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) / Heddlu Gwent Police (GWP)
Subject	Operator Initiated Facial Recognition (OIFR)
Summary	Outline of the legal basis for SWP/GWP's overt use of OIFR to use biometric templates of individuals to match against an Image Reference Database(s) for the purpose of uniquely identifying an individual
Author	

Project Name	Facial Recognition Technology
Senior Responsible Officer	ACC Trudi Meyrick
Business Area/Department	Digital Services Division
Proposed implementation date	14.12.2024

Change control:

Version	Date	Authority	Evidence of approval	Record of change
1	11.12.2024			New document

Contents

1 Introduction

Police use of OIFR is subject to common law and a framework of primary legislation. Compliance with this framework is further demonstrated in force documentation which provides data protection compliance, operational instructions and assurances around security, equality and oversight.

Tier one: Legislation	**Legal Power to use OIFR**	a) Common Law
	Regulating the use of OIFR	b) Human Rights Act 1998 c) Equality Act 2010 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

The core duty of the police service is to protect the public by detecting and preventing crime. This duty is established in common law (precedents set by decisions of the courts) and the police have both common law and legislative powers to execute it.

The use of police powers must be compatible with human rights and equalities legislation. Police personnel are individually responsible for ensuring their use of their powers is lawful, proportionate and necessary.

Police powers can be grouped into three categories:

1. Powers to investigate crime. This includes a range of powers to collect evidence needed to identify suspects and support their fair and effective trial.

2. Powers to prevent crime. This includes a range of powers to maintain public order, prevent anti-social behaviour and manage known offenders/ suspects.

3. Powers to 'dispose' of criminal cases. These powers allow police officers to dispose of criminal cases outside of court or charge suspects so they can be prosecuted.

Key common law powers SWP/GWP may rely on when utilising OIFR include the policing purpose 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 1: Outstanding Warrants

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.

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 facial recognition technology 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."

Whilst SWP/ GWP recognise that the case considered the use of LFR specifically, the fact that it was held by the Courts that the use of Facial recognition in policing was lawful needs to be considered more broadly. The policing purposes engaged for the purposes of using OIFR are similar to those of LFR, with the key difference being the means by which the technology is deployed.

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]."

2 Human Rights Act 1998

SWP/GWP acknowledge that a subject's Human Rights are engaged when OIFR is used or when they are included in the Image Reference Database. In particular there is likely to be an impact on Article 8 Right to respect for private and family life:

'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.'

The 4-part test in *Bank Mellat v HM Treasury (No2)[2014] AC700* determines whether an interference with Article 8 is proportionate:

Question	SWP/GWP response
Whether the objective of the measure pursued is sufficiently important to justify the limitation of a fundamental right	The objective is to identify an individual who has refused or is unable to identify themselves on request, who is suspected of committed or be in the process of committing a criminal offence or is unlawfully at large/ wanted on warrant or recall to prison with further police action required; is subject of bail conditions, court order or other restriction that would be breached if they were at the location at the time is a missing person deemed increased risk; is an immediate threat to life or immediate risk of serious harm, or; is deceased or it has been confirmed that they are deceased. Based on these grounds it is sufficiently important to justify limitation of a fundamental right.
Whether it is rationally connected to the objective	It is imperative for an officer to be able to respond proportionately and promptly, with information to support informed risk assessment and decision making, the outcomes being to apprehend the subject and protect the wider public safety or take appropriate actions to safeguard individuals at risk. Informed decision-making serves to support Operators in justifying intrusive tactical options

	such as arrest or to negate the necessity to arrest by providing information to the Operator at the point of interaction to support alternative, less intrusive outcomes. Therefore, the outcome must be that it is rationally connected to the objective
Whether a less intrusive measure could have been used without unacceptably compromising the objective	Less intrusive measures are employed as a matter of course i.e. traditional methods of requesting details from the individual under existing police powers. OIFR is intended to be utilised where reasonable less intrusive enquiries have been exhausted and it is necessary to identify the individual for a policing purpose. Where a policing purpose exists, OIFR enables the officer to identify the individual who has refused or is unable to identify themselves in response to a request at the scene, rather than detain the individual in front of others and at their inconvenience. Where there is no match between the biometric template and the Image Reference Database no record of the image of the Subject is retained, with the OIFR app automatically deleting the image with no means of recovery.
Whether, having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community.	Based on the information above and technical/organisational controls and measures detailed further in this document, there is a fair balance between the rights of the individual and the wider interests of the community. The processing will facilitate police actions which, if done via traditional measures will require more physical intrusion for the individual by way of possible detention, in detail and visible processing of more records and personal information to try to identify and match the subject manually whilst raising the potential risk of harm to the public or to the subject as a result of delays in accessing the relevant information in a timely manner.

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.

Example 2: 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.
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 3: Alternatives

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.

Privacy and security by design

Privacy and security by design are built into the OIFR process to minimise any impact on the public and those on an Image Reference Database, including:

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 i.e. where a person is subject to OIFR their image and biometric data is automatically deleted immediately following the matching process.

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 3: Privacy in certain locations

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.

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.

Article 9 – Right to freedom of thought, conscience and region

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.

Article 10 – Right to Freedom of Expression and Article 11 – Right to Freedom of Assembly and Association

Both have some relevance when considering the policing of assemblies and demonstrations and any use of OIFR which may impact on an assembly or demonstration. It should however be noted that OIFR is not intended to be deployed in densely populated circumstances as it is not designed to capture many images on a large scale. Article 10 may be relevant should people have reservations about expressing themselves as a result of OIFR use. Article 11 may also be 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 5: Assembly & demonstrations

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.

Article 2 – Right to Life

The first sentence of Article 2 states that public bodies must refrain from the intentional and unlawful taking of life, but also to take appropriate steps to safeguard the lives of

those within its jurisdiction. This obligation extends beyond its primary duty to secure the right to life by putting in place effective criminal-law provisions to deter the commission of offences against the person backed up by law-enforcement machinery for the prevention, suppression and sanctioning of breaches of such provisions. It is accepted that Article 2 may also imply, in certain well-defined circumstances, a positive obligation on the authorities to take preventive operational measures to protect an individual whose life is at risk from the criminal acts of another individual.

This 'operational duty' was first outlined in the case of *Osman v United Kingdom*[1] 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 (Prohibition of torture as well as inhuman or degrading treatment or punishment. This right is absolute and public authorities must not inflict such treatment nor allow others to do so).

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 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.

3 Equality Act 2010

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").

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 the FRT system (and then, if performance varies by any particular demographic), and (b) the operational use of OIFR and the 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] [1999] 1 F.L.R. 193 (ECtHR)

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:** Independent academic evaluation of Facial recognition technology has been undertaken by the National Physical Laboratory. This testing was undertaken in late 2022 with the results being published in 2023. The results are available at:

   Operational Testing of Facial Recognition Technology

   A summary of the findings of this testing, with specific reference to OIFR, showed that OIFR had 100% true positive identification rate, meaning that whenever OIFR was tested, it returned the correct Candidate Image at position 1. In the testing, there was no identifiable evidence of bias towards any of the demographics tested. A recommendation of the testing was to implement a Threshold Setting of 0.66 in order to prevent any high scoring non-mated comparisons being returned in the results for review by the Operator. SWP/ GWP have acted upon this guidance and implemented this Threshold Setting.

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 ("human in the loop") - 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 up to 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.

4 Data Protection Act 2018

The Data Protection Act 2018 provides principles on how personal information is used by organisations, businesses or the government. The policing purpose may fall under either Part 2 General Processing and Part 3 Law Enforcement Purposes.

Under both parts of the Act, biometric data processed for the purpose of uniquely identifying an individual is categorised as special category data/sensitive processing. This applies to the biometric templates being processed using OIFR of both the subject and the images on the Image Reference Database irrespective of whether there is any match.

Part 3 Law Enforcement Purposes

Law enforcement purposes are defined under s35(1) of the Act:

> "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."

Where sensitive processing takes place there is a requirement that it is strictly necessary for the exercise of the functions of a competent authority (an example of a competent authority is a police force).

'Strictly necessary' imposes a more exacting standard than 'necessary', and in practice calls for a more rigorous justification for processing the information. In this context use of OIFR has to relate to a pressing social need, and it is not reasonably viable to achieve the aim via less intrusive means.

The 'strictly necessary' standard will be informed by the Operator considering factors including:

1. 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 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).
4. the level of sensitive processing anticipated as a result of OIFR use; and
5. 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).

Where sensitive processing is taking place controllers must also satisfy additional conditions set out in Schedule 8 of the Act. The applicable conditions in relation to OIFR are:

Schedule 8 (1) Statutory etc purposes

Schedule 8 (2) Administration of Justice

Schedule 8 (3) Protecting individuals' vital interests

Schedule 8 (4) Safeguarding of children and individuals at risk

An Appropriate Policy Document is in place for sensitive processing under Part 3 in accordance with Schedule 1 Part 4.

Example 6: **Wanted Offenders**

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 etc is deemed to include a police officer working for the prevention, investigation, detection or prosecution of offences to keep the public safe under common law powers.

Part 2 General Processing

General processing under Part 2 of the Act is provided for in the UK General Data Protection Regulation. Special category data must meet a lawful condition under Article 6 and Article 9.

Article 6(1) (c) Processing is necessary to protect the vital interests of the data subject or another natural person

Article 6(1) (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

Article 9(2) (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

Article 9(2) (g) processing is necessary for reasons of substantial public interest

DPA Schedule 1 conditions for processing special category data and processing in the substantial public interests are:

Part 2 Substantial Public Interest Conditions

Para 5 Requirement for an appropriate Policy Document

Para 6 Statutory etc, and government purposes

Para 7 Administration of Justice

Para 10 Preventing or detecting unlawful acts

Para 18 Safeguarding of children and of individuals at risk

An Appropriate Policy Document is in place for processing data for OIFR under schedule 1 Part 2 of the Act.

Example 7:
The use of OIFR will support SWP/ GWP in identifying and safeguarding missing persons deemed increased risk.
Police do not obtain images of all missing persons however where there is suspicion that the person might be at increased risk of immediate threat to life or immediate risk of serious harm, an image of the missing person may be provided to Police for the purposes of supporting lawful enquiries to locate that person.
Police can use OIFR where they have reason to suspect that the person they are engaging with may be a missing person deemed increased risk. Where Operators suspect this individual might be at immediate risk to life or immediate risk of serious harm, there is a positive obligation on Police to ensure that all reasonable opportunities to preserve life and limb are explored.

OIFR presents an opportunity to identify the individual earlier and implement safeguards in line with force policies and utilising appropriate partner agencies to promote the safety and support for the individual.

Using a picture or a physical description where positive results would otherwise be less likely and the risk of people not being identified could lead to opportunities to engage and support vulnerable people in order to promote their welfare and wellbeing being missed.
Given the importance of addressing vulnerability and preserving life and limb, this use case would align with the objective of safeguarding children and individuals at risk and the risk to life or immediate risk of serious harm would be deemed as strictly necessary to preserve the life and promote the safety of the individual. This offers SWP/ GWP the best possible opportunities to understand the vulnerability of the individual, respond accordingly and to address a pressing social need.

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 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.

Appropriate Policy Document

Section 42 of the DPA and Article 30 UK 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 policy documents for processing under Part 2 and Part 3 of the Act. These documents explain:

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.

Data Protection Officer:

SWP/GWP has a Joint Data Protection Officer (DPO) whose role it is 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.

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 (now the role is held by the Biometrics and 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 publicly 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 the FRT System.
Monitored by trained individuals	The decision making by OIFR is undertaken by Operators who have received specific training on obtaining images suitable for OIFR and assessing Candidate images returned, alongside corroborating information on police record management systems to determine if a match has been made. OIFR only returns the top 6 Candidate Images that score above the Threshold Setting. If no Candidate Images score above the Threshold Setting, no matches will be returned. Once results are returned, it is for the trained Operator to decide if a match has been made and justify the most proportionate and justified course of action in response to any matches returned. 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.

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:

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

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

In recognition of its FOIA duties, SWP/GWP makes relevant OIFR information available via its website. This includes summary information relating to OIFR. SWP/GWP will also be responsive to FOIA requests.