



ROYAL GIBRALTAR POLICE

PUBLIC CCTV SYSTEM PRIVACY NOTICE

Public Safety and Law Enforcement CCTV Network

This privacy notice relates specifically to the operation of the public safety and law enforcement CCTV network and the processing of personal data through that system.

It should be read alongside the Royal Gibraltar Police's broader organisational privacy notices, policies, and other data protection information, which explain more generally how the Royal Gibraltar Police collects, uses, stores, and protects personal data.

To view our wider organisational privacy notice, please see: [Privacy Notice](#) and [General CCTV Privacy Notice](#)

Introduction

This privacy notice explains how the Royal Gibraltar Police (the "RGP") uses personal data collected through the operation of its public safety and law enforcement CCTV network.

The network operates across certain locations within Gibraltar in order to support public safety, protect individuals and infrastructure, assist operational response, and help prevent, detect, and investigate criminal or harmful activity.

Because CCTV records images of people, vehicles, incidents, and activity within monitored areas, the operation of the system involves the processing of personal data.

We recognise that surveillance can affect individuals' privacy and other rights, particularly where monitoring takes place in public spaces. For this reason, the network is operated within a legal and governance framework designed to ensure that surveillance remains necessary, proportionate, properly controlled, and subject to oversight.

This notice explains:

- Why we use CCTV;
- What information may be recorded;
- How we use and protect that information;
- When information may be shared;
- How long recordings are kept; and
- The rights available to individuals whose information may be processed through the network.



1. Who We Are

Data Controller

The RGP is the data controller responsible for the personal data we process unless stated otherwise. There are many ways you can contact us, including by phone, email, and post. Please see our contact details below:

c/o Royal Gibraltar Police
New Mole House
Rosia Road
Gibraltar
GX11 1A
Tel: (+350) 20072500
Email: generalenquiries@royalgib.police.gi

Data Protection Officer

If you want to contact the Office of the Data Protection Officer regarding the processing of your personal data or the operation of the CCTV network, you may do so using the contact details below:

c/o Data Protection Officer
Information Management & Vetting Unit
Royal Gibraltar Police
New Mole House
Rosia Road
Gibraltar
GX11 1AA
Tel: (+350) 20072500
Email: dpo@royalgib.police.gi

2. Why do we use CCTV?

We use CCTV to support our public safety, security, safeguarding, and law enforcement functions. This includes:

- helping prevent and detect crime;
- supporting public safety and operational response;
- assisting investigations and legal proceedings;
- protecting individuals, property, and infrastructure;
- supporting safeguarding activity;
- preserving evidential material; and
- assisting competent authorities exercising lawful functions.

We do not use CCTV for arbitrary or excessive monitoring of the public.

Before CCTV cameras are installed or operated, assessments are carried out to consider whether surveillance is necessary and proportionate in light of the risks being addressed. This includes consideration of the location, the operational purpose of the CCTV camera, the level of intrusion involved, whether less intrusive measures are available, and the impact surveillance may have on individuals.



The use of CCTV remains subject to ongoing oversight and review to help ensure that surveillance continues to be justified, proportionate, and connected to legitimate law enforcement and public safety purposes.

3. What Information We Collect

The CCTV network records video footage within monitored areas.

This may include:

- Images of individuals;
- Vehicles and vehicle registration numbers;
- Incidents and events;
- Date, time, and location information;
- Operator activity;
- Camera movement records; and
- Audit and access logs associated with the system.

Some cameras include pan-tilt-zoom ("PTZ") capability. This allows authorised operators to reposition or zoom cameras where operationally necessary. Because this capability is more intrusive than static surveillance, its use is subject to enhanced controls, audit logging, operational restrictions, and supervisory oversight.

PTZ functionality will only be used for legitimate operational purposes and will not be used for arbitrary, speculative, discriminatory, or unjustified monitoring of individuals.

Not all cameras are monitored continuously in real time. In many cases, footage is recorded and reviewed only where necessary for operational, evidential, safeguarding, or investigative purposes.

Live Facial Recognition

In certain locations, the RGP may use Live Facial Recognition ("LFR") technology as part of its CCTV network for law enforcement and public safety purposes. LFR compares facial images captured by cameras against authorised watchlists to assist in locating individuals who are lawfully sought by the RGP for policing purposes, including the prevention and detection of crime, the protection of public safety, and the safeguarding of national security.

The use of LFR is subject to strict legal, operational and data protection safeguards. These include carefully controlled watchlists, human review of all potential matches, restricted access to personal data, and ongoing governance, auditing and oversight of the system. An LFR alert does not, by itself, result in any automated decision being made about an individual. All potential matches are subject to assessment by an authorised RGP officer.

LFR data is collected when an individual passes through a designated Zone of Recognition. Appropriate signage is displayed before individuals enter a Zone of Recognition to provide notice that LFR technology is in use.

Where LFR is utilised, the information processed may include:

- Facial images captured by LFR cameras;
- Biometric facial templates generated from those images;
- Perceived age;
- Perceived gender;



-
- Perceived height;
 - Perceived ethnicity;
 - Location, date and time metadata associated with the image capture; and
 - Where apparent from the image, information relating to a relevant disability or gender transition.
 - In limited circumstances, and only where apparent from the imagery, the processing may also involve information capable of revealing religious or philosophical beliefs, health-related information, or sexual orientation.

The RGP treats biometric data processed through LFR as sensitive personal data. Biometric data is used solely for the purpose of comparing facial images against authorised watchlists and generating biometric templates which enable the operation of the LFR system. Enhanced technical and organisational security measures are applied to protect this information. Biometric data is retained only for limited periods and in accordance with applicable data protection and law enforcement requirements.

Further information about the RGP's use of LFR, including the safeguards in place, applicable retention periods, and your rights under data protection legislation, can be found at <http://www.police.gi>

4. Our Lawful Basis For Processing

We process personal data through the CCTV network in accordance with Part 3 of the Data Protection Act 2004 (the "DPA 2004"), which governs the processing of personal data for law enforcement purposes.

The network is operated by us as part of our policing, public protection, safeguarding, and public safety functions under Gibraltar law, including the Police Act 2006.

We use CCTV for purposes connected to the prevention, detection, investigation, and prosecution of criminal offences, the protection of public safety, the safeguarding of individuals, and the protection of property, infrastructure, and public order within monitored areas.

In some circumstances, CCTV recordings may incidentally capture sensitive personal data or criminal offence related information. Where this occurs, the information is handled with additional care and subject to appropriate security, access, and disclosure controls.

We recognise that surveillance may affect privacy and other individual rights, particularly within publicly accessible areas. For that reason, the use of CCTV is subject to ongoing oversight and review to help ensure that its use remains lawful, necessary, and proportionate.

5. How We Get Information

Most personal data processed through the CCTV network is collected directly through camera recordings within monitored areas.

We may also receive related information from:

- Law enforcement agencies;
- Emergency services;
- Public authorities;
- Safeguarding bodies;



-
- Regulatory and/or oversight bodies;
 - Operational personnel;
 - Complainants or witnesses; and
 - Organisations assisting with investigations or incidents.

We seek to ensure that individuals are aware when CCTV monitoring is taking place through clear signage and this privacy notice. However, some information relating to the operation of the network may not be disclosed where this is necessary and proportionate for law enforcement, public safety, security, or investigative purposes.

6. What We Do With The Information

We use CCTV footage only where necessary to support the lawful purposes of the network. This may include:

- Responding to incidents;
- Reviewing security or safety events;
- Supporting criminal investigations;
- Safeguarding vulnerable individuals;
- Preserving evidential material;
- Assisting legal proceedings;
- Investigating operational or security-related incidents;
- Using Live Facial Recognition technology in authorised deployments, where necessary for law enforcement purposes and subject to strict safeguards;
- Responding to lawful requests for information; and
- Maintaining the security, integrity, and effective operation of the CCTV network itself.

Access to recordings is strictly controlled. Only authorised personnel with a legitimate operational need may access the system, and access is capable of audit and review.

We maintain documented operational, security, and governance procedures designed to ensure that footage is handled lawfully, securely, and consistently. This includes controls governing:

- Access to recordings;
- Operator conduct;
- Disclosure and evidential handling;
- Audit and monitoring arrangements;
- Retention and deletion processes;
- Incident management; and
- Oversight of the system and its use.

We do not use CCTV footage for unrelated purposes and do not permit arbitrary monitoring of individuals.

7. Sharing Your Information

We may share information where it is lawful, necessary, and proportionate.



This may include sharing information with:

- Law enforcement agencies;
- Office of Criminal Prosecution and Litigation;
- The Gibraltar Law Courts;
- The Employment Tribunal;
- Emergency services;
- Safeguarding authorities;
- Regulators and oversight bodies; and
- Organisations exercising official public functions.

We use specialist service providers, JT Security, to support the day-to-day operation, maintenance, hosting, monitoring, and security of the CCTV network. JT Security process information on behalf of the RGP under strict contractual controls and are only permitted to handle information in accordance with our instructions and applicable legal requirements.

Gibtelecom acts as an approved sub-processor who provide services, including secure data hosting and infrastructure support, operating under equivalent contractual, security, confidentiality, and oversight obligations.

We remain responsible for ensuring that appropriate safeguards, technical and organisational measures, access restrictions, and audit arrangements are maintained throughout the processing chain.

Where information is shared or disclosed, we document our decision making and apply safeguards designed to minimise unnecessary or excessive disclosure. This includes controls relating to authorisation, redaction, secure transfer, evidential handling, audit logging, and access monitoring.

CCTV footage is not used for marketing purposes and is not made publicly available unless disclosure is required by law or is otherwise considered lawful, necessary, and proportionate in the circumstances.

8. International and Cross-Border Transfers

Due to the operational context of the CCTV network, it may, at times, be necessary to share information with competent authorities outside Gibraltar, including authorities within jurisdictions where this is necessary for law enforcement, safeguarding, public protection, or legal purposes.

Any cross-border disclosure is subject to applicable legal requirements, appropriate safeguards and must be assessed on a case-by-case basis to protect the confidentiality, security, and lawful handling of the information.

Cross-border disclosures are not carried out routinely and will only take place where there is a lawful and operationally justified reason to do so.

9. How Long We Keep Information

Routine CCTV footage is generally retained for approximately 31 days, after which it is automatically deleted or overwritten unless it is required for an active investigation, safeguarding activity, legal proceedings, complaint handling, evidential preservation, or another legitimate operational purpose requiring continued retention.



In certain operationally sensitive locations, and where supported by a documented operational justification, specific cameras may be subject to extended retention periods of up to 365 days. This may apply where longer retention is considered necessary for law enforcement, public protection, evidential, intelligence, or security-related purposes, including situations where incidents or investigative activity may not come to light immediately.

Where footage is retained beyond standard retention periods, retention is justified, appropriately authorised, and subject to ongoing review to ensure that recordings are not kept for longer than necessary.

10. Security and Confidentiality

We take the security of CCTV information seriously.

We apply technical and organisational measures designed to protect recordings and associated information against unauthorised access, misuse, disclosure, loss, alteration, or destruction.

These measures include:

- Access restrictions;
- Authentication controls;
- Encryption;
- Audit logging;
- Network protections;
- Operational monitoring;
- Secure export controls;
- Retention and deletion controls; and
- Incident response procedures.

Because CCTV footage may contain sensitive operational or evidential material, access to the system is carefully controlled and monitored.

Any misuse of the CCTV network, inappropriate disclosure of footage, unauthorised access, or excessive surveillance activity may result in disciplinary action, contractual enforcement measures, regulatory reporting, or legal proceedings where appropriate.

11. Your Data Protection Rights

Under data protection law, you have rights we need to make you aware of. The rights available to you depend on our reason for processing your information.

Right to be informed

You have the right to be informed about how your personal data is collected, used, stored, and shared. This includes information about the purposes for which your information is processed, the legal basis for the processing, how long information is retained, and who it may be shared with.

The RGP provides this information through privacy notices, operational notices, policies, and other transparency materials made available to the public.



Right of access

You have the right to request access to personal data held about you and, where applicable, obtain a copy of that information.

This is commonly referred to as a Subject Access Request. Before information is disclosed, we may need to verify your identity and request sufficient information to identify the relevant records.

Certain information may be withheld where exemptions apply under applicable legislation, including where disclosure would prejudice law enforcement activity, criminal investigations, public safety, national security, legal proceedings, or the rights and freedoms of others.

Right to rectification

You have the right to request correction of personal data that you believe is inaccurate or incomplete.

In the context of CCTV recordings and law enforcement processing, it may not always be possible or appropriate to alter original footage or evidential records. However, where appropriate, we may correct inaccurate associated information, update records, add supplementary information, or record that the accuracy of information has been challenged.

Requests for rectification will be considered on a case-by-case basis, taking into account the nature of the information, the purpose for which it is being processed, and any legal or evidential obligations that apply.

Right to erasure

In certain circumstances, you may request the deletion of your personal data.

This right is not absolute and may not apply where we are required to retain information for law enforcement, safeguarding, evidential, legal, regulatory, public protection, or statutory purposes.

Retention periods and deletion requirements are governed through internal retention and records management procedures.

Right to restrict processing

In certain circumstances, you may request that we restrict the processing of your personal data, for example, where the accuracy of the information is disputed or where there is a question about the lawful basis for the processing.

Where processing is restricted, the information may continue to be stored and may still be processed where this is permitted by law, including for law enforcement, public safety, safeguarding, legal, or evidential purposes.

Requests for restriction will be considered on a case-by-case basis, taking into account the nature of the information, the purpose of the processing, and any applicable legal or operational obligations.

Right to object

In certain circumstances, you may have the right to object to the processing of your personal data.

However, where personal data is processed for law enforcement purposes under Part 3 of the DPA 2004, this right may be limited or may not apply in the same way as it does under the Gibraltar General Data Protection Regulation.



Any objection will be considered on a case-by-case basis, taking into account the nature of the processing, the purpose for which the information is being used, and the legal and operational obligations of the RGP.

The right to object may be restricted where this is necessary and proportionate to avoid prejudice to investigations, legal proceedings, crime prevention activity, public safety, national security, or the rights and freedoms of others.

Rights relating to automated decision-making

You have rights relating to certain forms of automated decision making and profiling.

The RGP does not routinely make solely automated decisions that produce legal or similarly significant effects without meaningful human involvement.

The CCTV network covered by this notice does not currently use facial recognition technology, automated behavioural analysis, or automated decision-making systems to make decisions about individuals.

Right to data portability

In limited circumstances, you may request that personal data you have provided be transferred to another organisation or provided to you in a structured, commonly used, and machine readable format.

This right only applies in certain situations set out in data protection legislation and will not generally apply to information processed for law enforcement purposes under Part 3 of the DPA 2004.

12. Exercising Your Rights

Requests relating to your personal data may be made by you directly or, where appropriate, by a legal representative acting on your behalf.

Requests should normally be made in writing and should provide sufficient information to allow us to identify the records or information concerned.

We may request proof of identity before responding to a request. To help us identify relevant footage, we may ask you to provide information such as the approximate date, time, and location involved.

Where information is processed for law enforcement or public security purposes, some rights may be restricted where this is necessary and proportionate to avoid prejudice to investigations, legal proceedings, public safety, crime prevention activity, or the rights and freedoms of others.

Requests and enquiries relating to data protection rights may be sent to our Data Protection Officer at dpo@royalgib.police.gi.

We will respond to requests within the applicable statutory timeframes unless an extension is permitted by law.

13. Your Right to Complain

We work to high standards when processing personal data.

If you have concerns about how your information has been handled, please contact us first so that we can investigate the matter, via email to: dpo@royalgib.police.gi.



You also have the right to make a complaint to the Gibraltar Regulatory Authority (the "GRA") if you believe your personal data has been processed unlawfully or in a way that does not comply with applicable data protection legislation. You can contact the GRA at privacy@gra.gi.

14. Further Information

Further information about how we process personal data can be found in our privacy notices and related data protection documentation available on our website.

15. Changes To This Privacy Notice

We keep this privacy notice under regular review to ensure that it remains accurate, up to date, and reflects how the CCTV network operates in practice.

Changes to the operation of the CCTV network, the legal framework governing the processing, or the purposes for which the system is used may result in updates to this notice.