



Malta Police Force

CCTV & Telephony Systems Policy

Policy Document

Applicable To: General Application
Classification: Unrestricted
Authorisation: Data Protection Officer

Publication Date: 30/09/2026
Current Version Number: 2.0
Review Date: 30/09/2026

Reference Number: POL-CTV

Document and Version Control

This document is maintained by the MPF. Suggestions for improvement and comments relating to the accuracy and currency of the document should be forwarded to Data Protection Officer.

This Policy compliments and particularises the Data Protection Policy (POL-DPP) of the Malta Police Force (MPF). It sets out the framework for the use and management of CCTV Surveillance Cameras by the MPF as well as the processing of personal data over the telephony system held by the MPF in order to ensure that the processing activities involved are carried out in compliance with the relevant data protection laws, including, but not limited to, the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act, Chapter 586 and Subsidiary Legislation 586.08 of the laws of Malta.

The version number is allocated when it has been approved. Any major revisions will be designated by the next whole number (e.g. version 2.0, 3.0, 4.0). Any minor changes will increase incrementally by hundredths (e.g. 2.1, 2.2, 2.3). The current version number will appear on the front cover, footer and Table 1 of these SOPs.

The policies outlined in this document are generally applicable to all members of the Malta Police Force, but do not override any specific/required departmental policies and procedures, which other departments of the Malta Police Force may have. Therefore, specific departmental policies and procedures shall be always observed over the more generic documentation.

Table 1 – Version Control

Version Number	Approval Date	Changelog
Version 2.0	30/09/2026	• Incorporation Of The Rules On Telephony Systems And Consequential Amendments
Version 1.0	27/01/2024	• First Release

Acronyms, Terminology & Definitions

- i. **CCTV** – Closed-Circuit Television
- ii. **DPO** – Data Protection Officer
- iii. **GDPR** – General Data Protection Regulation
- iv. **MPF** – Malta Police Force

Table of Contents

Document and Version Control	1
Table 1 – Version Control.....	1
Acronyms, Terminology & Definitions	2
Table of Contents.....	3
1. Policy Overview.....	4
1.1. Objectives of the Policy	4
1.2. Scope	4
2. Purpose	5
3. Lawfulness & Necessity.....	6
3.1. Applicable Legal Framework.....	6
3.2. Processing For Law Enforcement Purposes.....	6
3.3. Processing For Administrative Or Organisational Purposes.....	7
4. CCTV	8
4.1. Locations.....	8
4.2. Signage.....	8
5. Telephony Systems	9
6. Storage & Retention Period	9
7. Access to CCTV Footage, Call Recordings, and Related Data.....	10
8. Rights Of The Data Subjects	11
8.1. Contact Details	12

1. Policy Overview

This Policy complements and particularises the Data Protection Policy (POL-DPP) of the Malta Police Force (MPF). It establishes the framework for the use and management of CCTV Surveillance Cameras by the MPF and aims to ensure that all related processing activities are carried out in compliance with the applicable data protection laws. These laws include the General Data Protection Regulation (EU) 2016/679 (GDPR), the Data Protection Act, Chapter 586 of the Laws of Malta, and Subsidiary Legislation 586.08, which transposes Directive (EU) 2016/680.

1.1. Objectives of the Policy

This Policy aims to:

- a) Define the purpose and scope of the processing of personal data through CCTV Surveillance Cameras and Telephony Systems operated by the MPF; and
- b) Establish the standards governing the access, disclosure, and use of video footage and recordings obtained through these systems.

The MPF is committed to ensuring that the collection, use, retention, disclosure, and any other processing of personal data carried out through CCTV Surveillance Cameras and Telephony Systems is lawful, fair, and transparent.

1.2. Scope

This Policy applies to CCTV systems operated by the MPF in police stations and other premises under its control. It also applies to cameras covering the immediate vicinity or perimeter of those premises, including entrances, exits, access points and adjoining areas, where the monitoring is reasonably connected to the security of the premises, the protection of persons present, detained or held there, or the protection of activities and operations carried out there. This Policy also applies to telephony systems operated and managed by the MPF.

This Policy does not apply to monitoring systems or recordings used in interrogation rooms or other locations used for questioning. Nor does it apply to CCTV, other surveillance systems or telephony

systems used directly in a specific case for the investigation, detection or prosecution of a criminal offence.

2. Purpose

The MPF uses CCTV systems installed around its facilities and buildings for the following purposes:

- To protect MPF premises, facilities, and equipment from abuse, unauthorised access, and intrusion.
- To ensure the safety of staff, members of the public, and visitors by providing a secure and protected environment.
- To capture and preserve information necessary for the prevention, investigation, and detection of offences.
- To support internal investigations or other inquiries into incidents, including those involving injuries or damage to property.
- To facilitate internal audits and examinations carried out by the Internal Audit and Investigations Unit.
- To prevent, manage, and respond effectively to complaints or incidents, including matters involving harassment, disorder, or misconduct.
- To support the quality, performance, and security of MPF services through monitoring, training, and audit activities.
- To safeguard the rights and legitimate interests of the MPF, its employees, and any other persons.

Similarly, the recording of telephone calls and the associated metadata serves the following purposes:

- a) To respond effectively to requests for assistance, intervention, or the reporting of crime or other incidents.
- b) To enable timely intervention to protect life, including circumstances involving imminent threats or attempted suicide.
- c) To capture and preserve information necessary for the prevention, investigation, and detection of offences.
- d) To support the quality, performance, and security of MPF services through monitoring, training, and audit activities.
- e) To safeguard the rights and legitimate interests of the MPF, its employees, and any other persons.

3. Lawfulness & Necessity

3.1. Applicable Legal Framework

The processing of personal data by the Malta Police Force (MPF) must always be assessed in light of the applicable legal framework. The MPF carries out both law enforcement functions and administrative or organisational functions. The data protection regime that applies in each case depends on the nature and purpose of the processing activity.

3.2. Processing For Law Enforcement Purposes

When CCTV systems or the recording of telephone calls are used for the prevention, investigation, detection, or prosecution of criminal offences, the processing is regulated by the Data Protection Act (Chapter 586) and Subsidiary Legislation 586.08.

Under this framework, personal data may be processed only where it is necessary for the performance of a task carried out by a competent authority for a law enforcement purpose. This principle is

reflected in Article 8 of the Law Enforcement Directive and in Regulation 5 of Subsidiary Legislation 586.08.

The MPF's statutory duties clearly establish the necessity of such processing. These duties include the following:

- Article 4 of the Police Act (Chapter 164), which sets out the general functions and objectives of the MPF.
- Article 346 of the Criminal Code (Chapter 9), which establishes the duty to prevent, investigate, and detect offences.
- The obligation to protect the vital interests of individuals in urgent or life-threatening situations.
- The need to ensure the safety, accountability, discipline, and integrity of the Police Force, including the provisions of Title IV of the Police Act.

The use of CCTV systems and the recording of telephone calls is therefore necessary and proportionate for the fulfilment of these statutory law enforcement tasks. These measures contribute to risk mitigation, the preservation of evidence, operational accountability, and the protection of officers, staff, and members of the public.

3.3. Processing For Administrative Or Organisational Purposes

Where CCTV systems or call recording are used for administrative or organisational purposes that do not relate directly to a law enforcement function, the processing may fall under the General Data Protection Regulation. Examples include the security of premises, visitor management, call quality monitoring, and other internal administrative functions.

In such cases, processing may be justified under:

- Article 6(1)(c) of the GDPR, compliance with a legal obligation.
- Article 6(1)(e) of the GDPR, performance of a task carried out in the public interest.

- Article 6(1)(f) of the GDPR, where the MPF is not acting in the exercise of its official public powers and where the processing is necessary for a legitimate interest.

In all instances, the MPF must ensure that the processing of personal data is necessary, proportionate, and limited to what is strictly required to achieve the stated purpose.

4. CCTV

4.1. Locations

The MPF installs CCTV systems in a number of premises operated or controlled by the MPF. The positioning and location of cameras are selected with great care to ensure that the processing of personal data contributes directly and in a proportionate manner to the purposes for which the data is collected. Cameras are placed only where necessary and are not installed in locations that would unduly intrude upon the privacy of individuals.

4.2. Signage

Data subjects have the right to be informed about the processing of personal data carried out by means of a CCTV system. In accordance with the requirements of applicable data protection law, the data controller is required to take appropriate measures to ensure that such information is provided in a clear and accessible manner.

For CCTV systems, the primary method of informing data subjects is the use of notices and signs displayed in prominent and easily visible places. These signs must be written in clear and plain language and must draw attention to the presence of CCTV equipment.

The MPF has issued this Policy for the general information of the public and ensures that appropriate signage is installed wherever CCTV equipment is in use. Notices are positioned in such a way that individuals entering a monitored area can easily see and read them before they are recorded.



Figure 1 – MPF CCTV Signage

5. Telephony Systems

The MPF operates a critical telephony system used for communication with the public as well as for internal operational purposes.

Recorded Calls:

- All external calls, whether incoming or outgoing, are recorded. This includes calls received from outside the police telephony systems, as well as calls made from within the police telephony systems to external numbers. It also includes calls made to officers' mobile phone numbers through authorised internal communication procedures.
- Additionally, all calls originating from or directed to the Command & Control Room are recorded. This includes calls made between internal lines within the Command & Control Room.

In most instances, callers are additionally informed through an automated notification at the start of the call that the conversation is being recorded.

6. Storage & Retention Period

CCTV footage, call recordings, and any related data are retained for thirty (30) days in accordance with the *Malta Police Force Data Retention Schedule* (POL-DRS). This retention period was established following an assessment of the MPF's statutory functions as Malta's primary criminal law enforcement

authority, the sensitivity of the data it processes, and the need to safeguard its information systems, operational environments, equipment, and other assets.

At the end of this thirty-day period, all such data is securely and automatically deleted from the relevant systems.

Where CCTV footage, call recordings, or related data are extracted for a lawful and documented purpose, including criminal investigations, internal or disciplinary inquiries, judicial proceedings, or the handling of legal claims, the extracted material shall be retained only for the period established in the Data Retention Schedule or until any related judicial proceedings are concluded or any legal claims have been fully resolved.

Once the relevant purpose has been fulfilled, the extracted material shall be securely deleted in accordance with the MPF's retention procedures and applicable law.

7. Access to CCTV Footage, Call Recordings, and Related Data

Access to CCTV footage, call recordings, and any related data is strictly restricted and carefully controlled. These measures protect the rights of the individuals concerned and ensure that, where such material is required for criminal or internal investigations, the integrity and continuity of the chain of evidence are preserved.

Only designated and authorised officers may access, view or listen to footages or call recordings. Monitoring or playback must take place in secure and controlled environments where unauthorised persons cannot view, overhear, or otherwise access sensitive information. The relevant Officers must ensure that monitoring consoles or playback stations are not visible or audible to others.

Access may be granted to:

- The Professional Standards Office, for internal investigations and disciplinary reviews, or any officer formally assigned to conduct such investigations.
- The Internal Audits Office, for quality assurance and audit purposes.

- Investigating officers or other personnel authorised to perform criminal investigations or other lawful tasks for which access to the recordings or footage is necessary.

All requests must be approved by designated reviewers and approvers.

Access by any other person is only permitted on the basis of a reasoned request for one of the purposes outlined above, where authorised by law, or in compliance with a judicial order or other binding legal requirement.

The MPF ensures that access is granted strictly on a need-to-know basis, is limited to what is necessary and proportionate, and is handled in a manner that maintains confidentiality and evidentiary integrity.

Copies of CCTV footage and call recordings shall be provided through secure electronic links or on approved digital media.

Any officer or member of staff who is granted access to such material, or to whom it is otherwise made available, shall prevent unauthorised persons from accessing, viewing or overhearing it.

Where footage or a recording must be shown or played for a lawful purpose but contains material unrelated to that purpose, the officer or member of staff responsible shall take reasonable steps to limit access to the unrelated material. These may include selecting the relevant extract or restricting who may view or listen to the material, while preserving the integrity of any recording retained as evidence.

8. Rights Of The Data Subjects

Data subjects may submit a written request to the Data Protection Officer (DPO) to exercise their rights in relation to personal data contained in CCTV footage or call recordings. Depending on the applicable law and the circumstances, these rights may include access, rectification, erasure or restriction of processing. Requests will be assessed in accordance with the applicable legal requirements, including any lawful restrictions.

A request should include sufficient details to verify the requester's identity and identify the relevant footage or recording, such as the date, approximate time, location or telephone number concerned. The MPF may request further information where necessary to verify identity or locate the material.

Data subjects may also lodge a complaint with the Information and Data Protection Commissioner. Further information on their rights and how to exercise them is available on the Malta Police Force website available at: <https://pulizija.gov.mt/en/data-protection/>.

8.1. Contact Details

Any request in the exercise of data protection rights shall be submitted to the Data Protection Officer on any of the following:

Address: The Data Protection Officer
Legal & Data Protection Unit,
Police Headquarters,
Floriana, Malta.

Email: dpu.police@gov.mt

Telephone: (+356) 2122 4001

URL: <http://www.pulizija.gov.mt>