



Policy Document

Policy Title	Royal Gibraltar Police Overt LFR
Policy Statement	Establishes procedures for the deployment of Live Facial Recognition (LFR) technology in support of policing and national security operations.

Managing Information	
Policy Owner	Superintendent Professionalism
Policy Author	Isolas LLP
Endorsed by	Supt S. Perera
Endorsement Date	15/07/2026
Signature	
Approval by the Gibraltar Police Authority	
Approval Date	

To be completed by Corporate Services only	
Reviewed	15/07/2026
Reviewed by	Aaron Ignacio
Next Review Date	

Contents

1.	Policy Overview	3
2.	LFR use cases	3
3.	How LFR works	4
4.	‘Where’- Date, Time and Location of LFR	5
5.	‘Who’ – Watchlist Generation and Criteria for an Image’s Inclusion on a Watchlist.	5
6.	Proportionality	12
7.	Management of Risk, Resource Levels and dealing with Alerts.	13
8.	Governance and oversight.....	14
9.	Data Retention, Data Management & Transparency	14
10.	Contact Information.....	15

1. Policy Overview

- 1.1. Facial recognition technology (“FR”) has several potential applications within a law enforcement context. The term “overt” is used to refer to the RGP’s use of live facial recognition (“LFR”) in a manner that can be detected by those members of the public who may be affected by it, particularly using awareness raising measures outlined in section 9.3 of this Policy.
- 1.2. The RGP uses LFR to assist with the prevention and detection of crime, the protection of public safety, the location of wanted and vulnerable persons as well as the discharge of its statutory law enforcement functions and for the protection of Gibraltar’s National Security.
- 1.3. This Policy sets out the principles and procedures which govern the RGP’s approach to LFR use, as well as explaining at a practical level how FR physically works within a live setting. LFR in Gibraltar comprises of a network of fixed cameras with LFR functionality installed at approved locations throughout Gibraltar which operates on a continuous and permanent basis. The purpose of this Policy is to ensure that the use of LFR:
 - (a) Is lawful;
 - (b) Is necessary and proportionate;
 - (c) Is subject to appropriate human oversight;
 - (d) Respects fundamental rights and freedoms;
 - (e) Complies with applicable data protection legislation as well as the Gibraltar Constitution; and
 - (f) Maintains public confidence through transparency and accountability.
- 1.4. Unlike temporary event-based LFR deployments, the RGP’s LFR capability operates through permanently installed infrastructure located at approved sites throughout Gibraltar and operates continuously subject to the safeguards contained in this Policy.

2. LFR use cases

- 2.1. LFR has been installed at various key locations throughout Gibraltar, which have been carefully selected to assist the RGP to pursue its statutory and policing objectives, the RGP may for various reasons need to locate individuals, including in respect of national security and the policing of Gibraltar’s fluid border with Spain. Such individuals are referred to in this policy as “Sought Persons”. LFR is a policing tool which harnesses digital technology, and in particular live FR technology, to assist the RGP in locating Sought Persons. The use of LFR may also serve to achieve the RGP’s policing objectives by helping to deter or disrupt criminality or other conduct posing a risk to public safety.

- 2.2. Pursuant to this policy, the RGP will only use LFR in support of Gibraltar's national security objectives to assist with the prevention and detection of crime, the protection of public safety and the location of wanted and vulnerable persons.

3. How LFR works

- 3.1. The RGP LFR system consists of a network of permanently installed fixed cameras located at approved operational locations throughout Gibraltar, but mainly in the vicinity of the land border with Spain and various junctions at Main Street. The system continuously analyses facial imagery captured within designated Zones of Recognition and compares such imagery against authorised watchlists.
- 3.2. The use of the core technical operation of LFR can be summarised in the following stages as follows:

Stage	Action
1	Construction of Watchlist Two tiers of Watchlist have been constructed using images of Sought Persons which are already held by the RGP or other International Law Enforcement Agencies. The LFR software then detects and analyses the facial features shown by the images to then express those features as a set of numerical values (i.e. a Biometric Template).
2	Facial image acquisition The LFR cameras provide CCTV footage of those persons who appear within the Zone of Recognition in real time, as a live feed to the LFR computer system.
3	Face detection The LFR software detects individual human faces within the images captured by the LFR live feed.
4	Feature extraction The LFR software produces a Biometric template of the facial features of each detected face.
5	Face comparison The LFR software compares the Biometric Template of the facial images of persons captured via the live LFR feed with the Watchlist Biometric Templates.
6	Matching When the Biometric Templates obtained via the live feed are compared with the Watchlist biometric templates, the LFR system generates a similarity score. This is a numerical value indicating the extent of similarity between the Templates, with a higher score indicating greater points of similarity. If the score surpasses a pre-set threshold value, the LFR software will generate an Alert to indicate that a possible match has occurred. For the avoidance of doubt, the RGP will not be monitoring the live CCTV feed, rather, following the matching process the RGP will review the images of persons whose image has generated an Alert. This approach to the operation of the LFR system has been adopted specifically to minimise the impact of LFR on members of the public.
7	RGP Officer consideration of matched images

	Once an Alert has been generated, RGP Officers who are trained on LFR use and who are aware of required and appropriate LFR operational responses, will assess the relevant candidate image against the relevant watchlist image images (via the adjudication process by a RGP officer in the control room) and make a decision as to whether they consider the match to be viable, and if so whether any further action is required.
8	LFR data destruction In the absence of an Alert, the biometric templates created in respect of members of the public whose images have been captured by the LFR will be deleted within 72 hours. Subject to the limitations described in paragraphs 9.3 below, all LFR CCTV footage is deleted within 31 days of capture.

4. 'Where'- Date, Time and Location of LFR

4.1. As highlighted at various junctures, the RGP has a network of permanently installed LFR cameras at various locations in Gibraltar which operate continuously on a 24/7 basis. These cameras are located at the following locations:

- Land border with Spain;
- Four Corners;
- Winston Churchill Avenue;
- Gibraltar Sir Joshua Hassan International Airport;
- Kingsway Tunnel;
- Casemates; and
- Main Street.

4.2. These locations have been specifically selected on the basis that the RGP considers there to be reasonable grounds to suspect that the Deployment Locations are one at which one or more persons on the Watchlist will attend at a time or times at which they are to be sought by means of LFR. They have also been carefully selected to ensure that the RGP maintains a level of oversight over those persons entering Gibraltar and ensure that those persons on Watchlists who may enter Gibraltar may be appropriately intercepted.

5. 'Who' – Watchlist Generation and Criteria for an Image's Inclusion on a Watchlist.

5.1. This section covers the composition, generation and management of Watchlists to be used in LFR Deployments and is structured to address:

- (a) Safeguards relevant to all Watchlists – including safeguards which apply to all Watchlists and further safeguards which have been adopted in relation to certain protected characteristics;
- (b) Who may be added to a Watchlist- including in relation to police-originated, and non-police originated imagery.

Safeguards relevant to all Watchlists

5.2. The criteria for the construction of the Watchlist for use with LFR has been approved by the Commissioner of Police. As LFR will be operating on a continuous basis, the RGP has created one watchlist with two distinct tiers, a Tier 1 and a Tier 2. Tier 1 being the most critical to detection and action, which will assist the RGP. The Watchlist and the images utilised have been designed to ensure that it complies with the following requirements:

Requirement	Rationale for the requirement
Intelligence: The Watchlist has been driven and determined by policing needs and based on intelligence cases which have been reviewed on an ongoing basis.	This approach has ensured that the make-up of the Watchlist is reflective of, and for the purpose of the RGP's statutory policing and national security objectives.
Image Sources: The RGP must be reasonably satisfied that images for use in the Watchlist is lawfully held by the RGP with consideration also being given as to: - the legal basis under which the image has been acquired; and - the source of the image, particularly where the image is derived from a sensitive or third-party source and may risk compromising that source or exposing that source to risk.	This requirement has ensured that all images which have been included in the Watchlist are lawfully held by the RGP- this includes considerations of the legal basis, human rights (including intrusion) and data protection considerations. This ensures that in all cases, the lawfulness and intrusion caused by using the image is considered and justified. It also ensures that where the legal basis limits how the police hold and process an image (for example for what purposes it may be used), this is considered to ensure legal compliance. Additionally policing has a responsibility to avoid compromising police tactics or exposing sources to risk- this requirement covers this point.
Image selection: The RGP has taken all reasonable steps to ensure that all images which have been used on the Watchlist: - Are of persons intended for inclusion on the watchlist; and - Is the most up to date and/or suitable image available to the RGP that is of appropriate quality for inclusion on the Watchlist. The RGP has also considered the prospects of the LFR System generating an Alert should an older image be used for inclusion on the Watchlist as individuals facial features may have changed or aged significantly since the	This requirement is to ensure that the act of placing a person on a Watchlist is best aligned with locating that persons should they pass the LFR System. This requirement and the prescribed False Alert Rate is also designed to minimise the likelihood of unduly inconveniencing others not of interest to policing whilst ensuring those sought are located. The RGP has determined the 1:1000 False Alert Rate represents an approach which balances these factors in a proportionate way.

image was taken. The RGP therefore endeavour to ensure that images used are the most up-to-date images available. The RGP has also had due regard to and the processor's aim to ensure that an acceptable False Alert Rate is achieved. Testing will take place throughout the operation of LFR to ensure that Thresholds may be adjusted to reach and maintain a False Alert Rate which is as low as possible.	
Watchlist currency: Watchlists will be updated every 3 to 6 months, or where no longer needed.	This is to ensure the ongoing currency of the Watchlist remains relevant
Watchlist design: Watchlists should benefit from technical measures being adopted through the segregation within the Watchlist.	This is to ensure the status of those on a Watchlist is recognised by those involved in undertaking Engagements in order to ensure the appropriate action is taken should an Alert be generated.

Additional Safeguards

- 5.3. The RGP has additionally created a best practice document, to ensure suitable controls, exist around the placing of persons with protected characteristics on the Watchlist. Any controls, mitigations and processes identified by the RGP in this document reflect the RGP's system performance and RGP's use case for LFR.
- 5.4. The RGP has confidence in LFR System's performance, particularly in relation to gender, age and race.
- 5.5. The RGP recognises that *regardless* of performance considerations, it should take particular care when considering and publishing details relating to (i) age including the protection of children- particularly the very young, (ii) the disabled, and (iii) those who have and/or are undertaking a gender reassignment. This is because:
 - a) There may be different privacy expectations around the use of LFR and that these can be particularly relevant in relation to these people given their potential vulnerability.
 - b) The RGP recognises that those involved in criminality have the wherewithal and capability to exploit information to their advantage. This may arise if there is a published performance differential that shows a lower performance level in relation to a particular protected characteristic.
- 5.6. Documenting composition: Prior to adding a person onto the Watchlist, the RGP will specifically identify and document whether the person is believed or suspected to be:

- a) aged under 18-years old;
- b) aged under 13-years old;
- c) a person with a relevant disability;
- d) a person who has undertaken a gender reassignment and it is believed or suspected to be that the image uploaded onto the Watchlist is an image of that person taken prior to their gender reassignment.

5.7. Safeguarding regarding composition: The following outlines further, specific safeguards that apply to the composition of the Watchlist:

	Age (U.18)	Age (U.13)	Disability	Gender Reassignment
Circumstances				
	LFR is used to locate a person under 18 and that person's records state that person is aged (or suspected to be under aged) under 18-years old.	LFR is used to locate a person under 18 and that person's records state that person is aged (or suspected to be aged) under 13 years-old.	LFR is to be used to locate a person and that person's records state that person has (or is suspected to have) a relevant disability.	LFR is to be used to locate a person and that person's records state that person has (or is suspected to have) (i) undertaken a gender reassignment and (ii) it is believed or suspected to be that the Watchlist would be using an image of that person taken prior to their reassignment
Safeguards				
Necessity	Specific regard needs to be had for the importance of locating the subject on a risk-based approach in line with SWP LFR Documents with a particular focus on ensuring the necessity case is fully made out.			
Watchlist Images		There is a particular need to ensure that the image is as current as possible and of a suitable quality for inclusion on the Watchlist.		
Legal Advice		Specific advice must be sought to assist the RGP in ascertaining whether to include on the Watchlist and		

		which will outline whether further safeguards should apply.
Technical Advice	Regard should also be had to consider System and Subject Factors and the ability for the LFR System to generate an accurate Alert against the image proposed for inclusion on the Watchlist.	
	Consideration should be given to the likely crowd flow/occlusion risk where shorter subjects may otherwise be blocked from the camera's line of sight.	Technical advice should be sought on a case-by-case basis to inform this assessment. Where authorisation is then sought, this advice needs to be provided to the RGP to help inform their decision making and allow the RGP Officer to record their decision regarding any inclusion on the Watchlist and outline further safeguards that should apply.

Police-originated images that may be included on a Watchlist.

5.8. Images that may be deemed appropriate for inclusion within an LFR Watchlist include custody images of individuals and/or police originated images other than custody images of people who are:

- a) wanted by the courts or the RGP for certain indictable only offences; and/or
- b) deemed to be a risk to Gibraltar's National Security; and/or
- c) suspected of having committed, or where there are reasonable grounds to suspect that the individual depicted is about to commit an offence or where there are reasonable grounds to suspect an individual depicted to be committing an offence; and/or
- d) missing persons deemed increased risk; and/or
- e) subject of information or intelligence that would lead to suspicions of an immediate threat to life; and/or
- f) subject of information or intelligence that would lead to suspicions of an immediate risk of serious harm- including safeguarding the welfare of vulnerable people, including children at risk of imminent abuse of otherwise harmed.

5.9. Where police originated images other than custody images are considered for use, consideration regarding the inclusion of such images is needed. Such consideration requires a case-by-case assessment. Relevant factors in that assessment may include the purpose for which the police hold such images, any processing limitations attached to the images, the importance of including such images on a Watchlist to meet a policing objective and the proportionality of using such images on an LFR System.

Non-police originated sources of Watchlist imagery.

5.10. Where it is viable to do so without unduly impacting on the performance of the LFR System, suitable police-originated images should be preferred for inclusion on a Watchlist. However, there will be occasions, where no image is held by the RGP or the wider law enforcement community, or if one is held, its quality or currency is not optimal for facial recognition purposes. In these circumstances, consideration may be given to the inclusion of non-police originated image. For the avoidance of doubt, this policy does not provide a basis to proactively acquire images solely for use on an LFR Watchlist.

5.11. Non-police originated images are images which have not been taken by law enforcement. The expectations of privacy, and the intrusion associated with such images can vary depending on the nature of the image and to aid decision making and foreseeability, these have been attributed to three 'layers of intrusiveness'.

Assessing Non-police originated sources of Watchlist imagery	
	
Imagery	Layer A Layer B Layer C
Image Layer	Outline
Non-Police originated image- Layer A	Non-police originated images where it is assessed that the public would expect the law enforcement to have access to them (but not including images obtained by covert means) with examples of criteria including: - circumstances where images are readily available to the police through open-sources and/or the public have provided information to the police, including but not limited to appeals for information, imagery and footage; - circumstances where the police have obtained the image because of a lawful power of search or seizure; - data held by public bodies including where there are information sharing arrangements to support the regular sharing of data or explicit legal powers for information sharing.
Non-police originated image- Layer B	Images where it is assessed that they raise elevated expectations of privacy or where otherwise obtained covertly without the knowledge of the subject.
Non-police originated image – Layer C	Non-Police originated images in circumstances where it is assessed that the public would not typically expect their image to be shared to or accessed by the police at the point they provided it but there is nevertheless a lawful basis for the police to hold the imagery it has received.

	To help the public foresee where this may arise, this could include circumstances where the public have shared their image with a controller of data for an explicit purpose (be with a person, business, public body or other third party) and it was not in their contemplation at the time of sharing their image that it may be used for a law enforcement purpose. This would be particularly relevant where the controller promotes an approach to privacy which does not typically collaborate with Gibraltar law enforcement.
--	--

5.12. Any non-police originated image should only be included in a Watchlist where the necessity test to do so is made out. The RGP should consider all the circumstances pertaining to the image and in particular which layers of intrusiveness the image is attributable to and the factors at 5.11 above.

5.13. The type of non-police originated images that may be deemed appropriate for inclusion within the LFR Watchlist are of people:

- a) wanted by the courts or the RGP for certain indictable only offences; and/or
- b) deemed to be a risk to Gibraltar's National Security.
- c) suspected of having committed, or where there are reasonable grounds to suspect that the individual depicted is about to commit an offence or where there are reasonable grounds to suspect an individual depicted to be committing an offence; and/or
- d) missing persons deemed increased risk; and/or
- e) subject of information or intelligence that would lead to suspicions of an immediate threat to life; and/or
- f) subject of information or intelligence that would lead to suspicions of an immediate risk of serious harm- including safeguarding the welfare of vulnerable people, including children at risk of imminent abuse of otherwise harmed.

5.14. **'Wanted by the courts or the RGP for indictable only offences'**- This term includes those with outstanding arrest warrants for indictable only offences or who are otherwise required by the courts in respect of those offences. The courts have already given consideration as to the necessity to locate this category of persons and given a direction that they should be apprehended. The RGP have also considered the need to locate and apprehend such persons. Such people pose a risk to the public in general.

5.15. **'Persons deemed to be a risk to national security'**- This term includes those who may be wanted by Interpol and included in Interpol Notices or those linked to or convicted with Terrorism related offences.

- 5.16. **‘Missing persons deemed increased risk’**- This term will be subject to the UK College of Policing definition of Medium Risk (or above)¹ that is contained in the Missing Persons APP, meaning that the risk of harm to the subject or public is assessed as likely but not serious. The harm can apply equally to the subject or any other member of the public. A decision to include a missing person on the watchlist should take into account the individual circumstances of each case, including the impact it may have on the missing person and their expectations or privacy.
- 5.17. **‘Immediate threat to life; and/or immediate risk of serious harm- including safeguarding the welfare of vulnerable people, including children at imminent risk of abuse or otherwise harmed’**. This ground will reflect that inclusion in the Watchlist is necessary to locate the person in order to manage risk of serious harm or an imminent need to safeguard an individual to ensure their continued welfare. The risk of harm will be informed by intelligence case.

6. Proportionality

- 6.1. Prior to the installation of the LFR Cameras, the RGP has considered whether the installation of the LFR cameras at their proposed locations is a proportionate means of achieving the RGP’s policing and national security objectives, in light of the impact of the rights and freedoms of members of the public.
- 6.2. The RGP has concluded that the use of LFR at the various set locations on a continuous basis is a proportionate means of achieving the RGP’s policing and national security objectives, in light of the rights and freedoms of members of the public, which has been created by virtue of the installation of LFR.
- 6.3. In particular, key regard has been had to Section 7 of the Gibraltar Constitution (Protection for Privacy of Home and other property) and the fixed locations of the LFR cameras have been carefully selected to ensure that they are not close to clinics or schools, in respect of which persons will have a higher expectation of privacy. The fixed locations of LFR have all been placed in locations where persons have a lesser expectation of privacy, including at the land border and the main entry/exit points of Main Street in Gibraltar.
- 6.4. The RGP has also considered the effects of Section 14 of the Gibraltar Constitution (protection from discrimination on ground, race, etc), which protects people from discrimination in the enjoyment of one or more other human rights, even when those other human rights have not been breached. The RGP is satisfied that the Deployment of LFR is proportionate as against the risk that LFR may have a particular impact on one group in society, for example because of characteristics relating to their sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property or birth.

¹ The RGP applies and follows UK practice as set down by the UK College of Policing.

- 6.5. In considering whether to deploy LFR across Gibraltar, the RGP has considered whether there are any alternative means of achieving the relevant policing and national security objectives, which would have a lesser adverse impact on the fundamental rights and freedoms of potentially affected members of the public. As part of the Deployment of LFR, the RGP is satisfied that the introduction of LFR in place of physical checks at the frontier is a less intrusive method of protecting Gibraltar's national security and that the installation of LFR does not amount to an undue interference with the rights and freedoms of members of the public.
- 6.6. The location of all LFR cameras has all been selected in locations which in the RGP's opinion, strike a fair balance between any interference with the rights and freedoms of those affected by the installation of LFR and the achievement of the relevant policing objectives. The RGP has had due thought and regard to the following circumstances:
- (a) *The degree to which the Deployment of LFR will enable policing and national security objectives to be achieved.*
 - (b) *The degree to which the Deployment of LFR supports fundamental rights and freedoms.*
 - (c) *The degree to which non-LFR alternatives could have been used.*
 - (d) *The degree to which the Deployment would interfere with fundamental rights and freedoms.*

7. Management of Risk, Resource Levels and dealing with Alerts.

- 7.1. In Deploying LFR, the RGP has considered the anticipated risk to officers and the public as against the overall intelligence picture, relevant factors linked to persons included on the Watchlist (e.g. seriousness of offences and warning markers linked to the use of violence, carriage of weapons, and propensity to escape, etc), the physical environment surrounding the locations where LFR has been installed and operates, the continuous duration, the need to protect Gibraltar's community, and the reality of a free-flowing border with Spain.
- 7.2. The RGP will ensure that there is a sufficient number of appropriately trained RGP officers to respond to Alerts. This is important to ensure that the LFR system, and the data processed by it, is being properly and effectively used. To assist, the RGP will also operate a two-tiered Watchlist, Tier 1 being the most critical to detect and action.
- 7.3. Response to an Alert- As the LFR cameras will permanently be installed in several locations across Gibraltar, it will not be possible for RGP Officers to be within the Zone of Recognition on a permanent basis. Accordingly, following the generation of an Alert, RGP Officers at the control room will undertake an Adjudication as to whether to initiate a Grade 1 response, having regard to the likelihood of Subject, System or Environmental Factors influencing the generation of an Alert. The decision to respond to an Alert will not be an automatic process. Subject to an Adjudication process and an assessment of risk, the general expectation is that

the Alert will trigger a Grade 1 response and RGP Officers will then respond to the Alert with a view to detaining the individual in question.

- 7.4. Whilst RGP Officers must exercise their own discretion when using their powers of arrest and detention, RGP policy is that an LFR system-generated Alert on its own, indicating that a person is on the Watchlist, should not be taken as providing sufficient grounds by itself for arrest, search or detention. Officers should seek to make sufficient additional enquiries to satisfy themselves of their grounds to arrest, search or detain. Where confronted with a non-complaint subject, and the circumstances are such that an officer has an honestly held belief that they must use their powers of arrest/detention before further checks have been possible, and this results in the use of those powers, then further checks (as necessary) should be made as soon as is reasonably practicable, so that the decision to arrest/detain is reviewed without unnecessary delay.
- 7.5. If an Engaged Individual cannot be identified or fails to confirm their identity, this alone does not constitute a criminal offence and does not necessarily render them liable to arrest. Officers must be in a position to justify the use of any powers, any action taken, and have a lawful basis for doing so.
- 7.6. All RGP officers and staff tasked with the operation and management of the LFR systems will receive LFR training.

8. Governance and oversight

- 8.1. Governance and operational oversight of the use of the technology is routinely carried out. In view of the permanent and continuous operation of LFR, relevant reviews will initially be carried out after the first 9 months of operations and yearly after that.
- 8.2. The continuous review of the LFR Deployment is such to permit and ensure that the use of LFR remains an effective and proportionate policing tool.
- 8.3. The retention of the CCTV footage for up to 31 days provides a means by which Alerts can be retrospectively reviewed by technical analysts to inform the future operation of the LFR System.

9. Data Retention, Data Management & Transparency

- 9.1. The RGP must ensure that the processing of any data associated with LFR is conducted in a lawful way and in compliance with the RGP LFR documentation. This means that a person's biometric data will be deleted within 72 hours, irrespective as to whether they generate an Alert or otherwise.

9.2. All CCTV footage generated from LFR Deployments is deleted within 31 days, except where retained:

- a) In accordance with the Data Protection Act 2004 and the Criminal Procedure and Evidence Act 2011 and/or
- b) In accordance with the RGP's complaints/conduct investigation policies.
- c) To support compliance the LFR application has a full audit capability, and the RGP officer log is retained in line with standard retention periods.
- d) in accordance with an approved programme of testing in order to provide for the continued evaluation of the LFR system using operationally realistic data, any requirement to retain the CCTV footage for longer than 31 days will be subject to an approved DPIA for such testing and arrangements to ensure data subjects are informed as to the arrangements that will apply to the use and retention of such data.

9.3. The public will be aware of the existence of LFR through the relevant signage which has been implemented and installed within all Facial Recognition Zones.

10. Contact Information

10.1. The RGP LFR team can be contacted using the following email address:
dpo@royalgib.police.gi

ANNEX A: Terms and Definitions

1. Terminology

1.1. Within the RPG and throughout the RGP's LFR Documents, the following terms and definitions apply in relation to Live Facial Recognition

Adjudication	Means a human assessment of an Alert generated by the LFR system by an RGP Officer (within the RGP Control Room), to decide whether to Engage with the individual matched to a Watchlist image. In undertaking the Adjudication process, regard is to be paid to Subject, System and Environmental Factors (as described further in the RGP's LFR Documents).
Alert	Means the alert generated by the LFR System when a facial recognition image from the video stream, which is being compared against the Watchlist, returns a comparison (similarity) score above the set Threshold.
Biometric Template or Template	Is a digital representation of the features of the face that have been extracted from the

	facial image. It is these Templates (and not the images themselves) that are used for searching. Note that Templates are proprietary to each facial recognition algorithm and new Templates will need to be generated from the original images if the algorithm is changed.
Blue Watchlist	A Watchlist comprising of known persons that can be used to test system performance. For example, police officers / staff may be placed on a Blue Watchlist and 'seeded' into the crowd who walk through the Zone of Recognition at the start of a Deployment to measure the True Recognition Rate.
Candidate Image	Means the image of a person from the Watchlist return as a result of an Alert.
Confirmed False Alert	Means, following an Engagement, it has been determined that the Engaged individual is not the same as the person in the Candidate Image in the Watchlist.
Confirmed True Alert	Means, following an Engagement, it has been determined that the Engaged individual is the same as the person in the Candidate Image in the Watchlist.
Deployment	Means the deployment of LFR across the various permanent locations in Gibraltar on a continuous rolling basis.
Engagement	Means when an RGP Officer communicates with a member of the public because of an LFR Alert.
Environmental Factor	An external element that affects LFR system performance such as dim lighting, glare, rain, mist, etc.
False Alert	Means that it is determined that the Probe Image is not the same as the Candidate Image in the Watchlist, based on an Adjudication without any Engagement.
False Alert Rate (also known as the False Positive Identification Rate.)	Describes the number of individuals that are not on the Watchlist who generate a False Alert or Confirmed False Alert as a proportion of the total number of people who pass through the Zone of Recognition
False Negative	Is where a person on the Watchlist passes through the Zone of Recognition but no Alert is generated.

Indictable Offence	
Probe Image	Means the facial image submitted for a facial search against the Watchlist.
Protective Security Operation	Means a specific security operation aimed at keeping the public safe and/or protection property or national infrastructure.
Sought Persons	Persons included on an LFR Watchlist.
Subject Factor	Means a factor linked to the individual. For example, the individual is wearing a head covering, is smoking, eating, or looking down at the time of passing the camera.
System Factor	Means a factor relating to the LFR system such as the algorithm
Threshold	Means the configurable point at which two images being compared will result in an Alert. The Threshold needs to be set with care to maximise the probability of returning correct suggested matches whilst keeping the number of False Alerts to an acceptable level. (NB. It should be noted that any FR algorithm is only returning 'suggested' matches, based on the chosen Threshold, and that it is for a human to assess the true likelihood that the images relate to the same person.
True Alert	When it is determined that the Probe Image is the same as the Candidate Image in the Watchlist.
True Recognition Rate (also known as the True Positive Identification Rate)	Describes the total number of times an individual(s) known to have passed through the Zone of Recognition and correctly generated an Alert, as a proportion of the total number of times the same individuals pass through the Zone of Recognition, regardless of whether an Alert is generated by the LFR system or not. By way of an example, the rate would be 90% if 10 people on the Watchlist each pass the LFR system, and an Alert is generated correctly for 9 out of 10 of those people. The same would be true if 5 people each pass the LFR system twice, and 2 Alerts were correctly generated for 4 of the people and only 1 correct Alert for the 5th person
Use Case	Means the RGP may for various reasons need to locate Sought Persons.

Watchlist	Means, as the inclusion of Sought Persons as a response to the particular Use Case, as outlined in section 4 of the RGP.
Zone of Recognition (ZoR)	Means 3-dimensional space within the field of view of the camera and in which the imaging conditions for robust face recognition are met. In general, the Zone of Recognition is smaller than the field of view of camera, e.g. not all faces in the field of view may be in focus and not every face in the field of view is imaged with the necessary resolution for face recognition.