proportionate. This is a matter of judgement and can often be difficult to determine. In such circumstances the school is strongly advised to seek professional/legal advice.

5 DATA SUBJECT RIGHTS[20]

5.1 General

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

(ii) The school 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.[21]

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

5.2 Right to Object

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

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

(iii) Regardless of the outcome of any assessment of the school's right to continue its processing of CCTV data in the face of an objection, the school 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 school's operation of its CCTV system.

5.3 Right of Access

(i) Any person whose image has been recorded can request a copy of the information which relates to them, and the School 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 School 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 School 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 school will examine whether the redaction or anonymisation of the images will allow for their release. The School in responding to a right of access must ensure that it does not adversely affect the rights of others.[22]

---

[21] That period may be extended by two further months where necessary. The school must inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

[22] In endeavouring to fulfil a data subject access rights, the school may also explore other options such as providing a still/series of pictures.

5.4 **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.[23]

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

(iii) Should you feel dissatisfied with how the school 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

Signed: *Mary O'Dwyer* Date: 13th February 2025

Chairperson

[23] Parents/Guardians may also, where applicable, have the option of invoking the school's formal complaints procedure (available from school).