



An Garda Síochána

Code of Practice

DRAFT

Public Closed Circuit Television (CCTV)
Garda Síochána (Recording Devices) Act 2023

Effective Date	**/**/2026
Version No.	
Approved by	The Minister for Justice, Home Affairs and Migration
Issued by	The Garda Executive
Introduced by	HQ Directive ***/2026
Policy Owner	Garda National Community Engagement Bureau

Table of Contents

Table of Contents.....	2
1 Overview	3
1.1 Introduction	3
1.2 Aims & Objectives	3
1.3 Legal Context (Scope and Application)	3
1.4 Relevant Terms & Definitions	4
1.5 Guiding Principles	6
1.6 AGS Decision Making Model	7
1.7 Roles & Responsibilities	7
1.8 CCTV Infrastructure.....	7
2. Data Confidentiality, Security, Storage, Access, Retention & Deletion	10
2.1 Data Capture and Quality	10
2.2 Data Confidentiality, Security, Access & Viewing	10
2.3 Access to and Disclosure of Public CCTV Images to Third Parties	11
2.4 Data Use and Governance	11
2.5 Data Retention & Disposal	12
2.6 User Training.....	13
3 Data Subject Rights	13
3.1 Data Protection Compliance	13
3.2 Access by Data Subjects	13
3.3 Data Protection Impact Assessment.....	13
4 Ethical Standards & Commitments	14
4.1 Approving Authority	14
4.2 Monitoring and Review.....	14
4.3 Consultation	14
4.4 Publication	14

1 Overview

1.1 Introduction

This Code of Practice (COP) is in accordance with Part 5 of the Garda Síochána (Recording Devices) Act 2023 (also referred to as “the Act”). The Act introduces the conditions governing the operation of Public Closed Circuit Television (CCTV) in a public place. This includes the need for all Public CCTV operating in public areas to have written authorisation from the Garda Commissioner.

This COP sets out the standards for operation of Public CCTV in public places by Garda personnel. Public CCTV authorised under Part 5 of the Act must be compliant with data protection legislation and the relevant technical specifications.

The fundamental principle underpinning this policy is that any action taken must comply with the fundamental principles of legality, necessity, proportionality, accountability and relevant Garda Síochána policy and Code of Ethics, and is applied in a non-discriminatory manner in accordance with the principles of the Constitution of Ireland 1937, the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union.

1.2 Aims & Objectives

Due to the construct of Part 5 of the Act, this COP establishes Garda policy for the use and operation of the following, by Garda personnel:

- CCTV cameras and monitoring software;
- the handling of digital recordings / evidence; and
- the processing of live feeds from local authority CCTV by An Garda Síochána

1.3 Legal Context (Scope and Application)

This COP pertains to An Garda Síochána in the operation of Public CCTV and the COP applies to all Garda personnel. The legal basis for operating Public CCTV is provided for in Part 5 of the Act. This COP is prepared under section 47 of the Act and provides further detail on the operation of Public CCTV and associated procedures. The COP includes provisions relating to the processing of data, gathered as a result of the operation of Public CCTV, in accordance with Data Protection legislation. Recordings and images on Public CCTV may be admissible in evidence in criminal, civil and/or disciplinary proceedings in accordance with section 48 of the Act.

This COP applies to Public CCTV only and does not include non-local authority CCTV live feeds or CCTV operated on Garda premises.

This COP applies to all Garda personnel in the use of Public CCTV and handling of Public CCTV recordings. Further information is contained within the procedure document. Local Authorities shall also comply with this COP as part of the CCTV infrastructure.

This Code should be read in conjunction with the relevant legislation and associated policies and procedures.

1.4 Relevant Terms & Definitions

Technical terms and abbreviations which are used throughout this document are defined in this section to ensure a common understanding by way of further detail in relation to the operation of Part 5 of the Act and this COP.

Term	Definition
CCTV	In relation to the Operation of Part 5 of the Act and this COP means a closed-circuit television system of one or more devices and includes any system for processing the images, any accompanying sounds, or other information obtained by those recording devices.
Code of Practice (COP)	As defined in section 2 of the Act, means a Code of Practice approved by the Minister by order under Part 8 and includes part of a Code of Practice.
Data Controller	In relation to the operation of Part 5 of the Act and this COP, the Data Controller is any person who decides the purposes for which and how personal data is processed. An Garda Síochána is the data controller for personal data processed within the scope and application of this Code of Practice. Each CCTV scheme authorised under this Code will have an assigned business owner responsible for ensuring An Garda Síochána's compliance with its responsibilities as a data controller.
Digital Evidence Management System (DEMS)	This is a software-based solution that enables an organisation to secure, store, process, retrieve and manage all their digital evidence throughout its lifecycle; and provide appropriate audit and controls to ensure data is handled in line with approved policies.
Document	As defined in section 2 of the Act, means any of the following: <ul style="list-style-type: none"> a) a book, record or other written or printed material, b) a photograph, c) any information stored, maintained, or preserved by means of any mechanical or electronic device, whether or not stored, maintained or preserved in legible form, and d) any audio or video recording.
Evidence	This refers to something that proves or disproves a particular fact; it includes items that are relevant to the defence and / or prosecution case.
Garda Personnel	This means: <ul style="list-style-type: none"> (a) members of An Garda Síochána, or (b) members of Garda Staff.
Policing Purpose	Any activity undertaken with the intent to: prevent, investigate, detect, or prosecute criminal offences; secure public order and public safety; or safeguard against, or prevent threats to public security, in accordance with the functions of An Garda Síochána set out in Section 9(1) of the Policing, Security and Community Safety Act 2024.



Term	Definition
Local Authority	This has the same meaning as it has in section 2(1) of the Local Government Act 2001, and refers to: <ul style="list-style-type: none"> a) a county council, b) a city council, or c) a town council.
Media storage device	This refers to any device on which a document(s) is or can be stored or transported. Note: this is distinct from 'Removable media' in the sense that a 'media storage device' as defined in this term maybe removable or irremovable.
Member of An Garda Síochána	This means a "member" within the meaning of section 2(1) of the Policing, Security and Community Safety Act 2024.
Member of Garda Staff	This means a "member of garda staff" within the meaning of section 2(1) of the Policing, Security and Community Safety Act 2024.
Member of Garda Personnel	This means a "member of garda personnel" within the meaning of section 44 of the Policing, Security and Community Safety Act 2024, other than in Part 6.
Minister	This refers to the Minister for Justice, Home Affairs and Migration.
Operation	In relation to CCTV this includes the maintenance and monitoring of the CCTV.
Personal data	Personal data is defined in accordance with section 2 of the Act as follows <ul style="list-style-type: none"> (a) an identified living individual, or (b) a living individual who can be identified from the data, directly or indirectly, in particular by reference to: <ul style="list-style-type: none"> i. an identifier such as a name, an identification number, location data or an online identifier, or ii. one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of the individual.
Public place	This means a place to which the public have or are permitted access, whether as of right or by express or implied permission and whether subject to or free of charge.
Recording device	Recording device means any of the following <ul style="list-style-type: none"> (a) a device or system that is capable of creating a record in any medium from which visual images (including moving visual images) or sounds, or both, may, by any means, be reproduced, (b) includes any devices or systems that are capable of processing the record made under paragraph (a), which may include— <ul style="list-style-type: none"> i. reproducing by any means the visual images (including moving visual images) or sounds concerned, ii. using ANPR in respect of the record, or iii. producing a document relating to the record or the processing concerned.

Term	Definition
	includes any device or system referred to in paragraph (a) or (b) that is in or affixed to a vehicle or a structure.
Relevant data	This means any data relevant which, when used lawfully, where necessity requires and is proportionate, assists in public safety; preventing, detecting, investigating or prosecuting criminal offences; preventing threats to national security, or public security; or for the purposes of providing or obtaining legal advice or for the purposes of, or in connection with, legal claims, prospective legal claims, legal proceedings or prospective legal proceedings or establishing, exercising or defending legal rights.
Removable media	This typically refers to data storage devices (such as CD-ROM, DVD, Memory pen-drive, or portable hard drive) capable of being removed from a computer system without powering off the system for the express purpose of copying and transporting document(s) (for example recordings or photos).
Structure	This means any building, erection, or other construction, erected, or made on, or in or under any land, or any part of a structure so defined.
Vehicle	Vehicle refers to any means in or by which any person or thing, or both, is transported or conveyed, that is designed for use or may be used on land, in water or in the air, or in more than one of those ways, and includes an unmanned aerial vehicle.

1.5 Guiding Principles

CCTV cameras and monitoring software must be operated fairly, responsibly, with respect for the rights of others, proportionately, necessarily and without unlawful discrimination for a policing purpose in accordance with the Act and this COP. Key primary principles, outlined below, have been developed to guide the overt use of digital recording devices:

- Authorisations issued under section 38 of the Garda Síochána Act 2005 will remain valid for up to four years unless revoked earlier by the Garda Commissioner;
- As described in the Act, recordings and images captured via Public CCTV will be the sole or primary purpose for a member of Garda personnel acting in the course of his or her duties in the prevention, investigation, detection or prosecution of criminal offences, safeguarding against, and the prevention of, threats to public security, including securing public safety and public order, or the protection of the security of the State;
- Public CCTV should be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value;
- When using Public CCTV cameras, consideration may be given to balancing the potential impact on individuals and their privacy against the common law duty on Garda personnel to seek out and preserve all evidence that has a bearing or a potential bearing on the issue of guilt or innocence. The right to privacy is not an unqualified right and its exercise may be restricted by the

constitutional rights of others, including a right to a fair trial, by the requirement of the common good and is subject to the requirements of public order;

- The use of Public CCTV must be as transparent as possible with clear guidance available to individuals and/or the public that recording is taking place (for example, use of signage to alert the public to the Public CCTV location);
- All recordings and imagery that is viewed, stored, processed, and shared from any digital recording device is subject to applicable data protection legislation; and
- As appropriate to their role, all Garda Personnel shall be trained in the use of Public CCTV, and acknowledge and comply with relevant Garda policy.

1.6 AGS Decision Making Model

The Garda Decision Making Model (GDMM) applies to all decisions made by Garda personnel from spontaneous incidents to planned operations, daily duties to strategic planning.

Where there may be situations which are not explicitly covered in this Code, Garda personnel should use the GDMM to inform their actions and decisions with respect to the use of digital recording devices.

1.7 Roles & Responsibilities

To ensure as far as possible that all matters relating to Public CCTV and its use are dealt with in a methodical and uniform manner, the development and implementation of Garda policy on Public CCTV usage, including the maintenance of this COP, is overseen by the CCTV Advisory Committee, appointed by the Garda Commissioner.

1.8 CCTV Infrastructure

Public CCTV accessible by An Garda Síochána is categorised under two types, as defined in Part 5 of the Act. The type dictates how Public CCTV is used, operated, and maintained.

The table below provides an overview of each type:

Type	Description
Authorisation to member of Garda personnel - (Garda Operated Public CCTV)	<p>A member of Garda personnel may apply to the Commissioner of the Garda Síochána under Section 27 of the Act for an authorisation for the installation or operation, or both, of Public CCTV in one or more specified locations for the sole or primary purpose of recording a public place for the purposes detailed under Part 5 of the Act.</p> <p>The operational management of Garda Public CCTV is the responsibility of the Chief Superintendent in charge of the Division. Chief Superintendents will ensure that all personnel who are detailed to monitor Public CCTV are familiar with this COP.</p>

Type	Description
	The monitoring of Public CCTV will be under the control of the Gardaí and will be monitored from a Garda premises. CCTV will be recording at all times, whether being monitored or not.
Authorisation to Local Authority - (Local authority operated CCTV)	<p><i>A Local Authority may apply to the Commissioner of the Garda Síochána under Section 28 of the Act for an authorisation for the installation of Public CCTV in one or more specified locations for the sole or primary purpose of recording a public place to assist the Garda Síochána in –</i></p> <ul style="list-style-type: none"> <i>a. the prevention, investigation, detection or prosecution of criminal offences,</i> <i>b. safeguarding against, and the prevention of, threats to public security, including securing public safety and public order, or</i> <i>c. the protection of the security of the State.</i> <p><i>The Public CCTV shall at all times:</i></p> <ul style="list-style-type: none"> <i>i. comply with any technical specifications that may be issued by the Commissioner of the Garda Síochána or Department of Justice from time to time, and</i> <i>ii. be installed and operated in accordance with this code of practice.</i>

1.8.1 Authorisation of Public CCTV

Authorisation for the use of Public CCTV is provided under Part 5 of the Act. When making an application to the Commissioner for the installation of Public CCTV, the member of Garda personnel shall provide information as to how they shall install or operate the Public CCTV, or both, or cause the Public CCTV to be installed or operated or both, in accordance with Garda Síochána procedures.

The Commissioner may authorise the use of Public CCTV systems for the purpose of policing specific events. As the CCTV Advisory Committee convenes on a quarterly basis to consider applications for permanent Public CCTV schemes, applications relating to specific events shall be managed through a separate and expedited process. Under this process, an operational business owner of Assistant Commissioner rank shall be designated to oversee the preparation and completion of the application. The completed application shall then be submitted for the consideration of the Commissioner and potential authorisation in accordance with Garda Síochána procedures.

The Commissioner of An Garda Síochána may review or revoke authorisation as outlined in Section 32 of the Act. The Act also provides for certain amendments or additions to be made to Public CCTV as outlined in Section 31 of the Act.

The Act provides that a person who operates Public CCTV without authorisation, fails to comply with the terms of authorisation, or without lawful authority interferes with the operation of Public CCTV, is guilty of an offence as outlined in Section 35 of the Act.

1.8.2 Public CCTV signage

The purpose of Public CCTV is to act as a deterrent and to prevent crime. A sufficient amount of signage shall be erected to ensure that the public are aware that they are entering an area which is covered by Public CCTV. These signs should be clearly visible and legible to members of the public. Such signs shall be compliant with the Data Protection Act 2018.

1.8.3 Public CCTV Criteria

Prior to making an application for new Public CCTV, or making revision to existing Public CCTV, Responsible Business Owner for the CCTV scheme should consider the following:

Purpose	<ul style="list-style-type: none"> Is there a clearly defined purpose for installing Public CCTV? What observations are intended to be captured? Is the Public CCTV to be used for security purposes only? If not, can the other purposes be justified? Will the use of the personal data collected by the Public CCTV be limited to that original purpose?
Lawfulness	<ul style="list-style-type: none"> What is the legal basis for the use of Public CCTV? Is the legal basis being relied on the most appropriate one?
Necessity	<ul style="list-style-type: none"> Can it be demonstrated that Public CCTV is necessary to achieve the goal? Have other solutions been considered that do not collect an individual's personal data by recording their movements and actions on a continuous basis?
Proportionality	<ul style="list-style-type: none"> Proportionality must balance an individual's and member of the public's right to privacy under the Constitution and Article 8 at the location where Public CCTV is proposed, against the benefits of having Public CCTV in that place for the purposes for which it is installed. Does the purpose for which Public CCTV is being put in place outweigh the privacy rights of those who may be affected?
Safety	<ul style="list-style-type: none"> What measures will be put in place to ensure that Public CCTV recordings are safe and secure, both technically and organisationally? (e.g. physical and electronic access controls to CCTV monitoring and storage areas, discourage the use of other recording devices, etc.). Who will have access to Public CCTV recordings in the organisation How will this be managed and recorded?
Privacy	<ul style="list-style-type: none"> What safeguards can be incorporated into systems to enhance privacy rights, including automatic settings for pan tilt and zoom cameras to return to default positions. What privacy masking can be implemented to mask private residences captured within the field of view of the cameras monitoring a public space.
Retention	<ul style="list-style-type: none"> Public CCTV recording retention will comply with policy and will be retained for a maximum of 31 days unless required for evidence or investigative purposes.
Audit	<ul style="list-style-type: none"> There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice.
Training	<ul style="list-style-type: none"> CCTV operators should be sufficiently trained with consideration given to any approved operational, technical and competency standards relevant to the Public CCTV and its purpose and should meet and maintain those standards.
Transparency	<ul style="list-style-type: none"> How will members of the public be informed that their images are being recorded and provide them with other information required under transparency obligations? Has consideration been given to the means by which they can request further information or request a copy of a recording?

Applications for Public CCTV and associated documentation will be forwarded through the Chief Superintendent in charge of the Division to the Assistant Commissioner Roads Policing and Community Engagement (RPCE). Applications for Public CCTV will be assessed by the CCTV Advisory Committee. The Committee will forward their recommendations to Assistant Commissioner RPCE. Assistant Commissioner RPCE will forward the decision of the Committee to the Garda Commissioner for consideration of formal authorisation.

Applications relating to specific events shall be managed through a separate and expedited process. Under this process, an operational business owner of Assistant Commissioner rank shall be designated to oversee the preparation and completion of the application. The completed application shall then be submitted for the consideration of the Commissioner and potential authorisation in accordance with Garda Síochána procedures.

2. Data Confidentiality, Security, Storage, Access, Retention & Deletion

This section provides an overview of the Public CCTV infrastructure and guidance on the handling and management of Public CCTV recordings and images obtained from Public CCTV to ensure a common understanding by way of further detail in relation to the operation of Part 5 of the Act and this COP.

2.1 Data Capture and Quality

Fundamental maintenance and quality principles must be upheld, for example:

- The equipment, including cameras, being used to capture image material should be maintained and serviced to a level where the quality of the images recorded meets the standard required by the technical specification;
- Cameras should be protected from vandalism to ensure that they remain in working order;
- Media storage devices should be adequately designed and maintained to ensure they perform as required and provide necessary data recovery mechanisms in the event of failure;
- Cameras should be situated so that they will capture images relevant to the purpose for which the Public CCTV has been established. In addition, cameras should be situated to limit the interference with the right to privacy of members of the public and incorporating masking of private residences as a relevant safeguard, consistent with achieving the purpose;
- If a camera is damaged, this must be reported so that repairs may be carried out.
- The Chief Superintendent in charge of the Division will maintain an appropriate record of the Public CCTVs effectiveness, including a maintenance log.

2.2 Data Confidentiality, Security, Access & Viewing

Only individuals authorised by the Responsible Business Owner for the CCTV scheme may be allowed access to monitoring areas and the media storage devices used in the Public CCTV. All recordings must be viewed and managed in accordance with relevant data protection legislation and the Garda Code of Ethics. Operators are to ensure that all uses of the Public CCTV are appropriate, authorised in the public interest and in line with this COP.

If Public CCTV is to be reviewed, it shall be accessed only by Garda personnel authorised by the Chief Superintendent in charge of the Division. Any Garda personnel making use of the review facility must complete an entry in official documentation, which will also include the Chief Superintendent's authorisation.

For installation and/or maintenance purposes, access to the recorded Public CCTV images will be restricted by the Responsible Business Owner to a designated person or persons who have been Garda vetted (Garda National Vetting Bureau). Organisations engaged to assist in the installation and/or maintenance of the CCTV scheme as a data processor, appropriate contractual controls will be put in place to ensure confidentiality of the system and compliance with data protection law. Other persons should not be allowed to have access to that area.

2.2.1 Vetting

For the purpose of ensuring that any employees of the Local Authority concerned who are involved in the installation, operation or both, of the Public CCTV shall be, and shall remain, of good character; the Commissioner may at any stage request vetting information regarding those persons from the Garda National Vetting Bureau.

2.3 Access to and Disclosure of Public CCTV Images to Third Parties

Access to Public CCTV images will be restricted to those personnel who need to have access to the Public CCTV. All access requests to media storage devices onto which images are recorded will be documented by the Responsible Business Owner or designated Garda personnel acting on the Responsible Business Owner's behalf.

Disclosure of recorded Public CCTV images to third parties by An Garda Síochána should only be made by the Responsible Business Owner in limited circumstances including, but not limited to:

- following a formal request from Garda personnel for disclosure of images on the grounds that the images are likely to be of use for the investigation of a particular offence;
- a requirement under any enactment, rule of law or court order to disclose the images;
- if required by the Responsible Business Owner's legal representatives where legal proceedings are being taken against the operator;
- media organisations, where it is decided that the assistance of the public is needed to assist in the identification of victim, witness, or perpetrator in relation to a criminal incident. As part of that decision, the wishes of the victim of an incident should be taken into account; and
- to people whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal inquiries or criminal proceedings).

2.4 Data Use and Governance

2.4.1 Relevant Data Controller

An Garda Síochána is the data controller for any personal data which is captured on Public CCTV administered by Garda Personnel.

2.4.2 Governance and Compliance

The effective management of Public CCTV requires that:

- The overall management of Public CCTV and the requirement to comply with the COP is the responsibility of the Chief Superintendent in charge of the Division;
 - Access to recordings and the monitoring area must comply with the COP and will be recorded and monitored; and
- The operational documentation required to run Public CCTV must be developed from and specifically linked to this COP.

Compliance with this COP and associated document(s) is mandatory for all Garda personnel. It applies to police officers from the Police Service of Northern Ireland (PSNI) seconded to An Garda Síochána under the provisions of section 53 of the Garda Síochána Act 2005 and in accordance with section 94 of the Policing, Security and Community Safety Act 2024.

2.5 Data Retention & Disposal

Public CCTV images should not be retained by the Data Controller for longer than is necessary. An Garda Síochána policy is that Public CCTV images should be retained for no more than 31 days unless there are specific, legitimate and reasonable grounds for the retention of images beyond that period. Public CCTV must be configured so that recorded images should be automatically erased after a maximum period of 31 days unless required for the investigation of offences or evidential purposes.

The matrix below documents the security aspects, retention policies, and handling caveats relevant for each recording type covered under Part 5 of the Act.

Forms of recordings / images	Markings	Handling instructions	Data aggregation	Audit requirements	Retention period (where not required to be retained for investigative purposes)
Garda Operated Public CCTV	Official - Confidential	Accessed only by personnel authorised by the relevant business owner for the CCTV system.			Maximum 31 days (Standard) Subject to regular reviews in line with policy and procedures.
Local Authority Operated Public CCTV	Official - Confidential	Live feed access is managed via a joint controller agreement with the relevant local authority, and that where a copy of video is required by An Garda Síochána in relation to a specific investigation this is requested in line with organisational policy for requests for data from third party data controllers.	Cross reference with other data sources, Meta-data could be used to analyse and capture potentially relevant evidential information.	Automated process required under Data Protection legislation for logging access to files – relevant for any data stored in an automated processing system Review of ongoing retention at regular intervals.	Maximum 31 days (Standard) Subject to regular review in line with internal policies and procedures.

2.6 User Training

Monitoring and control of screen displays will be carried out by suitably trained Garda personnel. A training program will be put in place for such personnel ensuring that they are proficient in the use of Public CCTV and its use is made known to them.

3 Data Subject Rights

3.1 Data Protection Compliance

As per Section 8(1) of the Data Protection Act 2018, the Data Protection Act 1988 (as amended) continues to apply to processing of personal data for State security purposes, and the General Data Protection Regulation (GDPR) (EU) 2016/679 applies to processing of personal data for non-law enforcement purposes. In processing digital recordings relevant to this COP (including arrangements for access, storage and retention of recordings), An Garda Síochána will ensure compliance with the relevant and applicable data protection legislative framework for the processing concerned.

3.2 Access by Data Subjects

An Garda Síochána will ensure that data subjects can exercise their rights as outlined under data protection legislation. An Garda Síochána has a dedicated Data Protection Unit that manages subject access requests under data protection legislation on behalf of the organisation. The Data Protection Unit ensures that subject access requests are managed in line with the requirements and timescales specified under data protection legislation. This includes reviewing relevant material in relation to a request, including digital recordings, to ensure that appropriate redactions or restrictions are applied, as required, to protect the data protection rights of third parties, or, where a necessary and proportionate measure under data protection legislation, including for the purposes outlined under Section 94 of the Data Protection Act 2018.

3.3 Data Protection Impact Assessment

In line with the requirements of data protection legislation, An Garda Síochána will ensure that a Data Protection Impact Assessment (DPIA) is conducted in relation to each Public CCTV scheme within the scope of this COP as part of the authorisation process for each scheme. DPIAs for Public CCTV schemes will include a general description of the proposed processing operations; an assessment of the potential risks to the rights and freedoms of data subjects as a result of the proposed processing; and a description of safeguards, security measures and mechanisms to be implemented to mitigate said risks. Such measures will include relevant internal policies and procedures, including this COP, and technical and organisational measures applied to technological solutions used by An Garda Síochána to capture, process, store and manage digital recordings.

4 Ethical Standards & Commitments

The Code of Ethics for An Garda Síochána sets out guiding principles to inform and guide the actions of all personnel of An Garda Síochána at every level of the organisation. The Code of Ethics states that Garda Personnel must treat information that is provided to An Garda Síochána with respect and in accordance with the law. This protects the rights of people who provide information and the rights of people to whom the information refers.

4.1 Approving Authority

Minister for Justice, Department of Justice, Home Affairs and Migration.

4.2 Monitoring and Review

This COP will be reviewed and amended where appropriate and in compliance with the provisions of Part 8 of the Garda Síochána (Recording Devices) Act 2023.

4.3 Consultation

An Garda Síochána has undergone the consultative process, in accordance with the provisions of Part 8 of the Garda Síochána (Recording Devices) Act 2023, to develop this Code of Practice

4.4 Publication

This document is available to the public.