Classification	OFFICIAL
Handling Instructions	No restriction on distribution
Disclosable (FOI / Publication Scheme)	Yes

Data Protection Impact Assessment (DPIA) – Stage 1	
Project Name	Live Facial Recognition
Project Lead	LFR Business Lead
SRO	A-Network Policing ACC Command
Division/Department	B-Division
Information Asset Owner	C/Supt Chris Casey
Date for start of intended processing	December 2025
Date submitted to Information Management	10/02/2026

A DPIA is a Data Protection risk assessment which must be considered and completed if required before commencement of any project or initiative involving the processing of personal data. Therefore, the process should be started during the early planning stages of any project and have received approval from the Force Data Protection Officer before any data is processed.

The DPIA processes helps the organisation to identify and fix any problems at an early stage in a project and therefore helps to avoid later data breaches or non-compliance with Data Protection requirements that can otherwise be the subject of significant financial penalties. The process assists BTP in complying with our obligations to process personal data in a lawful, fair and transparent manner and to be accountable for how we do so.

A DPIA is only necessary for systems or projects processing personal data of individuals. Please contact the Data Protection & FOI team if you have any queries or are unsure whether this applies.

Information Management Outcome (IM Use Only)	
Stage 2 DPIA not required – please retain this form with project documentation	☐
Stage 2 DPIA required	☒
Stage 2 DPIA required unless additional actions completed (see below)	☐
Assessed By	Deputy Data Protection Officer
Role	Deputy Data Protection Officer
Date	10/02/2026

Further Actions Required	
Completion of the below recommended actions will avoid the need for a Stage 2 DPIA. Once completed, this should be recorded below, and the form retained with project documentation.	
Required action:	
Required action:	
Required action:	
Actions Completed By	

Date	

Section 1: Purpose, Scope & Extent of Processing

In this section you will explain what personal data is used, how it will be used, in what context and identify the types of data subjects and the likely impact on them.

1.1 What are the aims and purpose of the project?
Briefly explain what the intended purpose, outcome and benefits of the project are.

Live Facial Recognition (LFR) is a real-time deployment of facial recognition technology, which compares live camera feed(s) of faces against a pre-determined watchlist and generates an alert when a possible match is found. Whilst appropriate use of LFR technology delivers clear value to UK law enforcement and to the public it is important to recognise that the use of LFR involves biometric processing, a particularly sensitive form of personal data, and as such is considered to be an example of processing likely to result in high risk to both data subjects and organisations.

Concerns raised around the use of LFR by Police Forces often relate towards unnecessary intrusion into civil liberties and also in particular where instances of false-reporting (inaccuracy of LFR systems), along with the potential for wide-scale monitoring through the use of LFR, and the possibility of and risks associated with automated decision making as a result of LFR processing.

It is therefore critical that BTP ensures that it deploys LFR technology lawfully and responsibly for legitimate policing purposes, and in a transparent manner to help ensure that public trust and confidence is not eroded in the use of LFR.

To that end this DPIA assesses BTP's intended pilot of deploying LFR technology for a policing purpose, to ensure that use of LFR adheres to the confines of data protection and human rights laws, whilst considering the impact on individuals and their reasonable expectations of privacy.

LFR works by analysing key facial features to generate a biometric representation of them. This representation is then compared against known faces held within a watchlist in order to identify possible matches. Where the LFR application identifies a possible match, the LFR system flags an alert to a trained member of BTP personnel who in real time will decide whether any further action is required. Used in this way, the LFR application works to assist BTP personnel to make identifications rather than acting as an autonomous machine-based process devoid of any human input.

The following are illustrative examples where LFR may assist BTP with its policing purposes:

- Proactive Deployments (hotspot deployments)
- Specific Intelligence Deployment (we have been advised a certain person is going to be at X location)
- Protective Security Operations (protecting critical infrastructure)
- Supporting the location and arrest of people wanted for criminal offences.
- Preventing people who may cause harm from entering an area (for example, sexual harm prevention orders, criminal behaviour orders).
- Support the locating and apprehension of people about whom there is intelligence to suggest that they may pose a risk of harm to themselves or others (for example, stalkers, terrorists, sex offenders, etc.).We are considering adding a caveat to the watchlist that will allow for the inclusion of an unknown person (from a CCTV image) if there was intelligence to demonstrate the necessity due to high threat / high harm / live incident but the pilot scope will be for known offenders only.

- In addition to the above, missing persons will not be included in the pilot however as a future ambition the project intends to further consider inclusion of missing persons.
- Supporting the use of targeted preventative policing tactics in areas where intelligence suggests violent crime may be committed or there is otherwise a need to secure an area with a precise crime fighting tool to better deter those who may pose a threat from attending.

Processes

The technical operation of LFR deployment comprises of the following eight stages:

1. Compiling/using existing database of images: The LFR application requires a watchlist of reference images against which to compare facial images from the CCTV feed. For images to be used for LFR, they are processed so that the 'facial features' associated with their subjects are extracted and expressed as numerical values (a Biometric Template). BTP LFR policy outlines considerations relevant to lawfully compiling a watchlist including determining which persons may be on a watchlist and the sources of watchlist imagery. In order to ensure sufficient image quality, images will be custody images sourced from BTP's Niche system (or from the Police National Database in the event that BTP does not hold an image). Use of a non-custody image in exceptional circumstances must be authorised by the Gold Commander.
2. Facial image acquisition: A CCTV camera takes digital pictures of facial images in real time, capturing images as a person moves through the zone of recognition and using it as a live feed. The siting of the CCTV cameras, and therefore the LFR deployment location is important to the lawful use of LFR. The BTP LFR policy and procedure provide considerations relevant to the locations BTP may select to deploy the cameras when using them for LFR.
3. Face detection: Once a CCTV camera used in a live context captures footage, the LFR software detects individual human faces.
4. Feature extraction: Taking the detected face the software automatically extracts facial features from the image, creating the Biometric Template.
5. Face comparison: The LFR software compares the Biometric Template with those held on the watchlist.
6. Matching: When the facial features from two images are compared the LFR application generates a similarity score. This is a numerical value indicating the extent of similarity, with a higher score indicating greater points of similarity. A threshold value is set to determine when the LFR software will generate an alert to indicate that a possible match has occurred. Trained members of police personnel will review the alerts and make a decision as to whether any further action is required. In this way, the LFR application works to assist police personnel to make identifications rather than acting as an autonomous machine based process devoid of user input. The Threshold Value BTP will be utilising is 0.64, this is above the threshold recommended to minimise false positive matches and allow greater confidence in matches made. This is in line with the recommendations as laid out by the College of Policing (CoP) Authorised Professional Practice (APP) for facial recognition and the established best practice currently in use at existing pilot forces (The Metropolitan Police and South Wales Police).
7. Engagement Officer consideration of matched images: When an alert is generated it will be the sent to both Engagement Officers (via handheld devices) and LFR Operators (via the LFR laptop). The LFR operator is 'trained' and accredited with NEC algorithm training and will provide that initial human adjudication of the matched face. They will liaise with the

Engagement Officers (who are not trained on the system but will be fully briefed by operation commanders) who will approach / not approach the 'matched' person.

8. LFR data destruction: Where an alert is not generated, the biometric templates created in respect of members of the public whose images have been captured by LFR are immediately and automatically deleted. Where the LFR system generates an alert, the biometric template is deleted as soon as practicable and in any case within 24hrs except to the extent that:
   • personal data is retained in accordance with the Data Protection Act 2018, Management of Police Information (MOPI) and the Criminal Procedures and Investigations Act 1996;
   • personal data is retained in accordance with BTP's complaints / conduct investigation policies.

LFR Watchlists are deleted as soon as reasonably practicable and in any event at the end of a deployment and in any case within 24hrs following the deployment.

All CCTV footage generated from LFR Deployments is deleted within 31 days, except to the extent that the footage is retained:

- in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996;
- in accordance with the BTP's complaints / conduct investigation policies;

To support compliance, the LFR log is retained in accordance with MOPI. (*The LFR log is a contemporaneous record of the LFR deployment including details of operators undertaking the work, numbers of subjects on the watchlist and the alerts generated by the system for example).

Supplier:
BTP will have responsibility for creation of the watchlists, however as part of Op Overwatch, BTP are working with a third party supplier (Bedroq) to acquire LFR camera modules and make use of the supplier's "Neoface" technology.

NEC and Bedroq have joined together and provided one quote as Bedroq are a reseller of NEC hardware. NEC is the current leading supplier and is in use by the MPS.

1.2 Will personal data will be processed? Please indicate Yes or No.
☒ Yes
☐ No
If "No" then the remainder of this form does not need to be completed.

1.3 What categories of personal data will be processed?
For example, names, addresses, dates of birth, health data, criminal records, IP Addresses, email addresses etc

Data will be processed from images captured at LFR camera deployments. Biometric profiles will be created of unique facial characteristics of individuals passing through the zone of recognition. These biometric profiles will be held on the LFR system which will compare the biometric profile(s) against known faces on a watchlist and will issue an alert to the LFR operator in the event that a possible match is identified.

Any biometric profiles created that do not result in a match will be deleted immediately.

Personal data processed within LFR watchlists:

A watchlist will be prepared twenty-four hours prior to the deployment. The criteria for the watchlist is manually selected, and the watchlist will have been created via an optimising script that takes data directly from our Niche crime recording system. The watchlist will be drawn from data subjects who are known to BTP for offending on the rail network and provide a reasonable prospect of passing through the zone of recognition.

Each watchlist entry for an individual must include the following fields*:

- Watchlist name
- Gender
- First Name
- Middle Name
- Last Name
- Warning Markers
- Date of Birth (DOB)
- Alert Type
- Unique Reference No (URN)
- Reported Time
- Info (contextual information in relation to the “wanted” status)
- RMS ID (the URN reference in the Record Management System)
- PNC ID (Police National Computer) ID
- Operational Unit
- Class (Wanted warrant, wanted crime)
- Crime Type
- Owner
- Date Image
- Image

* For the LFR technology to work each entry that is uploaded onto the watchlist must have all of the above fields completed.

The type of offences that would invite inclusion on a BTP watchlist for LFR include:

- Category A Court Warrants (Serious Offences)
- Category B Court Warrants (Victim Based Crimes)
- Category C Court Warrants (Domestic Violence or Violence Against Women and Girls only)
- Category A offences (Serious Offences) – Wanted for Questioning
- Category B offences (Victim Based Crime) – Wanted for Questioning
- Category C offences (Domestic Violence or Violence Against Women and Girls only) – Wanted for Questioning
- Category A offences (Serious Offences) – Live Bail
- Category B offences (Victim Based Crime) – Live Bail

- Category C offences (Domestic Violence or Violence Against Women and Girls only – Live Bail
- Sexual Harm Prevention Orders/Sexual Risk Orders/Criminal Behaviour Orders/Serious Crime Prevention Orders
- First Instance Warrants Category A/B (C if DASH or VIAWG related)

1.4 Will any special category data or criminal offence data be processed?
Special category data is personal data that needs more protection because it is sensitive.
Please select all that apply

☒ Race
☒ Ethnic origin
☐ Political opinions
☐ Sex life
☐ Religion
☐ Philosophical beliefs
☐ Trade union membership
☐ Genetic Data
☒ Biometric Data
☐ Sexual orientation
☒ Physical or mental health (Not for the purposes of the pilot of LFR)
☒ Commission of criminal offences

1.5 What categories of data subjects will you be processing data about?
Please select all that apply.

☒ Members of public
☒ BTP officers
☒ BTP staff
☐ Victims of crime
☐ Witnesses
☒ Suspects
☒ Offenders
☒ Vulnerable adults (Not for the purposes of the pilot of LFR)
☒ Children
☐ Other (specify below)

BTP Officers and staff will be processed as part of Blue Watchlist training
In terms of members of the public passing through the zone of recognition this could include children.

1.6 Where will the personal data come from?
Describe how you will obtain the data – how will it be collected, is it already held by the Force, will it be taken from other systems?

The data will be sourced from Niche by BTP Force Intelligence Bureau (FIB) and is subject to a process defining the range of personal data to be extracted. All of the data is existing data held by BTP for a law enforcement purpose. For the purposes of the pilot we will use NICHE images and only utilise PND for when BTP don't hold a custody image. Additional checks to ensure the custody image held on PND is lawfully held will be implemented but where that confidence cannot be

gained, the nominal will not be added to the watchlist. Any consideration around the quality of the image will be assessed on a case-by-case basis by the Authorising Officer.

For the purposes of the pilot images taken from CCTV and Bodyworn devices will not be standardly utilised. Only in exceptional cases where there is a proven, serious risk to the safety of the public may a CCTV probe image will be used, but this would be subject to authorisation before the image is used.

The type of data to be used in the watchlist will be custody images held on our systems Niche. In each case the latest available custody image should be used. In exceptional circumstances where there is an imminent and credible threat to public safety, a CCTV image of an unidentified suspect may be included on the Live Facial Recognition (LFR) watchlist. This inclusion must be authorised by the Gold Commander for the LFR operation and supported by a documented assessment demonstrating that the use of the image is lawful, necessary, and proportionate to prevent serious harm. The decision must consider the expected level of privacy intrusion (rated on a scale of 1–5 as outlined in the Appendix) and include a clear justification of the imminence of the threat and why alternative measures are insufficient. The Appendix will be uploaded onto BTP's website and on our internal policy portal when published.

In the event of any inclusion around Missing Persons/Vulnerable persons, there may not be any custody images available – in which case BTP may need to consider whether HO Police Forces will have any relevant images. However for the time being it is deemed that BTP will not be conducting LFR on missing persons/vulnerable persons for the pilot of LFR, due to the fact that we are not confident that we will have a reliable source of images for those individuals – more assurance work will need to be conducted before this can be taken forward as a proposal. ***at commencement of the pilot in February 2026 we will not be including missing people on watchlists until further use can be explored though the DPIA and EIA***

1.7 How many individuals are likely to be affected?
Estimate the number of data subjects likely to have their data processed.

More than 5000 data subjects

1.8 Does this initiative involve the collection of new information about individuals?
Will the force be collecting new information that we haven't previously collected or had access to?

Yes

1.9 Does the project/initiative involve collating or linking together data that has not previously been linked in this way?

Yes

1.10 External access to data.
Does the project/initiative involve the disclosure of BTP data to an external party that we are not legally required to disclose data to, or the use of an external processor to process, use or store the data on our behalf. Please select all that apply.

- ☐ Data shared with external parties (except where we have a legal obligation to share)
- ☐ Transferring or storing data outside the UK, but within the EEA
- ☐ Transferring or storing data outside the EEA
- ☐ Use a third-party data processor (including cloud storage provider)
- ☐ Access to BTP systems by non-BTP employees

1.11 High risk processing

The following factors are considered by the Information Commissioner's Office to indicate processing likely to result in a high risk to data subjects. Select any that apply to this project/initiative.
☒ Use of new or innovative technologies (including AI) ☒ Profiling of individuals on a large scale ☐ Automated decision making about individuals ☒ Systematic monitoring of a public area on a large scale ☒ Large scale use of special category data or criminal offence data ☒ Use of biometric or genetic data ☐ Combining, comparing or matching data obtained from multiple sources ☒ Invisible processing – processing personal data that the data subject would not know we have ☐ Tracking an individual's geolocation or behaviour ☐ Targeting children or vulnerable individuals for marketing or automated decision making ☐ Risk to the health and safety of individuals in case of a data breach ☐ Evaluating or scoring an individual's performance, economic situation, health, interests or behaviour ☐ Preventing data subjects from exercising their rights (eg. right to access to their data, right to rectify or erase their data, right to object, etc)
1.12 Information Asset Owner Who has been identified as Asset Owner for the Information Asset?
C/Supt Chris Casey
1.13 Review, Retention and Disposal Outline below the arrangements that will be in place for review of data held and for ad hoc or scheduled weeding and deletion of records. Is there an existing retention schedule that applies – specify or link to this if so.
BTP must ensure that the processing of any data associated with LFR is conducted in a lawful way and in compliance with the BTP Live Facial Recognition (LFR) Policy. This means that: • Where the LFR system does not generate an alert that a person's biometric data is immediately deleted by the LFR software. • The LFR watchlist is deleted as soon as reasonably practicable, and in any case within 24 hours, following the conclusion of the deployment. Where the LFR system generates an alert, all related personal data is deleted as soon as practicable and in any case no longer than 24 hours post deployment, except to the extent that: Where the LFR system does not generate an alert, all related personal data is immediately destroyed. All CCTV footage data (non-biometric) generated from deployments will be retained as per below: • CCTV footage from the camera mast will be deleted every 31 days (automatically records over unless we require it for a complaint or separate criminal investigation (such as one of our officers being assaulted whilst on an LFR operation). Biometric data will be destroyed immediately or no later than 24 hours after deployment: • In accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996. • In accordance with BTP's complaints/conduct investigation policies. • In accordance with an approved programme of testing in order to provide for the continued evaluation of the LFR system using operationally realistic data in line with the ongoing

nature of the Public Sector Equality Duty – any requirement to retain the Closed Circuit Television (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.

To support compliance the LFR system has a full audit capability, and the LFR log is retained in accordance with MOPI.

Any processing of data for the purposes of a 'blue watchlist' will be retained. A'blue watchlist' is a watchlist that includes images of known persons and is used to test system performance. This relates to volunteers (e.g. BTP employees) taking part in the pilot to test the technology prior to a deployment being live.

Section 2: Lawfulness of Processing

In this section you will explain the lawful basis for the processing of the data and why it is necessary and proportionate to process it in this way.

2.1 Will the project/initiative be processing data for 'law enforcement purposes'?
'Law enforcement purposes' are the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including prevention of threats to public security. If BTP are processing for law enforcement purposes, we need to refer to Part 3 of the Data Protection Act 2018. If we are processing data for 'general' purposes, we need to refer to UK GDPR.

Both types of data

If you have selected law enforcement processing only, there is no need to answer 2.4 and 2.5. If you have selected general processing only, skip 2.2 and 2.3. If you have selected both, you will need to answer all the questions.

2.2 What is your lawful basis for processing (law enforcement)?
The possible options are set out at Section 35(2) of the Data Protection Act 2018.

Necessary for a law enforcement purpose

2.3 What is your lawful basis for any 'sensitive processing'? (law enforcement)?
If you have ticked any boxes at question 1.3, then this is considered sensitive processing and a further lawful basis must apply (and be strictly necessary), from Schedule 8 of the Data Protection Act 2018.

Administration of justice

2.4 What is your lawful basis for processing (general processing)?
The possible options are set out at Article 6 of UK GDPR.

Performance of a task in the public interest

2.5 What is your lawful basis for any processing of special category or criminal offence data? (general processing)
If you have ticked any boxes at question 1.3, then a further lawful basis must apply from Article 9 of UK GDPR (also in conjunction with Schedule 1 Part 2 of the Data Protection Act in some cases). Please consult the source legislation for the requirements for each condition.

Either select one condition from the following list:
Choose one answer
Or the processing must strictly necessary for reasons of substantial public interest, and one condition be selected from the following list:
Statutory Purposes

Administration of Justice
Protecting of Individuals Vital Interests
Safeguarding of children or adults at risk

2.6 Are there any other laws or codes of practice that apply to this processing?
If we are mandated or permitted by a specific law to process data in this way, please specify here. Please also cite any codes of practice, codes of conduct or national police policies that apply.

Link to Legal Mandate; https://www.btp.police.uk/police-forces/british-transport-police/areas/about-us/about-us/facial-recognition-technology/

Acts and policies relevant to the use of LFR and the creation of the watchlist are:

- Common law policing duties
- Police and Criminal Evidence Act 1984 Code D
- Public Sector Equality Duty 2011
- The Human Rights Act 1998
- The Protection of Freedoms Act 2012
- The Equality Act 2010
- Regulation of Investigatory Powers Act 2012 which forms part of the NPCC legal framework. Legal-framework-and-governance-Appendix-A.pdf

The College of Policing APP on Live Facial Recognition states in relation to the rights established in the European Convention on Human Rights articles that are incorporated into UK Law through the Human Rights Act 1998 and set out in Schedule 1 to that Act that the use of LFR by Police has the potential to raise considerations around the below human rights:

- Articles 2 (right to life) and 3 (prohibition of torture and inhuman or degrading treatment), in the context where an alert is generated by the LFR system and, if confirmed, the person located would pose a real and immediate threat to life. Similarly, this may arise for individuals sought in relation to offences where Article 3 is engaged. In this context, forces should be aware of the potential positive 'Osman' duties arising, and should therefore consider their capability and capacity to respond to such alerts in a timely fashion.
- Article 8 (Privacy) - see section 2.7 below.
- Article 9 (freedom of thought, conscience and religion), in the context of where an LFR deployment is located, as well as the clothing that people wear. In normal circumstances (other than when a section 60AA Criminal Justice and Public Order Act 1994 order is in place), the police do not have a legal power to require persons to remove clothing simply because they are passing the LFR system. Officers should make use of the National Decision Model (NDM) when considering requests to remove articles of clothing.
- Articles 10 (freedom of expression) and 11 (freedom of assembly and association), especially if there are plans to use LFR in policing an assembly or demonstration where there may be a risk to the public safety from persons who need to be identified. This requires very careful consideration, supported by force legal advice, to ensure that LFR is a necessary and proportionate policing tactic to maintain public safety while minimising impact on those who wish to lawfully express their views or peacefully assemble with others
- Article 14. This right requires that all of the rights and freedoms set out in the Human Rights Act 1998 must be protected and applied without discrimination. This is based on the principle that everyone, no matter who they are, should enjoy the same human rights and

have equal access to them. The protection against discrimination is not 'freestanding'. To rely on this right, you must show that discrimination has affected your enjoyment of one or more rights in the act. However, you do not need to prove that this other human right has actually been breached. The use of LFR will be relevant in circumstances where demographic performance of the LFR algorithm varied to such an extent that people of a particular demographic were more or less likely to see a false alert generated against them. As a result, there are two points to consider in relation to the LFR system:

- Does the LFR system's demographic differential performance vary by a particular demographic, such as it results in a person suffering a discriminatory effect?
- If there is a difference in treatment, is there an objective and reasonable justification?

A BTP Equality Impact Assessment (EIA) relating has been produced;
https://www.btp.police.uk/police-forces/british-transport-police/areas/about-us/about-us/facial-recognition-technology/

The College of Policing (CoP) Authorised Professional Practice (APP):
The CoP has produced APP guidance in relation to the use of LFR -
https://www.college.police.uk/app/live-facial-recognition/live-facial-recognition

2.7 Interference with the right to a private life

BTP is a Public Authority and therefore subject to the Human Rights Act, including respect for the right to a private life (Article 8). Article 8(2) states that "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

Explain below:

- Why is it necessary to use personal data to achieve the aim in this project/initiative? What less intrusive methods have been considered?
- Why is it proportionate to use personal data in the way envisaged?

Use of LFR technology is being considered in order to enhance BTP capabilities in locating known nominals offending on the UK rail network. It is being assessed as an addition to existing tactics that primarily rely on planned/targeted operations, along with real time officer intervention and the support of established CCTV systems.

LFR is not a PACE Code D defined method of identification and Engagement officers are fully briefed on the requirement to establish true identify through other legal means to minimize collateral intrusion.

Before authorising an LFR deployment, the Authorising Officer (AO) **must** consider whether it would be a proportionate means of achieving BTP's policing objectives, considering the impact of the deployment on the rights and freedoms of members of the public. The impact of a deployment on the rights and freedoms of members of the public will vary, depending on the characteristics of the deployment.

There should be robust consideration of any interference with the rights and freedoms of members of the public that would be created by the proposed deployment. In particular **Article 8 of the European Convention on Human Rights (ECHR) (right to a private and family life)** will be relevant in all cases, but to varying degrees. AOs should always assume that Article 8 is **always** relevant when:

1. Someone passes an LFR system
2. Someone is placed on a LFR watchlist for deployment
3. Where someone is engaged as a result of their being subject to an alert

Article 8 may more strongly apply if the proposed deployment is to an area where members of the public have greater expectations of privacy, for example, close to a clinic or a school. The circumstances at the deployment location may also affect the intensity with which these privacy rights are engaged. For example, a sporting facility may attract a greater expectation of privacy when it is being used as a private members' club than if it is used to host a major ticketed sporting event.

Any proposed use of LFR by BTP will need to be subject to an intelligence led case with the objective of:

- Identifying offenders who are unlawfully at large and are wanted by Police or the Courts.
- Identifying offenders subject to prevention or restrictive Orders in relation to sexual offending, criminal behaviour orders (not strictly relating to sexual offending) to identify any non-compliance.

Whilst we recognise the momentary collection of biometric data for those passing through the zone of recognition interferes with persons right to a private life this is balanced with the policing mission to protect persons from serious harm, bring offenders to justice and investigate serious offences. The use of LFR for BTP will be overt, in locations where expectations for privacy are already minimal being on CCTV rich station environments and the deletion of biometric data for those NOT on the watchlist immediately after collection demonstrates a proportional, legal and necessary policing tactic to protect the public.