

HSE CCTV National Policy

National Policy ☒ National Procedure ☐ National Protocol ☐ National Guideline ☐ National Clinical Guideline ☐

HSE National CCTV Policy

DOCUMENT GOVERNANCE [1]			
Document Owner (post title):		Head of Data Protection Office	
Document Owner name:		Mary Deasy	
Document Owner email: (Generic email addresses only accepted)		DPO@hse.ie	
Document Commissioner(s): (Name and title of post holder):		Mary Deasy, Data Protection Officer	
Date Document Approved: **(**Formal ratification by the Governance/Steering Group)		08/09/2026	
Document Approved by: (Name and title of post holder)		Mary Deasy, Data Protection Officer	
Document Approver Sign-off: (e-signature)		Mary Deasy.	
Document Approver Registration number: (where applicable)			
Development Group Chair		Mary Deasy	
Development Group Name:		CCTV Policy Working Group	
DOCUMENT MANAGEMENT [2]			
Date effective from:		08/09/2026	
Date set for next review:		10/09/2029	
Current version no:	0	**Archived version no:**	N/A
Note: Original document is Version 0. First revision is Version 1. Second revision is Version 2, and so on.			
Note: HSE National PPPGs and Clinical Guidelines should be formally reviewed every 3 years, unless new legislative/regulatory or emerging issues/research/technology/audit etc. dictates sooner.			

[1] Records the governance and approval of the document.
[2] Records the control information about the document.

VERSION CONTROL UPDATE [3]		
Version No. (most recent version first)	**Date reviewed** (most recent date first)	**Comments** (1 sentence max, if required)
0	07/09/2026	Original publication, Titled: **HSE National CCTV Policy**

PUBLICATION INFORMATION [4]
Topic:
Close Circuit Television (CCTV)
National Group:
National Data Protection Office
Short summary:
The HSE National CCTV Policy sets out how CCTV will be used across HSE premises to support safety and security in a manner that is lawful, necessary and proportionate.
Description:
The purpose of this policy is to provide direction on the use of CCTV across HSE facilities in support of the safety and security of staff, patients, service users, visitors and public while respecting individuals' rights to privacy and data protection. The policy sets out principles and requirements for the lawful, necessary and proportionate use of CCTV, in line with GDPR, the Data Protection Act 2018 and guidance from the Data Protection Commission. The policy applies to all HSE-operated CCTV systems, including those managed by third-party service providers on behalf of the HSE, and covers the recording, storage, access, retention and disclosure of CCTV footage. This document does not replace local operational procedures, but provides a national framework to support consistent, transparent and accountable use of CCTV across the HSE.
Methodology:
The development of the policy was led by the National Data Protection Office, including representatives from Regional Data Protection teams, NCD Integrated Care, Mental Health Commission and Trade Unions.

[3] Records details of the document review or update, even if no changes are made.
[4] Records the document information required for publication on the HSE National Central Repository.

Contact details for the Data Protection Office are available here: About data protection

Table of Contents

01 **Introduction**
02 **Purpose**
03 **Scope**
04 **Glossary of terms**
05 **Legal basis**
06 **Responsibilities**
07 **Purpose of CCTV use**
08 **Processing activities**
- 8.1 Data collection
- 8.2 Special category data

09 **CCTV equipment**
- 9.1 Location of cameras
- 9.2 Location of monitors
  - CCTV awareness for vulnerable individuals
  - Covert CCTV
- 9.3 Maintenance

10 **Unauthorised recording**
11 **Data retention**
12 **Access to CCTV Data**
- 12.1 Authorised access
  - Playback
- 12.2 Subject access requests
- 12.3 Disclosure to third parties
  - An Garda Síochána (AGS)
- 12.4 Freedom of information act

13 **Signage and notification**
14 **Review policy**
15 **Complaints**

Appendices
- Appendix 1
- Appendix 2
- Appendix 3
- Appendix 4

01 Introduction

The Health Services Executive (HSE) is committed to ensuring the security and safety of its staff, service users, patients, volunteers, visitors, members of the public and HSE facilities. This policy outlines the principles and procedures for the use of Closed-Circuit Television (CCTV) systems within HSE facilities, in compliance with all applicable data protection laws, including the Regulation (EU) 2016/679 (General Data Protection Regulation) and the Data Protection Act 2018, and aligning to the CCTV guidance from the Data Protection Commission (DPC), Ireland.

CCTV systems are integral to maintaining security across the HSE, to protect staff, service users, patients, members of the public and to deter criminal activity, and ensure a safe environment. It is important to implement these systems responsibly and in compliance with data protection obligations.

This policy provides a comprehensive framework for all HSE management and staff regarding the management of CCTV within the HSE, supporting adherence to data protection legislation and industry best practices. Additionally, it outlines procedures for monitoring, recording, and storing footage to safeguard privacy and enhance security.

Related resources: General Data Protection Regulation, Data Protection Act 2018, Freedom of Information Act (2014), CCTV Guidance for Data Controllers - Data Protection Commission 2023[1], HSE Data Protection Policy 2019, HSE DPIA Process Guidance, HSE Privacy Notice – Patients & Service Users[2].

[1] *Reference 1*
[2] *Reference 2*

02 Purpose of the policy

HSE uses CCTV in appropriate locations in its facilities for the purpose of maintaining the safety and security of its staff, service users, patients, visitors and members of the public along with maintaining the security of its premises. The policy aims to offer clarity on how CCTV should be used within current regulatory guidance and legislative frameworks.

03 Scope

This policy applies to:

- HSE Facilities: This policy applies to all HSE facilities (exterior and interior of: hospitals, buildings, approved centres, ambulances, storage units etc.) where CCTV is operating.
- CCTV Operators: It covers all CCTV systems operated by the HSE, and to those managed by third-party providers who are bound by the same terms of this policy.
- Service users and patients, visitors and members of the public
- Staff: all employees of provider organisations including full time and part time staff, fixed-term staff, casual staff, and those engaged in any capacity to provide services or advisory to, or on behalf of the provider or its funded agencies on a consulting basis.
- Service Providers: any person, organisation, or part of an organisation delivering healthcare services, as defined in the Health Acts 2004 to 2007 and similarly by the Mental Health Act 2001. This would not normally include an individual employed by an organisation that would have corporate responsibility for meeting the Code of Conduct[3].
- Third Party Contractors: external parties who may be on the premises for maintenance, deliveries, or other services.

Please note: This policy only applies to the use of CCTV. CCTV footage must only be observed live by trained and vetted staff; live monitoring is strictly limited to authorised personnel. Other uses of video and other surveillance technology are not covered in this document. For example, video recordings or the use of live digital monitoring technologies that are made as part of a patient's treatment or clinical care are out of scope.

This policy does not apply to the use of dummy cameras. Dummy cameras should not be used as a form of deterrence in contexts where real CCTV would be disproportionate.

Mental Health units should continue to follow the existing HSE guidance Best Practice Guidance for Mental Health Services and regulation 25 of the Mental Health Act 2001 (Approved Centres) Regulations 2006, until the Mental Health Commission Code of Practice[4] is published.

[3] Supporting a Culture of Safety, Quality and Kindness: A Code of Conduct for Health and Social Service Providers, Department of Health, May 2018, page 18.
[4] Code of Practice is about the use of surveillance technologies in case some readers are unaware about this development

04 Glossary of terms

Authorised Personnel
HSE employee including security contractors who is authorised by the Hospital to process CCTV personal data

CCTV
Closed Circuit Television, the use of video cameras to transmit a signal to a specific, limited set of monitors. It differs from broadcast television in that the signal is not openly transmitted.

CCTV equipment
Cameras, monitors for displaying images, recording facilities, footage, etc.

Data Controller
A person or organisation that decides why and how personal data is collected and used.

Data Subject
Person to whom the personal data relates

Freedom of Information
A legal right that allows anyone to access records held by public bodies,

Obfuscate / Pixelate
Remove/blur images to ensure third parties are not recognisable from the footage

Subject Access Request
A request someone makes to an organisation to find out what personal data it holds about them.

05 Legal Basis

The HSE relies on Articles 6.1 (e)[5] and 6.1 (f)[6] of the GDPR as the legal basis for the use of CCTV.

The use of CCTV by the HSE is both in the public interest and supports the exercise of official authority because the HSE has an obligation to protect the health and welfare of the public under the Health Act of 2004.

The HSE also has a legitimate interest to protect their property and goods and maintain the safety of persons using their buildings and environs.

This policy prohibits the use of CCTV for any purposes other than those specified above.

[5]*Art. 6.1 (e) - Processing shall be lawful only if and to the extent that at least one of the following applies: processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.*

[6]*Art. 6.1 (f) - Processing shall be lawful only if and to the extent that at least one of the following applies: processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*

06 Responsibilities

Data Controller
The HSE is the data controller for all CCTV footage captured on its premises.

Chief Executive Officer
The CEO is ultimately accountable for ensuring that this policy and relevant data protection obligations are complied with.

Regional Executive Officers
Accountable for ensuring that this policy and relevant data protection obligations are complied with in their Regional Health Area.

Third party service providers
(security companies managing the CCTV/ CCTV software providers)
Third parties acting as data processors must be governed by a contract in accordance with Article 28 of the GDPR.

Data Protection Officer
Reviewing this policy and offering advice on data protection compliance, monitor / audit the Data Subject Rights (e.g., Subject Access Requests, objections).

Regional Data Protection Teams
Responsible for oversight of the compliance with the CCTV Policy.

Line Managers
Responsible for the implementation of this policy and must ensure that staff are informed about this policy.

Decision Makers
Decision makers in the service where the CCTV is operating should be aware of and refer to this policy when managing Subject Access Requests or Freedom of Information requests.

All Staff
All staff are required to make themselves familiar with, and adhere to, this policy and report any misuse or malfunction of CCTV systems to their line manager.

Manager of HSE facility
It is recommended that every facility implement local procedures and oversight to cover CCTV set up and arrangements specific for that particular facility (see Appendix 1). These procedures should clearly outline who is responsible for operating the system and who is responsible for processing the data on foot of a DP/FOI/legal request.

07 Purpose of CCTV use

The use of CCTV is appropriate and limited to what is required for the purposes set out.
The use of CCTV is intended to:

- Provide a safe environment for all staff, service users, patients, visitors and members of the public in HSE Facilities.
- Deter and prevent crime and anti-social behaviour.
- Protect premises and assets.
- Assist in the investigation of incidents and in defence of claims.
- Assist in the investigations of serious allegations under the Trust and Care Policy, Dignity at Work Policy or stage 4 of the Disciplinary Procedure (see Appendix 2) (requires written approval of Assistant National Director (AND) or grade above)
- Investigate incidents under health and safety regulations.
- Assist in investigations in exceptional circumstances under other HSE policies. In such cases the decision must be approved in writing by Assistant National Director (AND) or grade above.

Please Note:
CCTV is not used for the purpose of the routine monitoring or supervision of staff.

Employees have the right to request access to their personal data captured by CCTV.

08 Processing activities

8.1 Data Collection

CCTV systems will capture images. Audio recording should not be used as part of CCTV data collection and is outside of the scope of this policy. The data collected will be strictly limited to what is necessary for the purposes outlined in this policy.

8.2 Special Category Data

CCTV footage may record sensitive data, such as identifiable images of individuals, racial or ethnic characteristics, physical or mental health conditions, indirectly reveal religious beliefs or sexual orientation. The HSE will ensure that this data is processed in line with the HSE Data Protection Policy.

09 CCTV equipment

9.1 Location of cameras

Cameras should be clearly visible and positioned to capture images that align with the system's purpose, such as building entrances, exteriors, parking, waiting rooms, corridors and interior/exterior of NAS vehicles/HSE Fleet. Appropriate signage is addressed in section 13. Signage and Notification.

Before installing CCTV in a new location, a necessity and proportionality assessment must be carried out as part of a data protection impact assessment (DPIA) to ensure that the surveillance is essential for the intended purpose and does not unduly infringe on individuals' rights and freedoms. Each HSE region is required to carry out its own DPIA on CCTV use, since the purpose, necessity, scope and proportionality of CCTV may differ across regions and locations. CCTV DPIAs must be regularly reviewed to assess the necessity and proportionality of CCTV use.

9.2 Location of monitors

To maintain security, CCTV monitors and access to images should be restricted to authorised staff only and should not be located in areas where they can be viewed easily by the public or unauthorised staff.

CCTV Awareness for Vulnerable Individuals

It is recognised that some individuals, such as children, those who are visually impaired, not conscious, people with dementia, or those experiencing mental health difficulties, may not fully comprehend that CCTV is operating, even when signage is present. In these cases, staff should be especially mindful and ensure that its presence is explained clearly and sensitively where appropriate to legal guardians or nominated contact persons.

Covert CCTV

Covert use of CCTV (recorded or live) is strictly prohibited, unless part of a criminal investigation and approved by HSE where its use is deemed necessary and proportionate:

- Authorised in advance by the Chief Executive Officer (CEO) and assessed the Data Protection Officer (DPO)
- In conjunction with An Garda Síochána
- Proportionate to the risk involved (including a Data Protection Impact Assessment (DPIA))
- And supported by legal advice where appropriate

9.3 Maintenance

It is important that all CCTV systems are routinely checked on a scheduled basis to ensure that they are working properly and maintenance documented. This is to ensure that all cameras are working and have a view of the target area which has not become obscured i.e. by trees or shrubs and that the images are fit for purpose and that the system is accurately calibrated to date, time and place.

10 Unauthorised monitoring

The installation and use of privately operated CCTV, audio or other surveillance equipment by staff, members of the public, including family members or close contacts of service users (e.g., residents in nursing homes), is not permitted on HSE premises. This includes any form of monitoring device placed in rooms, communal areas, or other parts of HSE facilities.

The HSE reserves the right to remove any unauthorised monitoring devices from its premises.

11 Data retention

We recommend that there is a clear data retention period documented in the local SOPs. After this period, it is a normal practice that footage will be automatically overwritten. The recommended standard retention period for CCTV footage is 30 days.

Where necessary for an ongoing investigation or legal proceedings, the CCTV footage will be extracted and retention period will be extended.

12 Access to CCTV data

12.1 Authorised Access

Only authorised personnel will have access to CCTV footage.

Playback

Playing back (viewing) images on a CCTV system is considered to be processing data and any viewing of CCTV should be in line with the purposes listed above.

Request for footage that is required for internal investigation is formally submitted in writing and approved by a staff member at GM grade or higher clearly outlining the requirement for data.

12.2 Data subject rights

The rights available to data subjects under the GDPR are discussed in the HSE Data Protection Policy. Individuals can exercise their rights in respect to their personal data captured by CCTV.

For further details please follow this link Data Requests – HSE.ie

12.3 Disclosure to third parties

An Garda Síochána (AGS)

Requests for CCTV footage could be submitted by third parties including for example An Garda Síochána (AGS) or a solicitor acting for a claimant or defendant to litigation. Requests from An Garda Síochána (AGS) should be submitted in accordance with Section 41(b) Guidance:

- Any such disclosures must be fully documented,
- Disclosures are limited to what is necessary and proportionate in the circumstances
- Data Protection Officer is consulted in the assessment or processing of such requests.

If the HSE is on notice of an impending request for footage, we shall promptly take reasonable steps to preserve the relevant footage.

12.4 Freedom of information act

Requests for CCTV footage can be made under the Freedom of Information Act 2014:
Making a Request – HSE.ie

12.5 Unauthorised access

Unauthorised access to or disclosure of CCTV footage should be managed in accordance with the data breach process. Refer to data breach process guidance.

13 Signage and notification

Notification of CCTV usage can usually be achieved by placing easily read and well-lit signs in prominent positions, including in restricted areas. A sign at all entrances will normally suffice indicating the purpose of the CCTV system and the identity and contact details of the data controller. These signs should contain the following information:

A. The name of the organisation.
B. The purpose of the CCTV.
C. Contact details for inquiries regarding the CCTV system.



Standard signage:

CCTV Recording in Use [picture of a camera]

This area is monitored by CCTV for safety and security purposes.

Data Controller: Health Service Executive (HSE)

Contact: For more information, please contact [insert email address] (local HSE representative responsible for CCTV)

This sign should be printed and laminated.

14 Policy review

This policy will be reviewed every three years or sooner if significant legislative[7] or operational changes arise. Compliance will be assessed through regular audits and feedback from staff.

15 Complaints

Complaints regarding the operation of the CCTV system or concerns about privacy can be directed to the Data Protection Officer, or through the HSE complaints and feedback.

You also have the right to make a complaint to the Data Protection Commission (DPC) through their website www.dataprotection.ie/en

[7]It is expected that the next review will take place following publication of the Surveillance Code of Conduct issued by the Mental Health Commission.

Appendices

Appendix 1

CCTV Operation Summary and Compliance Checklist

The attached CCTV Operation Summary template must be completed by each service or location that have installed CCTV cameras. It must be reviewed annually.

The CCTV Compliance Checklist is designed to support the managers responsible for CCTV to ensure that all of the appropriate measures are in place to maintain compliance with this policy and applicable regulations.

CCTV Operations Summary

Location	*<Enter service/site/hospital/CHO/division etc.>*			
Date Completed	*<Date>*	**Completed by**	*<Name and title>*	
Date Last Reviewed	*<Date>*	**Reviewed by**	*<Name and title>*	
CCTV System Details	**Name of system**	*<Enter name>*	**Number and location of cameras**	
	System Operator	*<Company Name>* *<Contact details>*	*<How many cameras are in operation>* *<List each location or for a large facility or campus attach list from CCTV Operator>*	
	Operator Contract and Data Processing Agreement	*<Yes/No>* *<Date of Contract>*		
	Is there a maintenance contract?	*<Yes/No>*		
	Is system regularly tested?	*<Yes/No>*		
	CCTV signage	*<Yes/No>* **Note: Signs displayed at all public entrances and monitored areas**		
CCTV Operation	**HSE manager responsible for CCTV**	*<Name and job title of manager responsible>*		
	How are CCTV monitors kept private?	*<Briefly describe e.g. monitors not facing a public area, privacy screen, locked office, Keypad/swipe, codes/passwords, etc>*		
	Is the CCTV resolution sufficient to identify individuals?	*<Yes/No>*		
	Have CCTV operators completed the Fundamentals of GDPR training on HSELanD (or equivalent)?	*<Yes/No>*		
	Is there off-site monitoring of CCTV?	*<Yes/No>*		
	Is the CCTV footage overwritten every 30 days?	*<Yes/No>*		
	<If footage is not automatically overwritten please explain. This must be reviewed with the data protection team.>			

CCTV Compliance Checklist

Location	*<Enter service/site/hospital/CHO/division etc.>*		
Date Reviewed	*<Date>*	**Reviewed by**	*<Name and title>*

CCTV Awareness	**Is the standard HSE CCTV signage displayed at all public entrance and other monitored areas**	*<Yes/No>*
	Have all staff been made aware of the CCTV policy?	*<Yes/No>*
	Has there been appropriate communication/training on proper use of CCTV and restrictions on viewing and downloading?	*<Yes/No>*
	Have CCTV operators completed the Fundamentals of GDPR training?	*<Yes/No>*
Access to CCTV	**Is there a process for responding to a Freedom of Information, Data Subject Access or Legal requests for CCTV?**	*<Yes/No>*
	Are all requests authorised, logged and tracked?	*<Yes/No>*
	Is formal documentation retained for all Garda requests?	*<Yes/No>*
	Is there a list of who can authorise the use of CCTV footage?	*<Yes/No>*
	Is there a standard process for downloading CCTV footage?	*<Yes/No>*
	Are measures in place to safely store footage and delete once no longer required?	*<Yes/No>*
Risk Management	**Has the CCTV DPIA been reviewed?**	*<Yes/No>*
	Have the number and position of cameras been assessed for necessity and proportionality?	*<Yes/No>*
	Is the use of CCTV documented in the Record of Processing Activities (RoPA)?	*<Yes/No>*
	Is inappropriate use of CCTV included in data breach management process?	*<Yes/No>*
	Have local risks relating to CCTV been documented?	*<Yes/No>*

Appendix 2

Examples of serious allegations which may be dealt with from the outset under Stage 4 of the Disciplinary Procedure include, but are not limited to, the following:

a. Theft.
b. Serious breach of the HSE Policy on Fraud and Corruption.
c. Deliberate damage to property.
d. Fraud or deliberate falsification of documents, violation or misuse of confidential information or organisational property, material or equipment.
e. Unauthorised entry/access to computer and/or other records/files.
f. Serious breach of health and safety rules.
g. Serious bullying, sexual harassment or harassment.
h. Serious abuse of a patient/client.
i. Violent or anti-social behaviour.
j. Sexual assault.
k. Serious breach of the HSE National Policy and Procedure for the Management of Intoxicant Misuse 2025. Employees are prohibited from reporting to or attending at work while being under the influence of any **"intoxicant"** (meaning alcohol, prescribed drugs, or legal medication which have been used other than to comply with a prescription properly issued to the employee by a registered medical practitioner) or consuming any such intoxicant during working hours.

The foregoing list is not exhaustive.

Appendix 3

Consultations

The policy was developed with input from relevant stakeholders, including National and Regional Data Protection teams, Mental Health Commission, Trade Unions, HSE HR and Communications. Operational and governance perspectives were considered to ensure practical applicability across diverse HSE settings.

Appendix 4

Standard CCTV Sign

The sign on the next page should be printed and laminated. Signs should be displayed at all entrances and areas where CCTV is in operation.

The appropriate email address for the local contact for CCTV should be added before printing. It is recommended that an email address be set up for this purpose which can be automatically forwarded to the responsible person.



CCTV images are recorded for safety and security purposes

Data Controller: Health Service Executive (HSE)

For more information, please contact [*insert email address*]