Mercy Secondary School Kilbeggan

Disclaimer: This document is provided as a resource to assist schools. While every effort has been made to ensure the accuracy of the information provided, schools are advised to exercise common sense, consult up to date circulars, legislation, case-law, and/or guidelines from relevant agencies. Where specific queries arise, schools are urged to obtain timely advice from their management body. Data protection and education law change all the time, so each school needs to keep its policies and practices up to date. This document does not constitute legal advice.

CCTV POLICY

CONTENTS

1 SCOPE

1.1 The purpose of this CCTV Policy (the "Policy") is to regulate the use of CCTV within Mercy Secondary School Kilbeggan (the "School")[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.[2]

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.

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[3]:

- Offices;
- Meeting rooms;
- Classrooms;
- Changing rooms; and
- Toilets[4].

(vi) However, there may be exceptional circumstances where placing CCTV in such areas could be justified subject to a Data Protection Impact Assessment (DPIA).[5] 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.[6]

(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.[7]

(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 Mercy Secondary School Kilbeggan and operated by CSS 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 mercykilbeggan.ie

(iii) The signage at other locations within the school is used to indicate that CCTV is in operation.[8] 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.[9]

(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.[10] 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 the Caretaker.

(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.[11]

4 DATA PROTECTION[12]

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:

(i) Article 6 (1) (f) legitimate interest[13],

(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[14]:

.

.

(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.[15]

(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 has access to the recorded images of individuals, it is classified as a "data processor" and this imposes certain statutory requirements under the GDPR.[16] In these circumstances the School and the security company must have a written Data Processing Agreement (DPA) in place.[17]

(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[18]:

- 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
- 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[19]:

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 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 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.[20] 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.

.

5 DATA SUBJECT RIGHTS[21]

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.[22]

(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.[23]

.

.

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.[24]

(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: *Paul Daly* Signed: *Garrett Farrell*

Chairperson of Board of Management Principal/Secretary to the Board of Management

Date: **6th February 2025** Date : **6th February 2025**

Appendix 1. SYSTEM DESIGN AND OPERATIONAL SAFEGUARDS

NB It is not necessary to include these appendices as part of the school's CCTV Policy. Similarly, the footnotes are included as a guide to school management and can be deleted prior to wider publication.

Appendix 1 provides advice on design and implementation measures that should be considered prior to any installation and operation of CCTV within a school environment. Some of this guidance was drawn up with the school sector in mind, for example, extracts from the DPC Data Protection Toolkit for Schools, and as such are worthy of particular attention. Other guidance was aimed at the general audience of data controllers. The documents which provided the primary reference sources for Appendix 1 are listed in Appendix 2.

CCTV on school premises (Extract from *DPC Data Protection Toolkit for Schools*)

Queries are often raised with the DPC regarding the use of CCTV in schools. The DPC has published comprehensive guidance on the use of *CCTV for data controllers*, which schools should consult in the first instance.

Broadly speaking, the principles set out in this CCTV guidance apply equally to schools, save that schools must be particularly mindful that where CCTV is capturing images of children, a higher threshold of protection would be required owing to the fact that children merit specific protection under the GDPR. While this toolkit is focused on the processing of children's personal data in particular, schools must also be mindful that they are a workplace. The impact that CCTV may have on a school's employees and visitors must also be considered when determining if a CCTV system should be implemented in a school. All such processing of personal data must be in compliance with data protection law.

When considering the implementation of CCTV, schools must:

- Have a clearly defined purpose for installing CCTV in or around the school;
- Have a legal basis for the use of CCTV;
- Be able to demonstrate that the CCTV is necessary to achieve its stated purpose (e.g. they must be able to show that the purpose cannot be achieved by less intrusive means than CCTV. If the purpose can be achieved using less intrusive means, then the processing of personal data through the use of CCTV would not be lawful as it could not be deemed to be necessary);
- Be able to demonstrate that the use of CCTV is proportionate for its stated purpose;
- Be able to demonstrate that appropriate measures are in place to ensure that the CCTV recordings are safe and secure, both technically and organisationally, including who accesses and views CCTV recordings;
- Have retention policies in place;
- Have appropriate signage in place to inform people CCTV is taking place;
- Have an up-to-date CCTV Data Protection Policy in place, which should be brought to the attention of everyone whose data is captured or likely to be captured (for example, making the policy available on the school's website).
- Ensure that CCTV is not in operation in areas where students, staff or visitors would have an increased expectation of privacy (e.g. changing rooms).

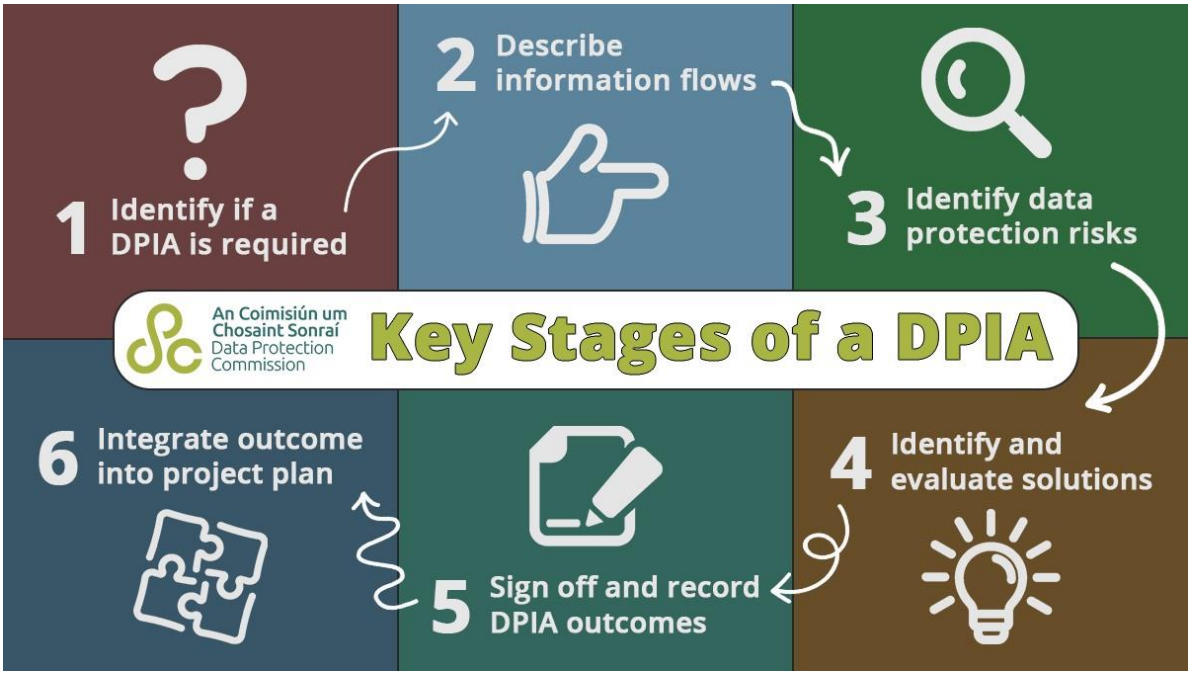
Data Protection Impact Assessments (Extract from *DPC Data Protection Toolkit for Schools*)

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.

Schools can demonstrate that they have considered in detail the above-mentioned criteria by carrying out a Data Protection Impact Assessment (DPIA). Article 35 of the GDPR states that a DPIA must be carried by a data controller where a type of data processing, in particular using new technologies, is likely to result in a high risk to the rights

and freedoms of individuals. The GDPR also sets out a number of specific instances in which controllers must conduct a DPIA. A DPIA describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. If required, a DPIA must be completed before the data processing has begun. DPIAs are important tools for negating risk, and for demonstrating compliance with the GDPR. In addition to the CCTV system example outlined above, a school may need to carry out a DPIA in other circumstances such as using third-party platforms to process student data (new EdTech platforms etc.) or in circumstances where student health data is being processed (e.g. health monitoring apps used by a school's football team).

The DPC has separate *guidance on DPIAs* available on their website. It is the DPC's position that where the processing of children's personal data is at issue, a data controller should carry out a DPIA given that children are a particularly vulnerable group. For further assistance on how to carry out a DPIA, please see the sample "DPIA Template" created for schools to use on page 66 of DPC's *Data Protection Toolkit for Schools*.



DPIAs are important tools for negating risk, and for demonstrating compliance with the GDPR. As a controller, your school needs to make sure that a DPIA is carried out where this is appropriate. An initial assessment of the risk arising from data processing, using the checklist (see DPIA Template in DPC Toolkit for Schools), can indicate whether a DPIA is likely to be necessary before introducing a new technological solution or method of working. When making this assessment, schools should take into consideration that the vulnerability of children is often indicative of a higher level of risk arising from the processing of their personal data.

While DPIAs may not always be mandatory for all types of processing that a school may carry out, they may still serve as a useful tool for schools to demonstrate compliance with the GDPR. DPIAs can help schools to document how their processing is both necessary and proportionate, and demonstrate that they have considered the risks involved in their processing of personal data and taken relevant steps to mitigate against these risks.

We have experienced repeated incidences of anti-social behaviour on the school premises and are considering installing CCTV cameras – can we do this? (Extract from *DPC Data Protection Toolkit for Schools*)

Schools should be aware that footage or images containing identifiable individuals captured by CCTV systems are personal data for the purposes of data protection law. Before making the decision to implement a CCTV system, schools should consider, amongst other things:

- whether they have a clearly defined purpose for installing CCTV in or around the school;
- What their legal basis is for the use of CCTV under Article 6;
- Whether they can demonstrate that the CCTV is necessary to achieve its stated purpose
- Whether they can demonstrate that the use of CCTV is proportionate for its stated purpose;

Schools must be particularly mindful that where CCTV is capturing images of children, a higher threshold of protection would be required owing to the fact that children merit specific protection under the GDPR.

A Data Protection Impact Assessment (DPIA) should be carried out before any processing commences. By conducting a DPIA, a school can identify and mitigate against any data protection related risks arising from the installation of CCTV, which may affect the school or the individuals it engages with, and in turn can ensure and demonstrate that the school is in compliance with the GDPR.

Necessity and Proportionality

A data controller must be able to justify the use of a CCTV system as both necessary to achieve their given purposes and proportionate in its impact upon those who will be recorded. Necessary processing using a CCTV system means more than the CCTV system being merely helpful to achieve a purpose. The data controller must be able to demonstrate why the use of a CCTV system is necessary for the purpose concerned. An assessment of the situation leading to the decision to install CCTV and of the practical implications of its use will assist in determining whether it is justified.

Before installing a video surveillance system, the controller should always critically examine if this measure is firstly suitable to attain the desired goal, and secondly adequate and necessary for its purposes. Video surveillance measures should only be chosen if the purpose of the processing could not reasonably be fulfilled by other means which are less intrusive to the fundamental rights and freedoms of the data subject.

Deploying CCTV in places where there is a reasonable expectation of individual privacy should only occur when there is a particularly serious and documented problem. If data controllers intend on installing CCTV in such areas, they will need to be in a position where they can provide detailed evidence, which clearly justifies their use at any given time.

Therefore, data controllers must establish the following:

1. The problem(s) being addressed is/are sufficiently serious to justify the use of CCTV in such locations;
2. The problem(s) cannot be addressed by less intrusive measures;
3. The use of CCTV addresses the problems identified; and
4. The risks posed to data subjects using the facilities have been fully assessed and mitigated to an acceptable level.

Good governance of CCTV is reliant on a robust risk assessment, where the primary objective is to identify and mitigate any risks to data subjects. This risk assessment may form an important part of a legitimate interests assessment or a data protection impact assessment, the latter being a statutory requirement in certain circumstances.

Public Interest as a Lawful Basis

Personal data could be processed through video surveillance under GDPR Article 6 (1) (e) if it is necessary to perform a task carried out in the public interest or in the exercise of official authority. It may be that the exercise of official

authority does not allow for such processing, but other legislative bases such as "health and safety" for the protection of visitors and employees may provide limited scope for processing, while still having regard for GDPR obligations and data subject rights.

Legitimate Interests as a Lawful Basis

Presuming that video surveillance is necessary to protect the legitimate interests of a controller, a video surveillance system may only be put in operation, if the legitimate interests of the controller (or those of a third party) e.g. protection of property or physical integrity, are not overridden by the interests or fundamental rights and freedoms of the data subject. The controller needs to consider (i) to what extent the monitoring affects the interests, fundamental rights and freedoms of individuals and (ii) if this causes violations or negative consequences with regard to the data subject's rights. Fundamental rights and freedoms on one hand and the controller's legitimate interests on the other hand have to be evaluated and balanced carefully.

According to GDPR Recital 47, the existence of a legitimate interest needs careful assessment. The reasonable expectations of the data subject at the time and in the context of the processing of their personal data have to be considered. The relationship between data subject and controller may vary significantly and may affect what reasonable expectations the data subject might have. The decisive criterion has to be if an objective third party could reasonably expect to be subject to monitoring in this specific situation.

Right to Object

For video surveillance based on legitimate interest, GDPR Article 6 (1) (f), or for the necessity when carrying out a task in the public interest, GDPR Article 6 (1) (e), the data subject has the right – at any time – to object, on grounds relating to his or her particular situation, to the processing in accordance with Article 21 GDPR. Unless the controller demonstrates compelling legitimate grounds that overrides the rights and interests of the data subject, the processing of data of the individual who objected must then stop.

CCTV in the workplace

The use of CCTV in the workplace can be contentious and it is not generally considered to be an appropriate tool to monitor staff attendance or performance. However, situations can arise where an employer needs to use CCTV footage for a purpose other than one identified at the outset such as to investigate an allegation of gross misconduct or other disciplinary matter. This may be legitimate where it is carried out strictly on a case-by-case basis, and is justified based on necessity and proportionality to achieve the given purpose. The employer must be able to demonstrate why the use of CCTV is necessary to provide evidence in a disciplinary matter, and that their access of CCTV footage is proportionate and limited in scope to the investigation of a particular matter. In such cases, the rights of the employee and their expectation of privacy will not be seen as overriding the interests of the employer, and the employee's data protection rights should not be seen as presenting a barrier to the investigation of serious incidents.[25]

Data protection by design and by default

Data controllers are obliged to adhere to the principles of data protection by design and by default. Data protection by design requires that appropriate measures to implement data protection principles are integrated at the planning stage of any data processing operation and maintained at all stages. This means that where the implementation of CCTV is being considered, data protection concerns are addressed at the earliest stage of the project.

[25] The DPC refers to a case where CCTV footage was shared by a bar hosting a work event on behalf of an employer, and during which a serious assault took place necessitating the attendance of An Garda. The DPC stated that the CCTV was processed in furtherance of the employer organisation's obligation to protect the health and safety of its employees and was satisfied that there was a legitimate interest justifying the processing. The disclosure of the CCTV in this instance was necessary for the legitimate interests pursued by the employer organisation so that it could investigate and validate allegations of wrongdoing against the complainant. The DPC considered that it would have been unreasonable to expect the bar to refuse a request by the employer organisation to view and take a copy of the CCTV footage, against a backdrop of allegations of a serious assault on its premises, especially where the personal data had been limited to the incident in question and had not otherwise been disclosed. A refusal of the request might have impeded the full investigation of an alleged serious assault, and the employer organisation's ability to protect the health and welfare of its employees. Accordingly the DPC considered that it was reasonable, justifiable and necessary for the bar to process the CCTV footage by providing it to the employer organisation, and that the legitimate interest of the employer organisation took precedence over the rights and freedoms of the complainant, particularly given that the processing did not involve sensitive personal data and there had not been excessive processing.

Data protection by default requires that technical and organisational measures be put in place to ensure that only personal data which are necessary for a specific purpose are processed. In the rollout of a CCTV system, this will have a bearing, for example, on the placement of cameras, the focus of the cameras, the capability of the cameras, the functionality of the cameras (have they pan, tilt or zoom functionality?) and privacy masking features as well as the determination of an appropriate retention period. Users of CCTV systems should be aware that the use of particular features, such as zoom capability, can increase the potential intrusion on individuals' privacy.

As stated in Article 25 GDPR, controllers need to implement appropriate data protection technical and organisational measures as soon as they plan for video surveillance – before they start the collection and processing of video footage. These principles emphasize the need for built-in privacy enhancing technologies, default settings that minimise the data processing, and the provision of the necessary tools that enable the highest possible protection of personal data.

Controllers should build data protection and privacy safeguards not only into the design specifications of the technology but also into organisational practices. When it comes to organisational practices, the controller should adopt an appropriate management framework, establish and enforce policies and procedures related to video surveillance. From the technical point of view, system specification and design should include requirements for processing personal data in accordance with principles stated in Article 5 GDPR (lawfulness of processing, purpose and data limitation, data minimisation[26], integrity and confidentiality, accountability etc.). Where a controller plans to acquire a commercial video surveillance system, the controller needs to include these requirements in the purchase specification. The controller needs to ensure compliance with these requirements applying them to all components of the system and to all data processed by it, during their entire lifecycle.

Data Protection Impact Assessment (DPIA) is often necessary and always recommended

Before a school installs a new or extended CCTV system, it is recommended that a data protection impact assessment is undertaken. Indeed a DPIA is a statutory requirement in certain circumstances.

According to GDPR Article 35(1) controllers are required to conduct a data protection impact assessment (DPIA) when a type of data processing is likely to result in a high risk to the rights and freedoms of natural persons. GDPR Article 35(3)(c) stipulates that controllers are required to carry out data protection impact assessments if the processing constitutes a systematic monitoring of a publicly accessible area on a large scale. Moreover, according to GDPR Article 35(3)(b), a data protection impact assessment is also required when the controller intends to process special categories of data on a large scale.

The outcome of the performed DPIA should determine the controller's choice of implemented data protection measures. It is also important to note that if the results of the DPIA indicate that processing would result in a high risk despite security measures planned by the controller, then it will be necessary to consult the relevant supervisory authority prior to the processing.

Data Minimisation is always a necessity

Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')[27].

In general, the necessity to use video surveillance to protect the controllers' premises ends at the property boundaries. However, there are cases where the surveillance of the property is not sufficient for an effective protection. In some individual cases it might be necessary to exceed the video surveillance to the immediate surroundings of the premises. In this context, the controller should consider physical and technical means, for example blocking out or pixelating non-relevant areas.

Transparency is key

A person whose images are recorded by a CCTV system must be provided with at least the following information (either directly or in a way the individual can easily access):

[26] by default in the sense of Article 25 (2) GDPR

[27] GDPR Article 5(1)(c)

- The identity and contact details of the data controller
- The purposes for which data are processed
- The legal basis for the processing
- Any third parties to whom data may be disclosed
- The retention period for CCTV footage
- The existence of data subject rights and the right to lodge a complaint with the DPC

Measures are needed to maintain security and control access

Data controllers are obliged to implement technical and organisational measures to ensure that personal data are kept secure from any unauthorised or unlawful processing and accidental loss, destruction or damage. For CCTV systems, this can include restricting access to footage and the use of encryption and password protection for devices storing CCTV footage. Generic or shared passwords should be avoided in order to reduce the risk of inappropriate use of the system occurring and going undetected. The storage medium should be maintained in a secure environment and the use and regular review of an access log can provide assurance that only authorised personnel have access to and may view the footage.

Some CCTV systems allow footage to be accessed remotely, via mobile phone for example. Remote access to CCTV cameras, by whatever means, is becoming more frequent with advances in technology. Such technology is 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, and further potential concerns from a data protection perspective arise where the remote access takes place in relation to areas such as manned workplaces and where workers perceive that their work performance is being monitored on a live basis. Employers may be tempted to use such technologies as a substitute for on-the-ground supervision by supervisory or managerial staff; this type of monitoring or surveillance is unlikely to justifiable.

Access control ensures that only authorized people can access the system and data, while others are prevented from doing it. Measures that support physical and logical access control include:

- Ensuring that all premises where monitoring by video surveillance is done and where video footage is stored are secured against unsupervised access by third parties.
- Procedures for granting, changing and revoking physical and logical access are defined and enforced.
- Methods and means of user authentication and authorization including e.g. passwords length and change frequency are implemented.
- User performed actions (both to the system and data) are recorded and regularly reviewed.
- Monitoring and detection of access failures is done continuously and identified weaknesses are addressed as soon as possible.

Use of a Data Processor

CCTV systems are often managed and maintained by third party contractors on behalf of the owners of premises. Security companies that place and operate cameras on behalf of clients may be considered "data processors", where they process personal data under the instruction of data controllers (their clients), subject to contract.

Data protection law places a number of obligations on data processors. These include having appropriate security measures in place to prevent unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all unlawful forms of processing. This obligation can be met by measures such as having appropriate access controls to image storage or having robust encryption where remote access to live recording is permitted. Staff of the security company must be made aware of their obligations relating to the security of data.

Clients of the security company should have a contract in place, which details what the security company may do with the data, what security standards should be in place, and for how long the data should be retained. Please note the guidance on data processing contracts available on the DPC website.

Retention of Personal Data

Data protection law requires that personal data should be retained for no longer than is necessary to achieve the identified purpose for which it is processed. The law does not define specific retention periods. A data controller needs to be able to justify a defined retention period, and data may not be kept on a 'just-in-case' basis. A data controller may wish to consider any previous incidents or situations giving rise to the necessity for access to CCTV footage to achieve a purpose that may have a bearing on the appropriate retention period.

As an example, Section 8 of the Civil Liability and Courts Act 2004 requires that where a letter of claim in a personal injuries action is served one month after the accident, the court shall draw such inferences as appear proper. A 30-day retention period may thus be deemed reasonable, proportionate and balanced for CCTV footage for the purpose of defending a potential personal injury action. For a normal security system, it would be difficult to justify retention beyond one month, except where the images identify an issue – such as a break-in or theft – and is retained specifically in the context of the investigation of that issue.

The retention period should be the shortest period necessary to achieve the purpose for which the system was installed and should allow the controller enough time to review any footage as necessary before deleting the data. Where a CCTV recording system or device has a default retention period, this should be reviewed by the data controller, and compared to their own assessment of what is a necessary retention period to avoid the retention of data for longer than is necessary.

Where footage has been identified that relates to a specific incident a longer period may be justifiable for the particular section of footage concerned, such as in the investigation of a workplace accident or where footage may be used as evidence in criminal proceedings. This footage should be isolated from the general recordings and kept securely for the purposes that has arisen.

Disclosure of CCTV to Third Parties

On occasion, a data controller may be asked to disclose CCTV recordings to third parties for a purpose other than that for which they were originally obtained. This may arise, for example, where a request is received from An Garda Síochána or another law enforcement body to provide footage to assist in the investigation of a criminal offence. In these circumstances, it is recommended that requests for copies of CCTV footage should only be acceded to where a formal written request is provided to the controller stating that An Garda Síochána (or other law enforcement body) is investigating a criminal matter. For practical purposes, and to expedite a request speedily in urgent situations, a verbal request may be sufficient to allow for the release of the footage sought. However, any such verbal request should be followed up with a formal written request. For accountability purposes a record of all Garda Síochána requests should be maintained by data controllers and processors detailing any provision of footage.

Where a data controller is asked to provide CCTV footage to a third party to investigate an incident, the same assessment procedure as applied for the original purpose should be applied to the new purpose to determine if it can be justified in the pursuit of a genuinely legitimate interest of the data controller or another party. Such eventualities will need to be assessed on a case-by-case basis to ensure that the principles of data protection are adhered to, and the rights of individuals are not prejudiced. It should be noted that the legitimate interests of a third party do not oblige a data controller to disclose CCTV footage but may permit such disclosure subject to assessment.

Questions to ask when designing or reviewing a CCTV system

Apart from the necessity of a DPIA, controllers should consider the following topics when they create their own video surveillance policies and procedures:

- Who is responsible for management and operation of the video surveillance system.
- Purpose and scope of the video surveillance project.
- Procedures for system procurement, installation and maintenance.
- Appropriate and prohibited use (where and when video surveillance is allowed and where and when it is not; e.g. use of hidden cameras and audio recording).
- Transparency and information obligations.

- How video is recorded and for what duration, including archival storage of video recordings related to security incidents.
- Who must undergo relevant training and when.
- Who has access to video recordings and for what purposes.
- Operational procedures (e.g. by whom and from where video surveillance is monitored, what to do in case of a data breach incident).
- What procedures external parties need to follow in order to request video recordings, and procedures for denying or granting such requests.
- Incident management and recovery procedures.

Issues that might be examined in a school environment include:

5. What is the school's purpose for using CCTV images? What are the issues/problems it is meant to address?
6. Is the system necessary to address a pressing need, such as staff and student safety or crime prevention?
7. What are the benefits to be gained from its use?
8. Can CCTV systems realistically deliver these benefits? Can less privacy-intrusive solutions, such as improved lighting, achieve the same objectives?
9. Will the system being considered deliver the desired benefits now and remain suitable in the future?
10. Are internal CCTV cameras justified under the circumstances?
11. Are internal CCTV cameras proportionate to the problem they are designed to deal with?
12. Can the location of each internal camera be justified in accordance with the overall purpose for the use of the CCTV system?
13. What future demands may arise for wider use of images and how will they be addressed?
14. Is the school acting as data controller for the entire CCTV system?
15. What are the views of those who will be subject to CCTV monitoring?
16. What could be done to minimise intrusion for those whose images may be captured, particularly if specific concerns have been expressed?
17. Will staff, students and visitors be confident that the CCTV system will be used only for the stated purposes?
18. Has appropriate signage been erected at the general location of each internal camera indicating that recording is taking place?
19. What security measures are in place to protect the CCTV system and recordings/images?
20. Who will have access to the system and recordings/images?
21. Are those who will have authorised access clear about their responsibilities?
22. Are monitors kept out of view with access restricted to a limited number of staff on a 'need to know' basis?
23. Is the room(s) which houses the camera monitors and the CCTV system secure when unattended?
24. Does the school have a procedure in place to ensure that recordings/images are erased or deleted as soon as the retention period (30 days) has expired?
25. Do school staff have an understanding about the process for handling requests for access to recordings/images from An Garda Síochána?
26. Has the right of access been communicated to staff, students and visitors?
27. Does the school have a procedure in place to handle access requests seeking a copy of images recorded by the CCTV system?
28. Has the school communicated its Policy on the use of CCTV to staff, students and visitors and how has this been done?

Appendix 2. SOURCE DOCUMENTS & WEBSITES

Data Protection Tookit for Schools (version published December 2024)
https://www.dataprotection.ie/sites/default/files/uploads/2024-12/DataProtection-ToolkitforSchools_EN_0.pdf

Note: The DPC Toolkit for Schools includes advice on CCTV in schools (which is reproduced in Appendix 1 of this JMB Template). The DPC Toolkit also includes an appendix (p64-76) that addresses how a school should carry out a Data Protection Impact Assessment (DPIA). The other DPIA Template published by the DPC (link included below) is aimed at a more general audience.

Guidance on the Use of CCTV – For Data Controllers. Data Protection Commission (latest version November 2023)
https://www.dataprotection.ie/sites/default/files/uploads/2023-12/CCTV%20Guidance%20Data%20Controllers_November%202023%20EN.pdf

A Practical Guide to Controller-Processor Contracts. Data Protection Commission
https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190624%20Practical%20Guide%20to%20Controller-Processor%20Contracts.pdf

Guidance for Controllers on Data Security. Data Protection Commission (latest version February 2020)
https://dataprotection.ie/sites/default/files/uploads/2020-04/Data_Security_Guidance_Feb20.pdf

Guidelines 3/2019 on processing of personal data through video devices. European Data Protection Board.
https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en

Data Protection Impact Assessment Template. Data Protection Commission
https://dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments#sample-dpia-template