South Wales Police / Gwent Police Operator Initiated Facial Recognition (OIFR) Legal Mandate

Summary: Outlines the legal basis for the South Wales Police / Gwent Police overt use of OIFR

Name of Force	South Wales Police (SWP) / Gwent Police (GWP)
Subject	Operator Initiated Facial Recognition (OIFR)
Summary	Outlines the legal basis for SWP/GWP's overt use of OIFR to identify persons on an Image Reference Database(s)
Author	Ch Insp Scott Lloyd

Project Name	Facial Recognition Technology
Senior Responsible Office-	ACC Mark Travis
Business Area/Department	Digital Services Division
Proposed implementation date	Immediately
Reference No. *(to be allocated by IM)*	

Change control:

Version	Date	Authority	Evidence of approval	Record of change
0.1	27.07.2021	Project Lead	Ch. Insp Scott Lloyd	Initial Draft
0.2	01.10.2021	Project Lead	Ch. Insp. Scott Lloyd	National Terminology
0.3	03.11.2021	FRT Board	Governance Review	No Amendments

0.4	25.01.2022	DSD Head	Ch Supt Simon Belcher	Pilot Sign off. No Amendments

Terms & Definitions: Capitalised terms used within this OIFR SOP shall have the meaning given to them in section 3 of OIFR Policy Document unless otherwise defined.

1 Introduction

1.1 OIFR for law enforcement purposes is not subject to dedicated primary legislation. OIFR is regulated by a number of sources of primary legislation as well as local policy. This 'tapestry' of legislation combine to provide a layered legal structure to use and regulate OIFR.

Tier one: Legislation	Legal Power to use OIFR	a) Common Law
	Regulating the use of OIFR	**Operational** b) Human Rights Act 1998 c) Equality Act 2010 **Data Management** d) Data Protection Act 2018/General Data Protection Regulation e) Protection of Freedoms Act 2012
	Requests for Information in relation to OIFR	f) Freedom of Information Act 2000 g) Data Protection Act 2018 (Subject Access Requests)
Tier Two: SWP/GWP OIFR Documents	Regulating the use of OIFR	a) SWP/GWP Policy Document b) SWP/GWP Standard Operating Procedures c) SWP/GWP Training Documents d) SWP/GWP Data Protection Appropriate Policy Documents e) SWP/GWP Data Protection Impact Assessment f) SWP/GWP Equality Impact Assessment g) SWP/GWP OIFR Legal Mandate

2 Common Law

2.1 The police have a number of long-established policing responsibilities and powers derived from common law which have been recognised by the courts. SWP is obliged to comply with common law and statutory safeguards in delivering its policing operational duties and relies on common law to discharge a number of its duties.

2.2 Key common law powers SWP/GWP may rely on when utilising OIFR include the policing common law powers to:

(a) protect life and property;

(b) preserve order and prevent threats to public security;

(c) prevent and detect crime;

(d) bring offenders to justice; and

(e) uphold national security.

Example: SWP/GWP has detailed uses of OIFR as a policing tactic for identifying those who are wanted for an outstanding warrant. In this context the use of OIFR to facilitate Operators to promptly identify those evading arrest would enable SWP/GWP to discharge its responsibilities to protect life and property. It would also be compatible with SWP/GWP's duty to bring offenders to justice by facilitating a prompt and effective investigation.

2.3 The use of SWP/GWP's common law power as a legal basis to support the use of facial recognition technology in the form of LFR has been considered and recognised by the courts in:

a) *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police [2019] EWHC 2341 (Admin)* (the "High Court Bridges" decision); *and*
b) R (on the application of Edward Bridges) v The Chief Constable of South Wales Police [2020] EWCA Civ 1058 (the "Court of Appeal Bridges" decision).

The Court of Appeal further summarised the legal basis in relation to compilation of Watchlists as being "both authorised under the Police and Criminal Evidence Act 1984 and within the powers of police at common law." The reference to the 1984 is a reference to imagery obtained pursuant to Section 64A (*Photographing of suspects etc.)* of the Act and particularly section 64A(4)(a) which allows a photograph taken under the section to be "used … for any purpose related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution or to the enforcement of a sentence". The Court of Appeal notes that "this was not an issue which we have to address in this appeal, since it is now common ground that SWP do have the power to deploy [LFR]."

3 Human Rights Act 1998

3.1 SWP/GWP use of OIFR will be in compliance with the Human Rights Act 1998. Use of OIFR engages the Human Rights Act 1998 and in particular has the potential to impact upon an individual's Article 8 rights, the right to respect for private and family life. This provides:

'There shall be no interference by a public authority with the exercise of the right except such as in accordance with the law and is necessary in a demographic 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.'

3.2 As a qualified right, any interference with an individual's Article 8 rights is only permissible if:

a) there is a **legal basis** for the interference with the qualified right that the public can understand;

b) the use of OIFR seeks to achieve the **legitimate aim**;

c) it is **necessary** for the purposes of that aim in a democratic society; and

d) the use of OIFR is **proportionate** to the legitimate aim being sought.

3.2.1 It is well-established that the reach of Article 8 can be broad. The case of *S v. United Kingdom1* confirms that this can relate to a person's right to their biometric data and any storing of data relating to it. Recognising that OIFR involves biometric processing, that case went on to recognise that, in protecting the personal data and other forms of biometric processing, the interests of the data subject and the community as a whole "may be outweighed by the legitimate interest in the prevention of crime".2

3.3 The High Court and Court of Appeal Bridges cases considered Article 8, specifically in the context of LFR technology and confirmed that Article 8 is engaged in so far as someone passes through the Zone of Recognition and in so far as someone is placed on a watchlist for a Deployment. Depending on the nature of the deployment, the Surveillance Camera Commissioner has identified that there are also potential impacts on other human rights. These include the right to freedom of assembly, freedom of thought, belief and religion, freedom of expression, freedom of association, and the protection of discrimination in respect of those rights and freedoms.

3.4 **There is a legal basis for the interference with the qualified right that the public can understand**

OIFR will be used to allow the SWP/GWP to discharge its well established operational duties pursuant to common law. The courts have recognised that "the rules need not be statutory, providing they operate within a framework of law and that there are effective means of enforcing them".[3]

In the case of *R (Catt) v Chief Police Officers [2015] A.C. 1065,* Lord Sumption recognised that applicants could have their personal information noted down and retained by the police as they occupied publically accessible space. The court recognised the police's common law powers to collect and store information are subject to an "intensive regime of statutory and administrative regulation" under the Data Protection Act and various guidance documents on the management of police information.

The courts have further recognised the right of the police to make use of a photograph of an individual. The courts accepted the purposes of preventing and detecting crime, the investigation of alleged offences and the apprehension of suspects or persons unlawfully at large. This was the case whether or not the photograph is of any person they seek to arrest or of a suspect's accomplice or of anyone else. The court confirmed the "key is that they must have these and only these purposes in mind and must … make no more than reasonable use of the picture in seeking to accomplish them".[4]

---

[1] *(2009) 48 EHRR 50, at [66 and 67]*
[2] *At [104]*
[3] R (*Catt) v Association of Chief Police Officers [2015] A.C. 1065* at [11].
[4] Per Laws J in *Hellewell v Chief Constable of Derbyshire [1995] 1 WLR 804 at 810F*

3.5 In the case of the SWP's use of LFR, the LFR Legal Framework outlines the legal basis for any interference with an individual's Article 8 rights. The High Court Bridges case confirmed the police's common law policing powers to be "amply sufficient" in relation to this type of use of LFR and confirmed that "the police do not need new express statutory powers for this purpose". This was further considered in the Court of Appeal Bridges case which also recognised the sufficiency of the legal framework, noting[5]:

> *"the legal framework which regulates the deployment of [SWP's use of LFR] does contain safeguards which enable the proportionality of the interference with Article 8 rights to be adequately examined."*

3.6 The Court of Appeal Bridges decision further noted that, to be 'in accordance with the law' the legal basis must:

> *"be 'accessible' to the person concerned, meaning that it must be published and comprehensible, and it must be possible to discover what its provisions are. The measure must be 'foreseeable' meaning that it must be possible for a person to foresee its consequences for them and it should not 'confer a discretion so broad that its scope is in practice dependant on the will of those who apply it, rather than on the law itself".*

3.7 In considering accessibility and foreseeability, the Court of Appeal considered the level of discretion that South Wales Police officers held in the case before it to determine *where* they deployed facial recognition technology and *who* they deployed it to locate those on an Image Reference Database. The court refers to this as the "Who Question" and the "Where Question".

a) The 'Who' Question: When considering how the 'Who Question' should be answered, the Court of Appeal made it clear that, the law does not seek specific confirmation as to who is on an Image Reference Database (they recognise the NCND principle6). The Court of Appeal recognised that individuals could be added to a watchlist on the basis that they are wanted on suspicion of an offence, wanted on warrant and vulnerable persons".

b) The Court of Appeal also explains why a category of those "other persons where intelligence is required" was not accessible and foreseeable to meet the 'in accordance with the law' test. They noted that the category was not readily understood, nor was it objective – it left "too broad a discretion vested in the individual police officer to decide who should go onto the watchlist" – essentially it allowed police officers to decide what 'other persons where intelligence is required' meant on a case-by-case basis rather than deciding if a subject met the criteria set out in the force policy.

c) Whilst it is recognised that there are distinct operational and legal differences between the deployment of LFR and OIFR, there is a need to address these points when utilising OIFR.

d) Following an approach recognised by the Court of Appeal[7], SWP/GWP addresses the 'Who Question' in its published SWP/GWP OIFR documents. SWP/GWP sets the

[5] *At [69].*
[6] *At [95].*
[7] *At [118].,*

criteria that applies to govern the images that may be included on an Image Reference Database and in what circumstances. It sets out the standard required for inclusion on an Image Reference Database, linking the necessity and criteria for the inclusion on an Image Reference Database with the policing need and the proportionality of taking any action.

e) The 'Where Question: The Court of Appeal noted that the South Wales Police team "was not able to draw to our attention anything which specifies where AFR Locate may be deployed". SWP/GWP OIFR documents answers this question. In answering this question, in many instances, the need to identify a person will determine where OIFR may be used.

With the benefit of the *Bridge's* decisions, the law has now been applied to the live use of facial recognition technology. The principles of these judicial decisions, taken together with the SWP/GWP's published documentation to support the use of OIFR and Legal Framework principles to be predictably applied to the use of OIFR in an accessible and understandable way. It allows the public subject to OIFR and those who may be placed on an Image Reference Database to understand the standards SWP/GWP operate to, including setting out the reason and grounds for OIFR use, details about where OIFR may be used, and the considerations and constraints relevant as to who may be placed on an Image Reference Database.

3.8 **The use of OIFR seeks to achieve a legitimate aim**

Article 8, recognises action in the interests of national security, public safety and the prevention of disorder and crime as legitimate aims. The use of OIFR in the context of assisting SWP/GWP identify offenders will help SWP/GWP achieve its law enforcement purposes.

3.9 **The use of OIFR is *necessary* for the purposes of that legitimate aim in a democratic society**

OIFR will be used in response to a pressing social need by helping SWP/GWP combat crime in areas where OIFR has the greatest potential to assist. It is a tool that helps SWP/GWP to discharge its operational responsibilities, primarily to help prevent and detect crime and protect the most vulnerable.

The following is an example of where OIFR may be used as a necessary tool to assist SWP/GWP in preventing crime and disorder. The examples are illustrative only and there will be other scenarios where the use of OIFR is justified.

Child sexual abuse: The use of OIFR will assist SWP/GWP in tackling child sexual abuse. OIFR could be used based on intelligence to find vulnerable individuals who are missing and believed to be at risk of child sexual abuse. Equally OIFR could be used at large crowded events known to be frequented by sexual predators in an attempt to identify and prevent similar attacks. Missing persons investigations use significant police resources where the need to locate is time critical. In such circumstances, it is of great importance to use all reasonable measures, to have the best chance of making a successful identification when the often scarce identification opportunities arise. At times, the police may also enlist the public

to help with locating missing people through the use of public appeals, by circulating a photograph of a vulnerable child across the media. This is a potentially much greater intrusion to the individual's privacy rights given the aim of the public appeal is for wide-scale awareness and that information goes outside of police control when it is placed in the public domain. Where it might be viable to use OIFR as a tool for identification instead, the intrusion on the individual's privacy rights can be lower, yet it still offers SWP/GWP a route to discharge its common law responsibilities to protect life.

Additionally, in a climate where police forces need to operate efficiently, SWP/GWP has also identified that technology such as OIFR can assist with the challenges of quickly and cost efficiently identifying those with outstanding warrants or who have otherwise breached their bail conditions. It is right and appropriate to bring those who are unlawfully at large to justice noting the need to protect the public in such circumstances.

3.10 **The use of OIFR is proportionate to legitimate aim being sought**

Whilst it is recognised that use of OIFR would not fall under the definition of a 'surveillance camera', SWP/GWP are committed to adhering to the identified principles. The benefits of using OIFR for an investigation or operation should not be disproportionate or arbitrary. In this respect the Surveillance Camera Commissioner recognises that:

"used appropriately, current and future technology can and will provide a proportionate and effective solution where surveillance is in pursuit of a legitimate aim and meets a pressing need".

An objective for the use of OIFR is to identify individuals who are of interest to the SWP/GWP and to utilise OIFR with a view to apprehending them, reducing the prevalence of crime within the relevant area.

a) *Consideration should be gives as to the extent of any proposed interference with privacy against what is sought to be achieved and if there are other viable methods to achieve the aim which involve a lower level of interference.*

The use of OIFR should be considered against other methods of identifying persons of interest to SWP/GWP and/or UK Law Enforcement. Consideration should be given as to the effectiveness and intrusiveness of other viable methods that could give the same result, with the least intrusive, viable method being adopted to progress an investigation.

Example: The use of OIFR to confirm or eliminate a person's identity may be less intrusive to arresting the individual in order to later confirm their identity at a police station using fingerprints or DNA.

Proportionality controls. Controls are also designed in to OIFR and its operation to help minimise any impact on the public and those places on an Image Reference Database as follows:

I. OIFR cannot be used to identify persons unless they have been included on an Image Reference Database.

II. Candidate images on an Image Reference Database will be lawfully held by SWP/GWP with all reasonable steps being taken to ensure that the image is of a person intended for inclusion on a given Image Reference Database.
III. On adding an image to the Image Reference Database the FRT system will assess the image for quality and suitability for matching in order to allow SWP/GWP personnel to consider and manage the risk of poor quality images generating inaccurate OIFR returns.
IV. All Image Reference Databases are balanced by design with the source databases via the comparison of image hash values.
V. The camera used in OIFR is of sufficient quality for the FRT system's needs.
VI. OIFR and FRT system is 'closed' and not directly connected to other SWP/GWP systems or the internet.
VII. OIFR is designed to assist SWP/GWP personnel identify people. OIFR will always identify six possible matches to the Operator for a decision on any further action rather than autonomously taking a decision on any action after making a possible match.
VIII. OIFR and the materials that support OIFR use will be subject to review post OIFR pilot to ensure that OIFR and its operation remains necessary, proportionate and effective in terms of meeting its use case.

Controls have also been implemented with regards to personal data retention to minimise the impact on the wider public and those on the Image Reference Database. The controls provide that:

1. a person that is subject to a OIFR their image and biometric data is immediately automatically deleted.

OIFR use location privacy considerations. OIFR use will be identified as being necessary by the information and intelligence when considering the reason and grounds for use and the case supporting the prospects of identifying a person. However, the Operator must also consider the reasonable expectations of privacy the general public may have when in a public and private place. Some places, and the people expected to be at some places by their nature attract greater privacy expectations than others.

Example: Areas particularly focused on providing facilities or attractions aimed at children would typically attract greater privacy expectations over an area that typically sees attendance from the public more broadly. There may nevertheless be instances where the information and intelligence case, and the need to protect children makes it necessary and proportionate to use OIFR in these areas. For example if it is known that wanted sex offenders are targeting those that visit the location and it not possible to identify them by less intrusive policing tactics. If it is necessary to use OIFR at the location, mitigations to reduce the privacy impact should be used wherever possible. Such as taking extra care to ensure no third party is captured in the probe image.

3.11 Wider Human Rights Act considerations

The right to privacy is a value which protects the autonomy and human dignity of individuals by enabling them to conduct their lives in a way of their choosing. There are therefore circumstances when freedom of thought, conscience and religion (Article 9), freedom of expression (Article 10) and freedom of assembly and of association (Article 11) may be particularly relevant.

a) *Article 9.* The clothing people wear can be an act of thought, conscience and religion and in normal circumstances, the police do not have the legal power to require a person to remove clothing (including any headdress) simply because they are subject to OIFR. Additionally, the location where people may by subject to OIFR may also engage Article 9.

b) *Article 10 and 11* have particular relevance when considering both the policing of assemblies and demonstrations and any use of OIFR which may impact on an assembly or demonstration. Article 10 is especially pertinent should people have reservations about expressing themselves as a result of OIFR use. Article 11 is also relevant should the use of OIFR deter people from attending an assembly or demonstration at all or otherwise cause people to minimise their involvement.

Example: The use of OIFR can assist SWP in policing an assembly or demonstration, particularly where there is an intelligence case supporting there being a risk to public safety. Specifically, OIFR can support Operators by efficiently identifying suspects for violence in crowded locations where it might otherwise be difficult to identify them. In deciding the use of OIFR is necessary and proportionate, regard should be had to an individual's Article 10 and 11 rights – noting there may be expectations of anonymity in a crowd and that individuals may choose to alter their means of demonstration as a result of OIFR use. Article 10 and 11 rights must be weighed against the need to use OIFR to enable an assembly that might otherwise be disrupted by the risk to public safety. In making this decision, consideration should be given to factors which could minimise the impact of OIFR use. These include ensuring the public understand the use of OIFR is to help them safety undertake their assembly.

c) Operational Duties

The 'operational duty' was first outlined in the case of *Osman v United Kingdom*[8] and concerned an alleged failure to prevent the young victim and his family from the risk to life posed by a stalker. The European Court of Human Rights in *Osman* found that the police were under a positive duty to take reasonable measures to avert a real and immediate risk to the life of an identified individual or individuals of which the police were, or ought to have been aware. Caselaw also supports that the police are under an Osman style duty to investigate serious allegations in a timely and efficient manner in order to uphold an individual's Article 3 rights.

The Osman operational duty has particular relevance to OIFR in two contexts (i) being used to identify those posing a threat to the public or themselves where a real and

[8] [1999] 1 F.L.R. 193 (ECtHR)

immediate risk to life is identified and OIFR is thought to provide an appropriate response to such risk and (ii) on the return of the six possible matches the need to engage the Osman operational duty with measures being put in place should a person being matched seek to evade officers.

4 Equality Act 2010

4.1 The Equality Act 2010 provides a legal framework to protect the rights of individuals and advance equality of opportunity for all. The Equality Act 2010 prohibits discrimination based on different treatment on the basis of a protected characteristic. The prohibition of discrimination applies to both direct and indirect discrimination. As a public authority, SWP/GWP must comply with section 149 of the Equality Act 2010 which is most commonly known as the Public Sector Equality Duty ("PSED").

4.2 SWP/GWP is required to take measures to ensure that the use of OIFR complies with the Equality Act 2010. Particular attention is needed in two respects: (a) the technical performance of OIFR and FRT system (and then, if performance varies by any particular demographic), and (b) the operational use of OIFR and FRT system:

a) The technical performance of OIFR and FRT system.

The Court of Appeal Bridges decision makes it clear that the PSED requires SWP/GWP to take reasonable steps to satisfy itself, either directly or by way of independent verification, that the algorithm in this case does not have an unacceptable bias on grounds of race or sex. To assist the public with understanding how SWP/GWP meets its PSED duties, SWP/GWP has published the SWP/GWP OIFR Equality Impact Assessment. This includes:

1. **Independent evaluation:** A number of studies highlight the varying performance of facial recognition algorithms and the potential for the performance of algorithms vary dependant on demographic factors. As a result SWP/GWP has paid regard to the evaluations undertaken by the National Institute of Standards and Technology (NIST) who have evaluated circa 200 facial recognition algorithms for statistical accuracy and demographic performance, including those submitted by NEC – the provider used by SWP/GWP.

2. **Ongoing assurance:** SWP/GWP OIFR documents provide for ongoing evaluation and a post-deployment review process. This reflects the ongoing nature of the PSED duty and also offers SWP/GWP a chance to monitor for technical issues by reviewing all possible matches and monitoring for trends. Should a concern be identified, SWP/GWP would then be in a position to explore that further and test for issues under the oversight and scrutiny of the SWP Facial Recognition Technology and Biometrics Programme Board.

3. **Independent academic evaluation:** SWP have commissioned an independent evaluation of all aspects of Facial Recognition Technology to include OIFR. The evaluation will be conducted by independent academics and will focus of equitability particular to ethnicity, age and gender. The study is to commence in

Q3 of 2021 with ongoing reviews during the life of the study being considered under the oversight and scrutiny of the SWP Facial Recognition Technology and Biometrics Programme Board.

b) The operational Deployment of OIFR and FRT system.

SWP/GWP OIFR documents are also responsive to the Subject, System and Environmental Factors to ensure OIFR is suitable for its intended use and operating correctly. Subject, System and Environmental Factors including aspects such as camera configuration, lighting conditions, the distance at which people will be from OIFR Device camera and points relating to an individual's age and appearance have been considered carefully in SWP/GWP OIFR documents to ensure the efficacy of OIFR and FRT system and the SWP/GWP's compliance with its Equality Act 2010 duties.

By way of example, SWP/GWP OIFR documents provide that OIFR users are trained to identify issues with probe images which may impact on system performance. Where the need to use an image is deemed to be necessary and proportionate, those using OIFR have received training to maximise OIFR performance and to effectively consider any issues arising from the use of such images as part of the identification process.

As a result of having taken reasonable steps to understand the statistical accuracy and equitability performance of the SWP/GWP OIFR and then in light of points relating to Subject, System and Environmental Factors, SWP/GWP has adopted a 'fail-safe' position to ensure that absent there being other lawful grounds to take policing action:

> **no automated decision making will occur with the Operator reviewing OIFR possible matches, thus reaching their own opinion that there is a match between the Subject and the Candidate image.**

This means OIFR is not making any automated decision to match the images, the Operator is making this decision - just as officers make similar decisions to engage with members of the public every day (without the support of OIFR). The Operator is best placed to make this decision, drawing on their training and policing experience.

Similarly the Operator is best placed to consider the impact of any Subject, System and Environmental Factors which may have influenced OIFR when it generates the six possible matches and if such factors combine to assist with further engagement with a member of the public.

Beyond Subject, System and Environmental factors, SWP/GWP personnel are also familiar with managing the PSED requirement whilst undertaking policing activities from a number of other crime fighting techniques, for example, 'stop and search'. In this respect, it is important

that the use of OIFR is driven from the need to meet a legitimate aim, such as the prevention of crime and disorder. The Equality Impact Assessment informs the
plan to support the use of OIFR to mean SWP/GWP upholds the Public Sector Equality Duty. Compliance with the Equality Impact Assessment will then be monitored and reviewed for the duration of the OIFR pilot.

5 Data Protection Act 2018

5.1 SWP/GWP processes personal data for OIFR 'based on law'; specifically its legal powers identified in relation to the common law as well as human rights and equality considerations as outlined in this Legal Mandate, and the policies put in place by SWP/GWP OIFR documents. The Appropriate Policy Document and other SWP/GWP OIFR documents published by SWP/GWP as a public bodies allow the public, to include those subject to OIFR and those who may be placed on an Image Reference Database to understand the standards SWP/GWP operates to, including setting out the reason and grounds to use OIFR, details about where OIFR may be used, and the considerations and constraints relevant as to who may be placed on an Image Reference Database.

5.2 For the purposes of preventing crime and disorder, Part 3, Data Protection Act 2018 (DPA) regulates the processing of personal data, including sensitive processing, whether processed on a computer, CCTV, still images or other media. Any recorded image from a device which can identify a particular person is 'personal data'. The DPA therefore applies to the processing of data for OIFR both in terms of identifying those on an Image Reference Database but also in terms of processing biometric information of members of the public to confirm they are not on an Image Reference Database. These actions are covered by the processing of data for law enforcement purposes, as defined in s.31 DPA:

"For the purposes of this Part, "the law enforcement purposes" are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."

a) Strictly necessary in this context means that the processing has to relate to a pressing social need, and it is not reasonably viable to address this through less intrusive means. Any personal data collected via OIFR is not used in a manner that is contrary to the identified law enforcement purpose.

b) The 'strictly necessary' standard may be informed by the Operator considering factors including:

1. what other policing methods have been used / discounted when seeking to identify an individual(s) on the Image Reference Database or to provide a series of tailored security measures;

2. the importance of achieving the law enforcement purpose and the prospects of achieving the law enforcement purpose through the use of OIFR at the proposed location with the proposed Image Reference Database (for example, the use is always intelligence-led or otherwise

supported by information which confirms that OIFR can be expected to get results in the circumstances being contemplated);

3. the size and scale of the planned OIFR use and associated Image Reference Database and the level of sensitive processing anticipated as a result of OIFR use; *and*

4. if the law enforcement purpose which underpins the use of OIFR is strictly necessary and proportionate to the need to undertake sensitive processing and the risk to individuals' rights this entails (subject to the protections and safeguards implemented).

Important note to Operators: Operators need to be satisfied that the processing satisfies one of the Schedule 8 conditions or Article 9 conditions as set out below and complies with the six data protection principles.

5.3 Schedule 8 conditions of the DPA are engaged:

- necessary for judicial and statutory purposes – for reasons of substantial public interest;
- necessary for the administration of justice;
- necessary to protect the vital interests of the data subject or another individual;
- necessary for the safeguarding of children and of individuals at risk; **and**
- necessary for the purpose of preventing fraud.

Example: The use of OIFR will assist SWP/GWP in fighting knife crime in support of its common law policing powers. OIFR could be used to identify wanted offenders who have failed to comply with court bail relating to such offences. Used in this way, OIFR would assist in the prevention, investigation, detection or prosecution of criminal offences.

OIFR offers advantages over other potential policing methods such as a police officer using a picture or a physical description where positive results would otherwise be less likely and the risk of people not being identified. Given the importance of tackling serious and violent crime, a clear law enforcement purpose can be identified. In this context OIFR use may be seen as strictly necessary to support the investigation of knife crime, to enable the SWP/GWP to effectively respond to a pressing social need.

Similarly, the Schedule 8 condition of being necessary for statutory purposes for reasons of substantial public interest can be seen in this context to include a police officer working for the prevention, investigation, detection or prosecution of offences to keep the public safe.

5.4 SWP/GWP has also undertaken a number of steps in accordance with the Data Protection Impact Assessment (DPIA) to manage and mitigate the impact of any personal data processing using OIFR. Particular actions are set out in the remainder of this section.

5.5 *Data Protection Impact Assessment:*

A DPIA has been conducted to support the use of OIFR in order to identify and minimise the data protection risks. Whilst the overall DPIA will be reviewed annually, the governance provided by the Facial Recognition Technology and Biometrics Board will ensure consideration should to be given to:

a. if the risks and controls remain current and sufficient for the planned use of OIFR; and
b. if the planned use for OIFR poses any other risks which are capable of mitigation beyond those identified in the DPIA.

5.6 *Data Protection by Design*:

A number of data protection controls have been designed into OIFR in order to mitigate processing impacts on privacy and to comply with the general obligation in Part 3 of the DPA to implement appropriate technical and organisational measures having considered and integrated the principle of data protection into OIFR processing activities. The designed-in measures identified include measures to:

a. limit the amount of personal data collected;
b. limit the extent of personal data processing;
c. limit the period of personal data storage.

Additionally, SWP/GWP has acted to ensure that OIFR performs to a level where the statistical accuracy of the data being processed and fairness 'by design' is ingrained into SWP/GWP's OIFR. SWP/GWP OIFR documents and other published supporting information explain how SWP/GWP is assured that its OIFR operates with a high degree of statistical accuracy and in a way that does not lead to unjust results between demographics.

OIFR also includes a number of physical and technical security measures including:

a. OIFR and FRT system is a fully closed system with two layers of password protection to access the application.
b. Role based access controls with limited user permissions are implemented on the FRT system;
c. Data is sent between the OIFR Device and FRT system via a secure Virtual Private Network (VPN).
d. A full audit is maintained of all user initiated actions undertaken during the course OIFR use; *and*
e. Technical issues with OIFR are always dealt with by member of the technical staff who support the use of OIFR and FRT system.

5.7 Appropriate Policy Document:

Section 42 of the DPA and Article 30 General Data Protection Regulation requires that, at the time that the processing is carried out, the controller has an appropriate policy document in place. SWP/GWP has produced these documents and published them. This document allows the public to understand details of the:

a. the data being processed by OIFR, how often it is processed and whose data is processed;
b. procedures, safeguards and accountability principles for complying with the data protection principles when relying on a condition from Schedule 8 to process biometric personal data both for those on the Image Reference Database and those subject to a OIFR enquiry;
c. procedures, safeguards and accountability principles for complying with the data protection principles when relying on a condition from Article 9 of the GDPR and Part 2 and Schedule 1 of the DPA to process special category data both for those on an Image Reference Database and those subject to OIFR;
d. SWP/GWP policy for the retention and erasure of personal data for OIFR processing.

5.8 Data Protection Officer:

SWP/GWP has appointed a Data Protection Officer (DPO) in compliance with Part 3 DPA who has been consulted in relation to OIFR. The DPO is available to inform and advise the Chief Constable (as data controller) and SWP/GWP personnel about their obligations in relation to the DPA. The DPO also provides an internal function to monitor compliance with the DPA and is an active member of the Facial Recognition Technology and Biometrics Board.

6 General Data Protection Regulation

6.1 As part of SWP/GWP' common law powers to protect and preserve life and property, we process special category data in accordance with the requirements of Article 9 of the GDPR (which is incorporated into UK law under and supplemented by Part 2 and Schedule 1 of the DPA).

6.2 The Schedule 1 DPA conditions for processing special category data require SWP/GWP to have an APD in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 GDPR (relating to processing of personal data) and policies regarding the retention and erasure of such personal data.

6.3 Article 9 conditions of GDPR are engaged:

- explicit consent;
- substantial public interest; and
- historical research or statistical purposed.

Section 10 DPA supplements Article 9 GDPR, requiring the following conditions of Schedule 1 to be satisfied where SWP/GWP relies on Article 9(2)(g) substantial public interest.

6.4 Schedule 1 DPA are engaged:

- research;

- statutory etc and research government purposes; and
- safeguarding of children or individuals of risk

Example: An academic evaluation of OIFR is to be conducted with regards equitability. The sharing of data will be subject to a Service Level Agreement. Any sharing of data will be time limited via a web-based sharing platform rather than data transfer. The platform will be accessed by academic partners via a secure log on for a time limited period. The scientific research purpose is relied upon here. Where possible anonymised or pseudonymised data is used. Where members of police staff consent to the use of their images for testing or evaluation of performance of the system this is collected in accordance with recognised research ethics standards. (To note – consent collected for research does not refer to the data protection definition of consent).

7 Protection of Freedoms Act 2012

The Protection of Freedoms Act 2012 (PoFA) has seen the introduction of a new surveillance camera code issues by the Secretary of State (the Code) and the appointment of a Surveillance Camera Commissioner. SWP/GWP will have regard to the Code for the use of OIFR. This includes regard to the 12 guiding principles that system operators should adopt. The Code makes a number of specific points in relation to automated recognition technologies which SWP/GWP have regard to as follows:

Code	SWP/GWP approach
Fair processing information to data subjects	SWP/GWP processing information publically available to data subjects. It makes information relating to OIFR and data processing available via its website.
Appropriate retention and disposal systems	The necessary systems are addressed SWP/GWP OIFR documents.
Suitable technological and physical security measures	These measures have been addressed by design and are also covered in SWP/GWP OIFR documents.
Cameras of sufficient quality to meet the intended purpose	This requirement is addressed by the design of OIFR and FRT system.
Monitored by trained individuals	OIFR will always return six possible matches to a trained member of SWP/GWP personnel for a decision on any further action. In this way, OIFR works to assist SWP/GWP personnel to make identifications rather than acting as an autonomous machine-based process devoid of user input.

8 Freedom of Information Act 2000

The Freedom of Information Act 2000 (FOIA) provides public access to information held by public authorities. It does this in two ways:

8.1.1 public authorities are obliged to publish certain information about their activities;

8.1.2 members of the public are entitled to request information from public authorities.

In recognition of its FOIA duties, SWP/GWP makes significant OIFR information available via its website. This includes summary information relating to OIFR including the Image Reference Database size, OIFR trial dates, OIFR use to include arrests and disposal. SWP/GWP will also be responsive to FOIA requests.