



CCTV - Guide for best practice

Guidance document for CCTV systems in schools/centres/administration offices.

This document should be read in conjunction with LMETB CCTV Policy and CCTV Privacy Notice.

Version 2.0, May 2023

TABLE OF CONTENTS

1. DATA PROTECTION IMPACT ASSESSMENT (DPIA)	4
2. JUSTIFICATION FOR THE USE OF CCTV	4
3. LOCATION OF CCTV CAMERAS	5
4. COVERT SURVEILLANCE	5
5. NOTIFICATION AND SIGNAGE	6
6. MANAGEMENT, CONTROL AND ACCESS.....	7
7. GARDA REQUESTS	8
8. CCTV/SECURITY COMPANIES.....	9
9. IMPLEMENTATION AND REVIEW	9
APPENDIX 1: DEFINITIONS	10
APPENDIX 2: CCTV SIGNAGE	11
APPENDIX 3: PROCEDURE FOR MANAGING CCTV FOOTAGE REQUESTS FROM AN GARDA SÍOCHANA.....	13
APPENDIX 4: TEMPLATE TEXT TO ACCOMPANY RELEASED FOOTAGE	14
APPENDIX 5: TEMPLATE DATA PROTECTION IMPACT ASSESSMENT.....	15
APPENDIX 6: CCTV ACCESS CONTROL SHEET.....	19
APPENDIX 7: CCTV COVERT RECORDING REQUEST FORM	20
APPENDIX 8: AUTOMATED NUMBER PLATE RECOGNITION (ANPR)	22

Introduction

This document is designed to provide guidance to Schools/Colleges/Centres and Administration Offices on the installation and management of CCTV systems. It contains advice on choosing appropriate locations of cameras and on the security and management of CCTV. Particular emphasis is given to the importance of conducting a Data Protection Impact Assessment (DPIA) before installation of any proposed CCTV system or camera, or before carrying out any significant amendments to existing CCTV systems.

This document should be read in conjunction with:

- LMETB's CCTV Policy
- LMETB's Data Processing Policy

The use of any CCTV system must be conducted in a professional, ethical and lawful manner. Any use of CCTV for any other purposes other than those outlined in LMETB's CCTV Policy or CCTV Privacy Statement can only commence if there is a clear and sound legal basis, supported by a prior Data Protection Impact Assessment (DPIA), and/or there is a clear legal obligation.

This document is intended as a general guidance document only and is subject to change. Always consult your Data Protection Officer if you are considering installation, amendment or upgrading of a CCTV system or equipment.

1. Data Protection Impact Assessment (DPIA)

The General Data Protection Regulation refers to the mandatory requirement for a DPIA:

*“Where a type of processing in particular using new technologies...**is likely to result in a high risk to the rights and freedoms of natural persons**, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.”*

CCTV systems are considered ‘high risk,’ particularly because if they are not carefully installed and managed, they can potentially involve unreasonable and unlawful interference with the data protection rights and privacy rights of individuals, and with their freedom to behave naturally. It is therefore mandatory to carry out a DPIA on all installations: the appropriate time to do so is prior to the procurement of a new CCTV system, prior to the installation of additional camera(s), or prior to the upgrading of systems that introduce additional functions that might intrude on people’s right to privacy in unexpected ways or lead to ‘function creep’ (usage for new purposes not originally planned for). Examples of such functions are:

- Auto tracking (cameras detecting and following movement)
- Audio recording
- Pan, tilt, zoom and panoramic view-enabled cameras
- Automated number plate recognition (ANPR) and facial recognition
- Remote monitoring, either online or via an offsite security company, for example.

This list is inevitably non-exhaustive, as technological developments and new features are constantly emerging.

For existing CCTV systems, periodic reviews, to include a DPIA, must also be carried out.

A DPIA template is included at Appendix 5 of this document.

2. Justification for the use of CCTV

Personal data should not be collected on a “just-in-case” basis but only where there is a clearly identified purpose. LMETB must therefore be able to justify the installation of CCTV systems and cameras on any LMETB premises, and only after less intrusive measures have been considered. The DPIA referred to above and elsewhere in this document offers detailed assistance to LMETB seeking to assess and demonstrate whether CCTV is justified.

3. Location of CCTV Cameras

CCTV cameras must be positioned where they are least intrusive to the people using the building and its grounds. Locating cameras in areas where individuals would have a reasonable expectation of privacy would be difficult to justify e.g. classrooms, changing facilities, toilets. If you are in any doubt over whether a camera poses a risk to the privacy rights of an individual, consult your Data Protection Officer beforehand.

External cameras should be positioned in such a way as to prevent or minimise the recording of passers-by or neighbouring private properties. The CCTV cameras should only capture images within the perimeter of the ETB premises.

Examples of CCTV installation may include the following:

- **Protection of School/College/Education & Administrative Centre Buildings and property** - Building perimeter, entrances and exits, lobbies and corridors, special storage areas, server rooms, cashier locations, receiving areas for goods/services, roof access points (especially on multi-storey premises) and any areas considered high risk from a Health and Safety perspective.
- **Investigation of activations of Alarms**, alarms, exit door controls, external alarms and/or restricted access points.
- **Monitoring of specific external areas:** parking areas, main entrance/exit gates, Traffic Control, grounds, bicycle sheds.
- **Protection of Pedestrians** - pedestrian and vehicle traffic activity within the perimeter.

This is a non-exhaustive list. Locations chosen must be consistent with the permitted purposes listed in the CCTV Policy.

4. Covert Surveillance

Covert surveillance (i.e. where the data subject is unaware that they're being filmed), must only be implemented in strictly exceptional cases, for the purposes of preventing, detecting or investigating serious offences, or apprehending or prosecuting offenders. Hence it must not be considered without the active prior involvement of An Garda Síochána or other prosecutorial authority.

Where An Garda Síochána requests to carry out covert surveillance on LMETB premises, such covert surveillance may require the consent of a Judge. Accordingly, any such request should be made in writing and LMETB will seek legal advice where necessary. (See Appendix 7 for request form).

5. Notification and Signage

Data subjects are entitled to fair warning of the existence of CCTV in operation at any LMETB site. This should follow a layered approach, in the following order:

1. **CCTV signage** – the sign at Appendix 2 below must be displayed prominently as follows:

External signage

External signage must be prominently displayed at the perimeter gates of the ETB premises, and at any other entrance to the site. The sign should give adequate warning to would-be visitors that they are about to enter an area that is monitored by CCTV. Signage should also be placed at any entrance door to the premises.

Internal Signage

Signage shall be placed internally in each premises in the vicinity of where CCTV cameras are located and at all exits to outdoor areas that are also captured by filming, to inform people that CCTV is in operation in that area.

2. A **CCTV Privacy Notice** (see Appendix of the CCTV Policy) – to be displayed on arrival at the building, e.g. in reception.
3. The **CCTV Policy** – to be available as a link in the signage and Privacy Notice (items 1. & 2. above), or on request from the school/centre or via the Data Protection Officer's (DPO) email address.

6. Management, Control and Access

The CCTV system - monitoring screens, system controls and the system hard drive - must be kept in a secure location. Access to this area must be restricted to authorised persons only e.g., Principal/Manager/Coordinator, the Gardaí, approved third-party CCTV contractors. 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. Where available, access to the system should be protected by password/PIN, with a unique password/PIN issued to each user. Access must be promptly revoked if the staff member ceases to work for the organisation.

In general, CCTV should not be used as an indiscriminate live monitoring tool, unless a particular matter is brought to the attention of management that requires such monitoring and further investigation e.g., reports of ongoing anti-social behaviour in a particular location, reasonable suspicion of theft. In the event that such monitoring requires further action or intervention on the part of management, details of this should be kept in a log which may need to be produced in the event of a Data Subject Access Request, or as evidence in legal proceedings, or in respect of an insurance claim, but primarily to show that such monitoring was proportionate and justified.

In relevant circumstances, CCTV footage may be shared with or transferred to certain other bodies/agencies where/when LMETB is required to do so. A non-exhaustive list of such recipients can be found in the LMETB CCTV Policy under the heading "Recipients of CCTV Recordings." If you are in any doubt over whether footage may be shared, consult your Data Protection Officer (DPO) beforehand.

Under the GDPR, individuals have the right to request a copy of any of their personal data which are being held or used in any way by LMETB – a so-called Data Subject Access Request. Remember that such requests must be responded to within one month and should be immediately notified to your DPO upon receipt. The DPO will examine the request, and advise on any further steps e.g., the requirement for pixilation of the footage to prevent the release of images of any third parties.

The recommended maximum retention period for CCTV footage is 30 days. A shorter period is permissible if required, but footage should not be retained for longer than 30 days, unless it is required as part of an ongoing investigation or Data Subject Access Request or Garda request.

7. Garda Requests

From time to time, An Garda Síochana may approach LMETB if they believe that CCTV footage may be of assistance with an investigation.

If they make their request by phone or in person, they should be advised that the request must be made in writing and forwarded to dataprotection@lmetb.ie immediately.

If a school/centre receives a data access request from a member of An Garda Síochana please ensure the following:

- ✓ It must be received in writing on official Garda letterheaded paper - this can be sent by post or as an attachment to an email,
- ✓ You must advise your Data Protection Officer of the request immediately,
- ✓ It must indicate that it is for the prevention, detection, investigation or prosecution of a criminal offence,
- ✓ The request must state that it is made pursuant to section 41(b) of the Data Protection Act 2018,
- ✓ The request must be signed by a Garda of the rank of Superintendent, or above,
- ✓ It must include the requesting Garda's name and badge number,
- ✓ It must include the investigation pulse number.

The data protection office will contact the school/centre to discuss the request and give guidance. When responding, include a cover letter with the data being provided - use the template text at Appendix 4 below.

In each case, any footage disclosed should be limited to what is necessary and proportionate in the circumstances. This is a matter of judgement and can often be difficult to determine. For example, it would not always be proportionate to release a week's worth of footage if the matter under investigation only concerns a 30-minute window.

Always seek the advice of the Data Protection Office if in doubt.

Section 41 of the Data Protection Act 2018

“Without prejudice to the processing of personal data for a purpose other than the purpose for which the data has been collected which is lawful under the Data Protection Regulation, the processing of personal data and special categories of personal data for a purpose other than the purpose for which the data has been collected shall be lawful to the extent that such processing is necessary and proportionate for the purposes

- a) *of preventing a threat to national security, defence or public safety*
- b) *of preventing, detecting, investigating or prosecuting criminal offences, or*
- c) *set out in paragraph (a) or (b) of section 47.”*

8. CCTV/Security companies

The ETB may decide to engage a contractor or professional that installs, monitors, or provides maintenance for a CCTV system. Their services may also extend to video extraction, video redaction, pixelation, remote monitoring and other services.

Any such any provider used by LMETB for this purpose will probably be classified as a data processor if it has access to the recorded images of individuals, and will be required to guarantee that it has appropriate security measures in place to prevent any unauthorised access, alteration, disclosure, or destruction of any LMETB data (images) it may access or handle. Providers must also be made aware of their data protection obligations when processing the data, including their duty to support accuracy of data by achieving and maintaining high technical standards in the imagery produced. Providers and their staff must be bound by a strict duty to keep all footage confidential. To help put these measures into effect, LMETB is required to have a Data Processing Agreement in place with any such CCTV business. Please contact your DPO who can make the necessary arrangements.

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.

9. Implementation and Review

Document Reference Number	CCTV Guide
Revision Number	002
Document Reviewed By	ETBI DP & FOI Forum
Review Date	May 2023
Date of Original Policy Implementation (Version 1)	May 2018
Previous Review Dates	N/A
Next Review Date	May 2025

Appendix 1: Definitions

CCTV – Closed Circuit Television is the use of video cameras to electronically capture and record images on tape, DVD, or a digital recording mechanism.

Data – information in a form that can be processed electronically or manually. Footage or images containing identifiable individuals captured by CCTV systems are personal data for the purposes of data protection law.

Data (Subject) Access Request (aka DSAR or DAR) – where a data subject makes a request to LMETB for the disclosure of their personal data as per their rights under Data Protection Law.

Data Controller – a person or organisation who controls the contents and use of personal data. For the purposes of this guidance document, LMETB is a data controller.

Data Processing – performing any operation or set of operations on data, including:

- Obtaining, recording or keeping the data
- Collecting, organising, storing, altering or adapting the data
- Retrieving, consulting or using the data
- Disclosing the data by transmitting, disseminating or otherwise making it available
- Aligning, combining, blocking, erasing or destroying the data

Data Processor – a person or organisation who processes personal data on behalf of a data controller

Data Subject – an individual who is the subject of the personal data, e.g. anyone recorded by a CCTV system

DPIA – a Data Protection Impact Assessment is a mandatory requirement under the GDPR for all high-risk data processing systems, of which CCTV is likely to be one.

GDPR – the General Data Protection Regulation applies to the processing of personal data in the EU, setting out more extensive obligations on data controllers and processors, and providing strengthened protections for data subjects. In Ireland, the national law which gives further effect to the GDPR is the **Data Protection Act 2018**.

Personal Data – Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.



Appendix 2: CCTV SIGNAGE

Insert School/Centre/logo



RABHADH CEAMARAÍ TCI I BHFEIDHM

Tá an córas seo á rialú ag <Name>School/Centre agus BOOLM agus á fheidmiú chun na críocha seo a leanas: iompar frithshóisialta, bulaíocht agus coireacht a chosc; ar mhaithe le sábháilteacht na foirne, na ndaltaí agus na gcúairteoirí; ar mhaithe le slándáil agus cosaint BOOLM agus a mhaoín; chun críocha fíoraithe agus réitigh díospóidí, go háirithe in imthosca ina bhfuil díospóid ann maidir le fíorais agus ina bhféadfadh na taifeadtaí a bheith in ann an díospóid sin a réiteach, agus; a chinntiú go gcomhlíontar rialacha agus beartais BOOLM maidir le sláinte agus sábháilteacht, slándáil, iompar agus smacht.

Beidh an córas seo i bhfeidhm 24 uair sa lá, gach lá. Más gá, is féidir taifeadtaí a chur ar aghaidh chuig an nGarda Síochána agus/nó ár gcomhairleoirí dlí/árachóirí.

Le heolas iomlán a fháil faoi chuspóirí agus úsáidí taifeadtaí, féach le do thoil ar Pholasaí TCI BOOLM agus Fógra Príobháideachta TCI ag www.lmetb.ie

Chun tuilleadh eolais a fháil faoi oibriú an chórais seo, déan teagmháil le **NAME AND CONTACT
DETAILS OF PERSON RESPONSIBLE FOR MANAGING CCTV SYSTEM AT THAT LOCATION**

Cé go ndéantar gach iarracht a chinntiú go bhfuil ár gcóras TCI agus ár gceamaraí ag feidmiú i gceart, ní féidir aon ráthaíocht a thabhairt maidir le hinfhaighteacht nó cáilíocht aon taifeadta nó maidir leis an taifeadadh a bheith ann.



WARNING

CCTV CAMERAS IN OPERATION

This system is controlled by **<Name>School/Centre** and LMETB and operated by for the following purposes: preventing anti-social behaviour, bullying and crime; for the safety of staff, students and visitors; for the security and protection of LMETB and its property; for verification and dispute resolution purposes, particularly in circumstances where there is a dispute as to facts and the recordings may be capable of resolving that dispute, and; to ensure compliance with LMETB's rules and policies on health and safety, security, behaviour and discipline.

This system will be in operation 24 hours a day, every day. If necessary, recordings may be passed to An Garda Síochána and/or our legal advisors/insurers.

For full information about purposes and uses of recordings, please see LMETB CCTV Policy and CCTV Privacy Notice at www.lmetb.ie

For more information about the operation of this system, contact **NAME AND CONTACT DETAILS OF PERSON RESPONSIBLE FOR MANAGING CCTV SYSTEM AT THAT LOCATION**

While every effort is made to ensure our CCTV system and cameras are working properly, no guarantee can be given as to the existence, availability or quality of any recording.

Appendix 3: Procedure for managing CCTV footage requests from An Garda Síochana

1505297502090_PastedImage

CCTV Footage Requests from An Garda Síochana - Procedure

If a school/centre receives a request for CCTV footage from a member of An Garda Síochana please ensure the following:

- ✓ It must be received in writing on official Garda letterheaded paper - this can be sent by post or as an attachment to an email,
- ✓ You must advise your Data Protection Officer of the request immediately,
- ✓ It must indicate that it is for the prevention, detection, investigation or prosecution of a criminal offence,
- ✓ The request must state that it is made pursuant to section 41(b) of the Data Protection Act 2018,
- ✓ The request must be signed by a Garda of the rank of Superintendent, or above,
- ✓ It must include the requesting Garda's name and badge number,
- ✓ It must include the investigation pulse number.

Please forward the request to dataprotection@lmetb.ie without delay.

The data protection office will contact the school/centre to discuss the request and give guidance.

Data disclosed should be minimised and only include what is necessary and proportionate in the circumstances.

Appendix 4: Template text to accompany released footage

School/Centre Headed Paper

DATE

NAME

ADDRESS

RE: Request for data pursuant to Section 41(b) of the Data Protection Act 2018.

Dear XXXXXXXX,

I refer to your letter/email dated DATE which was received on DATE requesting for data held by SCHOOL/CENTRE NAME. I now formally respond to today, DATE. I would like to thank you for your patience with this process. Your request sought:

[COPY WORDING]

I can confirm to you that this process involved the retrieval of NUMBER records which I have numbered and attached.

I wish to confirm that SCHOOL/CENTRE NAME has done everything reasonably possible to comply with your request for data which has been processed under Section 41(b) of the Data Protection Act 2018.

Yours sincerely,

Principal/Deputy Principal/Co-ordinator name,
School/Centre name

Appendix 5: Template Data Protection Impact Assessment



CCTV Data Protection Impact Assessment

Name of School / Centre:		Date of DPIA:		DPIA undertaken by:	
--------------------------	--	---------------	--	---------------------	--

Name of Installation Company:		PSA Licence Number:		Licence Expiry Date:	
-------------------------------	--	---------------------	--	----------------------	--

This assessment should be completed prior to all new installations, additional camera/hardware installations, new functionality being added to existing systems, e.g. ANPR; and for any periodical review at the direction of the LMETB's Data Protection Officer.

Please note:

- **Dummy/non-operational cameras do not record data subjects, and hence as no data processing occurs, they fall outside the scope of this guidance.**
- **Where required, the CCTV contractor should assist with the completion of this DPIA and provide any necessary information.**
- **The Guidance Notes in each section below refer to the principal considerations to be taken into account, but please refer to LMETB CCTV - Guide for best practice document for further assistance.**

No:	JUSTIFICATION	RESPONSE
1.	What is the purpose for the installation of the proposed CCTV camera(s)?	
<p><i>Question 1 Guidance Notes:</i></p> <ul style="list-style-type: none"> • <i>What are the issues/problems that the images will be used to address (for example: Is the system necessary to address a pressing need, such as staff and student safety and/or crime prevention, as opposed to something fictional or speculative?)</i> • <i>What evidence base exists for this issue/problem? (Refer to any evidence on file, e.g., a log of security/behavioural incidents, accidents/near misses, complaints records, surveys etc) – this may need to be gathered over time to strengthen any argument for justifying installation of CCTV.</i> • <i>Is the installation of this CCTV system and/or the addition of extra cameras and/or the relocation of existing cameras justified under the circumstances, in light of the issues identified?</i> 		
2.	Does the purpose comply with the permitted grounds for installation as outlined in LMETB's CCTV Policy and Data Processing Policy and LMETB CCTV – Guide for best practice ?	
<p><i>Question 2 Guidance Notes:</i></p> <ul style="list-style-type: none"> • <i>Refer to LMETB CCTV - Guide for best practice, CCTV Policy and Data Processing Policy for further information.</i> 		
3.	Is it possible that other less intrusive methods or solutions could achieve the same objective?	

<p><i>Question 3 Guidance Notes:</i></p> <ul style="list-style-type: none"> • <i>Could less privacy-intrusive solutions, such as improved lighting, perimeter security (locks, windows, door, fencing), walkabouts, security patrols, gatekeepers or non-continuous monitoring, achieve the same objectives?</i> • <i>Could enhanced supervision in the specific area negate the requirement for use of CCTV?</i> • <i>Would the provision of anti-graffiti paint/surfaces negate the requirement for CCTV installation?</i> 		
4.	Does the proposal to install the CCTV camera(s) follow a recommendation from LMETB’s Insurance provider?	
No:	LOCATION OF CAMERAS	RESPONSE
5.	Does the location(s) of the proposed external CCTV camera(s) comply with the guidelines issued in LMETB’s CCTV Policy and Guide for best practice on the positioning of the camera(s) within the perimeters of the campus?	
<p><i>Question 5 Guidance Notes:</i></p> <ul style="list-style-type: none"> • <i>Are external cameras justified under the circumstances?</i> • <i>Are external cameras a balanced approach to the problem they are designed to deal with?</i> • <i>If a portion of a camera/s covers a public area, and the camera angle/focus cannot be adjusted to avoid this, can image masking/cloaking (physical obstruction of a portion of the lens) be used?</i> • <i>If it is not possible to minimise intrusion in a public area, please list the reasons why.</i> • <i>Where it is not possible to mitigate the risk of capturing detailed images of neighbouring properties or passers-by, the Data Protection Commission must be contacted for further guidance.</i> 		
6.	Does the location(s) of the proposed internal CCTV camera(s) comply with the guidelines issued in ETB’s CCTV Policy and Guide for best practice on the positioning of internal camera(s)?	
<p><i>Question 6 Guidance Notes:</i></p> <ul style="list-style-type: none"> • <i>Are internal cameras justified under the circumstances?</i> • <i>Are internal cameras a balanced approach to the problem they are designed to deal with?</i> • <i>Will cameras intrude on the privacy rights of individuals, especially in areas where there is a legitimate and enhanced expectation of privacy (e.g., at work, learning, or in bathrooms, changing rooms, classrooms, staffrooms, canteens, offices etc).</i> • <i>If it is not possible to minimise intrusion in these areas, please list the reasons why, providing evidence as backup (e.g., incident reports, surveys etc).</i> • <i>If the system, and its cameras have additional features (e.g., ability to rotate, pan, tilt, zoom etc.) will this be clearly detailed in the CCTV policy?</i> • <i>Where it is not possible to avoid or mitigate the risk of capturing CCTV images in these areas, serious consideration should be given to the possibility of not proceeding with installation, and other methods of achieving the desired results explored. If there is a fully justifiable reason for why the installation of the camera should proceed despite an obvious high risk to privacy, the Data Protection Commission must be contacted for further guidance.</i> 		
7.	Have occupants of the building (staff, students) been notified of the proposed location(s) / relocation of the CCTV camera(s), affording them an opportunity to provide their feedback, suggestions or to voice their concerns?	
<p><i>Question 7 Guidance Notes:</i></p> <ul style="list-style-type: none"> • <i>In the interest of fairness and transparency have staff and students been informed of the reasons why their images will be captured? How was this done?</i> 		

	<ul style="list-style-type: none"> • Have the views of staff and students regarding the location of cameras been taken into account? • Have they been informed of the intention to use the images only for the purposes stated? • Have they been informed that no covert monitoring of staff or students is permitted? 	
8.	Has the location for appropriate CCTV Signage been considered, taking into account the right of students, staff, visitors and stakeholders to be notified of the presence and operation of the CCTV system?	
<p><i>Question 8 Guidance Notes:</i></p> <ul style="list-style-type: none"> • Have appropriate signage locations been identified, e.g., at entrance points to the building and at site boundaries to the property and close to the operational area of cameras generally? • Have appropriate locations for internal signage been identified, i.e., near the location of each area monitored by cameras? • Are the proposed signs compliant with the signage template in LMETB CCTV – Guide for best practice document, both in Irish and English? 		
No:	MANAGEMENT, CONTROL AND ACCESS	RESPONSE
9.	Will there be a CCTV/Security professional or business supporting your CCTV system?	
<p><i>Question 9 Guidance Notes:</i></p> <ul style="list-style-type: none"> • Has a Data Processing Agreement (DPA) been drawn up, clearly outlining the respective duties of controller (ETB) and processor (the professional/business)? • Does the professional/business have a valid license from the Private Security Authority (PSA)? • Has the professional/business been consulted in the compilation of this DPIA? 		
10.	Who will have operational responsibility for managing the CCTV system in the school or centre, on a day-to-day basis?	
<p><i>Question 10 Guidance Notes:</i></p> <ul style="list-style-type: none"> • Please provide name and contact details • Ensure that responsibility for management of the system rests with the minimum number of staff, on a needs-must basis – but sufficient to provide cover in the event of absences. 		
11.	Please identify the staff members who will have authorised access to the CCTV system, and/or the CCTV management company contact details (if applicable).	
<p><i>Question 11 Guidance Notes:</i></p> <ul style="list-style-type: none"> • Please name and provide contact details for all personnel who have access to the CCTV system • Ensure that responsibility for access is granted to the minimum number of staff, on a needs-must basis – but sufficient to provide cover in the event of absences. 		
12.	Please advise how changes to authorised access levels will be managed (starters and leavers).	
<p><i>Question 12 Guidance Notes:</i></p> <ul style="list-style-type: none"> • Please outline procedures in place for prompt addition / retraction of authorised permissions e.g., return of keys to CCTV control room, changing of PIN access to CCTV control panel 		
13.	If remote viewing access is going to be a feature of the system, you must contact your DPO and/or ICT Support to establish if such use is permitted?	

<p>Question 13 Guidance Notes:</p> <ul style="list-style-type: none"> • If the system is to be controlled/monitored online via app or website, wirelessly or otherwise remotely, will this be done on an ETB-approved device with appropriate security measures, e.g., encryption, regular software updates, etc.? • If a third-party e.g., security firm is used, has a Data Processing Agreement been put in place (see Q9 above)? • Contact your DPO for guidance 		
14.	How is access managed, controlled and logged in the event of an incident or request for footage?	
<p>Question 14 Guidance Notes:</p> <ul style="list-style-type: none"> • How is access managed, controlled and logged in the event of an incident or request for footage? • Is a CCTV Access Control Sheet used to record each time CCTV footage is accessed? 		
15.	Will a secure room/area be available where monitoring screens and recorded footage can be held, keeping in mind that access to this room must be restricted?	
<p>Question 15 Guidance Notes:</p> <ul style="list-style-type: none"> • Are the camera monitors kept out of the view of staff, students and visitors? • Is the room(s) which houses the camera monitors and the CCTV system securely locked when unattended? • Access to the CCTV system must be restricted to authorised personnel only as outlined in LM ETB's CCTV Policy and LMETB CCTV – Guide for best practice. 		
16.	What protocols are in place, or will be put in place for requests for images, and the viewing, extraction and/or removal of same?	
<p>Question 16 Guidance Notes:</p> <ul style="list-style-type: none"> • Is the retention period set to a maximum of 30 days? • A procedure for handling requests for information from An Garda Síochána is contained in LMETB CCTV – Guide for best practice.. • Is there a procedure in place to handle data subject access requests seeking a copy of images recorded by the CCTV system (within the statutory timeframe of 30 days)? • If digital extraction is available, does the school/centre have access to pixelation services where multiple parties recorded need to be obscured from recordings? • If digital extraction is available but not viable, provision of manual, screen-grab extractions is required at a minimum rate of one frame per second. • If a pixelation service is available, is a data processing agreement in place with the provider of that service? 		
No:	NOTIFICATION	RESPONSE
17.	How will students, staff, visitors and stakeholders be notified of the presence and operation of the CCTV system?	
<p>Question 17 Guidance Notes:</p> <ul style="list-style-type: none"> • Will approved Irish and English signage be placed in the appropriate area close to the operational area of cameras? (Refer again to Question 8 above) • Can the CCTV Privacy Notice be placed in a location where it will readily be seen e.g., on a reception message board? • Will the school/centre make the LMETB CCTV policy readily available on request e.g., in a convenient location such as 'Policies' on its website. 		

Please return this completed draft copy to your Data Protection Officer (DPO) for approval to dataprotection@lmetb.ie Additional evidence/information may be required before installation is granted

Appendix 6: CCTV Access Control Sheet

Insert School/Centre/ logo



CCTV Access Control Sheet

ACCESS DETAILS			
Date of access:		Accessed by:	
Time of access:		Access approved by:	
Access purpose: <input type="radio"/> Internal review <input type="radio"/> Garda Síochána request <input type="radio"/> Other (please specify).....			
INCIDENT / EVENT SEARCH DETAILS			
Date being reviewed:		Time span being reviewed:	
Camera number/s reviewed:		Location/s:	
Reason for accessing footage:			
Description of what was observed:			
DATA PROCESSING ACTIONS			
Was data and/or images and/or footage extracted? <input type="radio"/> Yes <input type="radio"/> No			
If extracted, total number of individual files extracted:			
Extracted files stored: <input type="radio"/> PC Hard Drive <input type="radio"/> CD <input type="radio"/> Encrypted Memory Stick <input type="radio"/> Other (specify).....			
Do extracted images need to be redacted? <input type="radio"/> Yes <input type="radio"/> No			
Has a back-up copy been created and retained safely? <input type="radio"/> Yes <input type="radio"/> No			
Who is responsible for the extracted files?			
Who is responsible for the back-up files?			

Signature of Principal / Centre Manager:

Date:

Appendix 7: CCTV Covert Recording Request Form



CCTV Covert Recording Request Form

REQUESTOR DETAILS			
<p>Please note: Any request for installation of covert surveillance using CCTV equipment must:</p> <ul style="list-style-type: none"> • be requested by the Principal or Manager of the location where the surveillance is required, and; • be recommended by the Director of that section, before; • being submitted to the Chief Executive for final decision. <p>Covert surveillance (i.e., where the data subject is unaware that they're being filmed), must only be implemented in strictly exceptional cases, for the purposes of preventing, detecting or investigating serious offences, or apprehending or prosecuting offenders. Hence it must not be considered without the active prior involvement of An Garda Síochána or other prosecutorial authority.</p>			
Name of Requestor:		Position Held:	
Date of Request:		Proposed location for Recording:	
Installation purpose: <input type="radio"/> Internal request (please specify below) <input type="radio"/> Garda Síochána request (please specify below or attach documentary request)			
Proposed Installation Date:		Proposed Removal Date:	

INSTALLATION COMPANY DETAILS			
Installation Company:		PSA Licence Number:	
Installer Name:		PSA Licence Expiration Date:	

EQUIPMENT & CAMERA DETAILS			
Will proposed cameras be added to existing system?		<input type="radio"/> Yes <input type="radio"/> No	
If installed as a new/stand-alone system: <ol style="list-style-type: none"> Where will this monitoring/recording system be located? Who will have access to the equipment? (specify names) Will the system be remotely monitored? If remotely monitored, who will monitor it and why is it required? 			
Location of Camera 1:		Camera 1 Model/Description:	
Field of view Camera 1: (What will this device capture?):			

Location of Camera 2:		Camera 2 Model/Description:	
Field of view Camera 2: (What will this device capture?):			
SIGNATURES			
Signature of Principal / Centre Manager:		Signature of Director:	
FINAL DECISION			
Application:	<input type="radio"/> Approved <input type="radio"/> Declined	C.E. Signature:	Date:

Appendix 8: Automated Number Plate Recognition (ANPR)

Typically used by police forces to identify vehicles of interest, this is now offered as a feature on commercial and domestic CCTV systems too, as a means of distinguishing approved visitors from unwelcome intruders.

Any consideration of such a system must be preceded by a robust DPIA. The following non-exhaustive list of points should also be borne in mind:

- Any use of recognition systems must be justified and proportionate, lawful, necessary, and the amount of data captured by such a system kept to a minimum.
- Where a system identifies a non-approved vehicle, human intervention should always follow before any decision is taken that might affect an individual adversely. In other words, the approved operator should investigate before taking any further action.
- The system should automatically delete material after a limited timeframe – this is less intrusive than constantly reviewing the recorded footage.
- Any list or database compiled for the purposes of identifying ‘permitted’ individuals i.e., registration numbers of vehicles that are approved to drive into a premises, must be kept up-to-date and accurate, and of sufficient quality to prevent mismatches. The criteria for the data to be included on such lists must be clear, proportional and kept to a minimum, and access limited on a strictly needs-must basis. Operators or ANPR-enabled systems must ensure they have the necessary administrative resources to support this requirement.
- A clear procedure for what happens when system identifies a non-approved registration number must be established and followed, particularly for distinguishing between vehicles that present a concern and those that don’t. For example, an approved student or staff member may decide to leave their car at home and take a lift with a non-approved driver.
- The comments made earlier in this document in relation to system technical quality and accuracy apply equally here: poor quality of vehicle registration plates can cause poor or inaccurate data.