



Home Office

Handling facial image search requests from within the Home Office

Version 1.0

This guidance for Home Office staff sets out how to consider and handle requests made internally from other operational teams across the Home Office to conduct searches against the Passport and Immigration facial image databases.

Contents

Contents	2
About this guidance	3
Scope	3
Contacts	4
Publication	4
Changes from last version of this guidance	4
Introduction	5
Policy intent	5
Requirements	6
Direct access to immigration facial images	6
Direct access to passport facial images	7
Basis for searching facial images	8
Legal basis	8
Necessity and proportionality	8
Searching facial images	10
Necessity and proportionality	10
Purpose of search	10
Witnesses & Victims	11
Prioritisation	11
Completing the template	11
Response protocol	14
Matches	15
Rejected requests	15
Non-relevant information	15
Data transmission and storage	16
Retention of information	16
Audit and assurance	16
Sharing information	16
Vulnerable people and sharing data outside of the Home Office	17
Request template	18

About this guidance

This guidance sets out the policy on how HM Passport Office (HMPO) and Customer Operations Support Services (COSS) must treat requests to search facial images from operational teams across the Home Office against the Passport and Immigration facial image databases (facial image search).

This guidance explains the requirements which must be met before a facial image search can be performed, and before the results of that search can be shared and used.

Scope

For the purpose of this guidance:

‘HO staff’ means a person who is employed within the Home Office in one of the following specialist roles, and who has been given bespoke training on conducting facial image searches and the terms of this policy a:

- a caseworker within the Immigration Fingerprint Bureau (which is the team in VPCRS that processes requests from UK Law Enforcement Organisations (LEO) to search facial images)
- a passport counter fraud officer

‘officer’ means

- a person who is employed within the UK Home Office in a law-enforcement capacity, specifically within Immigration Enforcement, Border Force or Border Security Command, and who has been given bespoke training to exercise statutory immigration and/or customs powers, including the control of entry to and exit from the United Kingdom, the examination of persons and goods, and the enforcement of immigration and / or customs and related criminal legislation.
- passport counter fraud officer (CFO)

Immigration Fingerprint Bureau (IFB) is the team within COSS that processes requests from an officer to search facial images held on the Immigration and Asylum Biometric System (IABS))

His Majesty’s Passport Office (HMPO) relates to a passport counter fraud officer (which is the team in HMPO that processes requests from an officer to search facial images held on the passport facial image gallery).

The ‘Passport gallery’ refers to the data store of facial images, gathered from the facial photographs provided by people as part of the passport application which, along with relevant biographical information, such as names and dates of birth, are processed under the Royal Prerogative, for the purposes of maintaining a secure

passport system and border security and other purposes ancillary to the issuance and cancellation of passports.

‘Passport photographs’ are facial images that meet the standards set by the International Civil Aviation Organization (ICAO) to enable a passport to be issued.

The ‘immigration facial image database’ refers to the Immigration and Asylum Biometric System (IABS), which contains facial images provided to COSS under the:

- The Immigration (Provision of Physical Data) Regulations 2006
- The Immigration (Biometric Registration) Regulations 2008
- The British Nationality (General) Regulations 2003
- Part 2 of the Immigration (Collection, Use and Retention of Biometric Information and Related Amendments) Regulations 2021

Contacts

If you have any questions about the guidance and your line manager or senior caseworker cannot help you or you think that the guidance has factual errors, then email the Identity Security team.

If you notice any formatting errors in this guidance (broken links, spelling mistakes and so on) or have any comments about the layout or navigability of the guidance then you can email the Guidance Rules and Forms team.

Publication

Below is information on when this version of the guidance was published:

- version **1.0**
- published for Home Office staff on **31 July 2026**

Changes from last version of this guidance

This is new guidance.

Related content

[Contents](#)

Introduction

There are circumstances in which operational teams across the Home Office

Official – sensitive: start of section

The information in this section has been removed as it is restricted for internal Home Office use.

The information in this section has been removed as it is restricted for internal Home Office use.

Official – sensitive: end of section

need to request IFB or HMPO to carry out searches of facial images they have obtained against facial images held on Home Office facial image databases.

Policy intent

Facial images increasingly play a significant role in delivering identity assurance and security across the border, immigration and citizenship system. They enable quick and robust identity assurance and allow us to maintain a secure border.

Allowing facial images of people of interest to be searched against the passport and immigration facial image databases, helps to protect the UK's border and national security, prevent abuse to the immigration system and ensure public safety.

When searches are made it is recognised that it involves an intrusion on the privacy rights of people on the database, and as such a fair balance must be struck between the necessity of the search and the privacy rights of people whose data can be searched.

The Secretary of State has adopted the policy set out in this guidance with the intention of ensuring compliance with all relevant legislation, which includes human rights, data protection and equalities legislation. Any requests from officers to HM Passport Office (HMPO) and / or COSS to conduct searches against the HMPO or COSS facial image galleries must be carried out in accordance with the Human Rights Act 1998 and the Data Protection Act 2018, with particular regard to Article 8 of the European Convention on Human Rights which concerns the right to a private and family life.

Requirements

Officers making requests must use the appropriate form. To enable HMPO and / or IFB to undertake a search the officer must adhere, as far as possible, to the specifications about the quality [requirements](#) of images to be searched, which includes information about the size and format of the facial image to be searched.

Direct access to immigration facial images

Some operational commands due to the nature of their work may have direct access to a search function against the immigration facial image database. Officers with direct access must adhere to this policy guidance when considering whether to search a facial image against the immigration facial image database.

This means the officer must only conduct searches where they have a business requirement to do so in the discharge of a function of their role, it is lawful, necessary, proportionate and in accordance with the [eligibility criteria](#) contained within this guidance. Where it is unclear whether a search would meet the [eligibility criteria](#), they must consult with the [Identity Security team](#).

Any searches undertaken must be recorded for [auditing purposes](#).

Any officer who is to be given access to IABSWeb **must** receive training on using the system and demonstrate they are sufficiently skilled in facial matching.

Where IABSWeb identifies potential matches, it will provide a score (High, Medium & Low). While this is an indicator, it is not definitive and officers will need to satisfy themselves whether there is a match and confirm their decision with another officer.

Official – sensitive: start of section

The information in this section has been removed as it is restricted for internal Home Office use.

The information in this section has been removed as it is restricted for internal Home Office use.

The information in this section has been removed as it is restricted for internal Home Office use.

The information in this section has been removed as it is restricted for internal Home Office use.

The information in this section has been removed as it is restricted for internal Home Office use.

Official – sensitive: end of section

Direct access to passport facial images

Home Office staff outside of HMPO do not have direct access to HMPO facial images and any request to search the HMPO facial image gallery by an official outside HMPO must be submitted to them using the [Request Template](#) form.

Related content

[Contents](#)

Basis for searching facial images

This section sets out the basis for HMPO and IFB to consider requests to search facial images from within the Home Office against the passport and / or immigration facial image databases.

Legal basis

HM Passport Office (HMPO) process facial images supplied with passport applications under the Royal Prerogative. Furthermore, it may perform searches under the Royal Prerogative and common law powers, including where, it is in the interest of national security, for the purposes of preventing, investigating or prosecuting crime, for the purposes of preventing serious risk to life, or where it is carrying out a function under the Immigration Acts or for nationality.

Home Office officials can use biometric information obtained under Regulation 8 of the Immigration (Provision of Physical Data) Regulations 2006, Regulation 9 of the Immigration (Biometric Registration) Regulations 2008 or Regulation 4 of the Immigration (Collection, Use and Retention of Biometric Information and Related Amendments) Regulations 2021, which include:

- the exercise of a function by virtue of the Immigration Acts
- the exercise of a function in relation to nationality
- in connection with the prevention, investigation or prosecution of an offence
- for a purpose which appears to the Secretary of State to be required in order to protect national security
- in connection with identifying persons who have died or are suffering from illness or injury
- for the purpose of ascertaining whether a person has acted unlawfully, or has obtained or sought anything to which the person is not legally entitled

Necessity and proportionality

All facial image searches, and any sharing of the resulting data, must be necessary and proportionate. In summary, this means the purpose of the search must be sufficiently important in the public interest to outweigh the individual interests of those whose privacy rights are engaged, to justify the intrusion into people's privacy.

The officer must have a genuine business need to request a facial image to be searched, which is defined by their role and the discharge of their public duty. Any request made to HMPO or IFB must be recorded within the officer's team, including the reasons for making the request. The officer requesting a search must weigh up the need to undertake a search against the rights of people whose privacy will be intruded upon when carrying out such the search.

To assist HMPO and IFB officers to consider whether to search a facial image provided by another part of the Home Office against the passport and / or

immigration facial image databases and return any resulting matches, this policy guidance requires specified criteria to be met before any search can be considered.

The criteria include that:

- the search is in the public interest
- the search is likely to achieve its aims
- all other reasonable alternative avenues with lesser intrusion have been exhausted before requesting a facial image search
- the intrusion on privacy rights is proportionate to the aim being pursued - to assist in particular with this balancing exercise, the purposes for which searches can be conducted have been limited to areas where there are high levels of public interest (specifically serious crime, national security, and the protection of life)

Related content

[Contents](#)

Searching facial images

This section tells officers about making requests to IFB and HMPO and to search a facial image against the immigration and/or passport facial image databases.

Officers may only request a search of a facial image where it is necessary in connection with their lawful duty such as:

- border security (including general customs and customs revenue matters as defined in sections 1(2) and 7(2) of the Borders, Citizenship and Immigration Act 2009)
- exercising a function of the immigration acts or nationality
- in connection with the prevention, investigation or prosecution of an offence
- for a purpose which appears to the Secretary of State to be required in order to protect national security
- in connection with identifying persons who have died or are suffering from illness or injury
- for the purpose of ascertaining whether a person has acted unlawfully or has obtained or sought anything to which the person is not legally entitled

Necessity and proportionality

All facial image searches must be necessary and proportionate. In summary, this means the purpose of the search must be sufficiently important in the public interest to outweigh the individual interests of those whose privacy rights are engaged, to justify the intrusion into people's privacy. This requires officers requesting a search to weigh up the need to undertake a search against the rights of people whose privacy will be intruded upon when carrying out such a search.

To assess whether to request a search a facial image against the passport and / or immigration facial image databases, officers must satisfy themselves that their request meets specified criteria below:

- the search is in the public interest
- the search is likely to achieve its aims
- all other reasonable alternative avenues with lesser intrusion have been exhausted before requesting a facial image search
- the intrusion on privacy rights is proportionate to the aim being pursued - to assist in particular with this balancing exercise, the purposes for which searches can be conducted are limited to one or more of the purposes set out in the [Purpose of Search](#), where there is a primary interest in border security, a function of the Immigration Acts or nationality

Purpose of search

Officers may submit a request to HMPO and/or IFB to search a facial image where the request is for a purpose that is in connection with border security (including a

general customs or customs revenue matter), a function of the immigration acts or nationality, but may also include:

- where they are seeking to prevent, investigate or prosecute a crime
- where required to protect national security
- to identify people who have died, or are suffering from illness or injury
- to ascertain whether a person has acted unlawfully, or has obtained or sought anything to which the person is not legally entitled

Officers must only use the results arising from a search for the purpose they requested it. If they need to share it with any other organisation, including law enforcement organisations, they must follow the section on sharing data.

Witnesses & Victims

Officers may only request HMPO and/or IFB to search a facial image of an essential witness or victim, where it is necessary and proportionate to identify them. For example, where an officer needs to identify a possible victim of modern slavery or trafficking or needs to identify an essential witness to support an investigation or prosecution on a matter that would also be considered to be a serious crime as set out in the “[Handling facial image search requests from Law Enforcement Organisations](#)” guidance, and not identifying them significantly risks undermining any investigation or prosecution.

Prioritisation

Where an officer considers their request to be urgent, they must state this on the [request template](#), so HMPO and/or IFB staff can flag it up for prioritisation. They will endeavour to process urgent requests as quickly as possible, but this will be dependent upon demand and resource availability. Officers need to be aware they must avoid making urgent requests, unless it is absolutely necessary as this could adversely affect processing of other more pressing urgent requests.

Completing the template

The requesting officer must confirm on the [request template](#) to HMPO and/or IFB that they have exhausted all other reasonable avenues to identify the person of interest, including making checks against any databases they have access to, and that they have been unable to identify a person through their databases and any other operational means. They must also confirm that the request has been approved at the appropriate level, which is normally the equivalent of a Senior Officer or Senior Executive Officer grade.

Official – sensitive: start of section

The information in this section has been removed as it is restricted for internal Home Office use.

The information in this section has been removed as it is restricted for internal Home Office use.

The information in this section has been removed as it is restricted for internal Home Office use.

Official – sensitive: end of section

Requests to identify a facial image must be sent on an individual basis or contained within a list if part of a single investigation. Within each request, a small number of related images, such as video frames captured by a CCTV camera may be acceptable.

Related content

[Contents](#)

Vulnerable people

Officers must take steps to protect people whose identities, once exposed, could reveal sensitive personal information about them. Such information must be treated sensitively and, on a need-to-know basis and must not be shared beyond the individual members of HMPO and / or IFB and officers who need sight of the information. For example, a facial matching exercise might reveal a person has changed their gender or is a victim of domestic violence who has changed their name, and unnecessarily exposing their previous identity might cause undue harm. When transmitting such information, it must be sent to a specific person and not a generic team address to minimise disclosure. The officer will need to contact HMPO counter fraud and/or the Immigration Fingerprint Bureau team(s) to identify the relevant person.

HMPO and/or IFB staff must review the online form to check whether the officer has flagged they suspect the person in question may be vulnerable.

Related content

[Contents](#)

Response protocol

HM Passport Office (HMPO) or COSS will respond to requests as follows:

- **decline the request** if it is not found to be lawful, necessary and proportionate, and provide an explanation for the decision
- **report no match found** - this is when HMPO or IFB cannot establish any matches to the image provided - this does not mean the person's facial image is not held on either of the HMPO or IFB databases, but simply means the image could not be matched
- **report a match and return data in one of two ways:**
 - **where an officer provides an image of a person who they cannot identify**, HMPO or IFB will provide the officer details of the match, including any images and associated biographical information of the potential matches.
 - **where the officer knows to whom the image relates** but is seeking to establish whether the person has any other identities, HMPO or IFB will provide the officer with details of the person or persons it holds, including any facial images to enable the officer to confirm whether the identities relate to the same person

The level of support that HMPO or IFB will be able to offer will also be determined by capacity to process any requests.

Any matches will be returned to the requesting officer to be used only for the purposes for which the request was made; with border security (in respect of people and/or goods), a function of the immigration acts or nationality, but may also include:

- where they are seeking to prevent, investigate or prosecute a crime
- where required to protect national security
- to identify people who have died, or are suffering from illness or injury
- to ascertain whether a person has acted unlawfully or has obtained or sought anything to which the person is not legally entitled

Where an officer is seeking to share the results with another UK Law Enforcement Organisation (LEO), they must follow the steps set out in [Sharing information with third parties](#)

In cases where a person's image is matched against a facial image on the database, HMPO and IFB may provide the following associated biographical information:

HMPO	IFB
• name • date of birth • nationality • sex marker • passport number	• name • date of birth • sex marker • port / local reference: • person nationality code • passport nationality code:

HMPO	IFB
	• passport number • Home Office reference • biometric recording officer • biometric recording date • biometric recording location

Last known address, other contact, biographical details or other relevant data necessary for the purpose of the search may also be provided to the officer, where available.

Matches

A decision that an image provided by the officer matches an image on the passport and/or immigration facial images databases involves a judgment that the images stored on one of the databases are very similar to the facial images the officer wanted HMPO and/or IFB to search. Where matches are produced after carrying out a search following a request from an officer on the person of interest and / or unconnected people, HMPO and IFB will provide the images that the Passport or Immigration facial image databases identify as a possible match. It is the responsibility of the officer who requested the search to assess whether the facial image(s) is/are a match for the facial image(s) provided by HMPO and or IFB. Any matches **must** be assessed by at least one other officer by undertaking a visual comparison of the returned facial images.

Rejected requests

HMPO and/or IFB staff must inform the officer when they have declined a request to undertake a facial search. Where the officer wants that decision to be reviewed, their manager or senior colleague may email the responsible team with its reasons. A team leader who is responsible for the team that made the decision to reject the request will consider the request to review the decision and will inform the requestor on whether they will change the previous decision. The scope of any review will be limited to decisions on whether the request met the eligibility criteria.

Non-relevant information

Where, HMPO or IFB provides an officer with images and details of a person whom the officer ascertains is not relevant to their investigation, the officer must take steps to delete such information immediately.

Related content

[Contents](#)

Data transmission and storage

All data transmission must be undertaken securely using secure digital means, such as secure email.

Facial images must be stored on secure electronic storage systems and emails containing facial images, including any associated biographical information must be deleted immediately after the data has been transferred onto the secure storage system ahead of processing.

Retention of information

Officers must ensure that personal information is processed in a manner that ensures appropriate security of that information, using appropriate technical or organisational measures. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. Personal information must only be retained for as long as it needed and in line with other data retention policies and legislation.

Facial images from the immigration facial image database must be retained in line with the Retention and usage of biometric information guidance. For facial images held on HMPO's facial image gallery, this is set out in the [HMPO privacy information notice - GOV.UK](#).

Audit and assurance

HMPO, IFB and officers making requests must retain a record of the requests and decisions for up to 6 years. The record must include details of the requestor, the date of the request, whether the search was authorised and if so, the outcome of the search.

The information may be used for internal and external assurance purposes to ensure officials and officers adhere to the Data Sharing Agreements (DSA) and this policy guidance.

Sharing information

Where an officer who has received results from a facial search by either HMPO or IFB or both needs to share the information with an external LEO, who they are embedded or working in partnership, the officer must ensure that any decision to share the information with that organisation is lawful and in line with the overall intent of this policy and their respective DSA with the Home Office.

Officers may only share the information with another LEO, where the purpose of the request is:

- for the purposes of prevention, investigation and prosecution of “serious crime”
- in the interests of national security

- for the purposes of prevention of serious risk to life

Serious crime is defined in the “[Handling facial image search requests from Law Enforcement Organisations](#)” guidance.

Officers must only share the facial image and associated data they have agreed with another officer to be a match against the image they requested HMPO and/or IFB to search.

Where it is unclear whether the need to share information relates to the purposes of the embedded or partnership relationship, the officer must direct them to the “[Handling facial image search requests from Law Enforcement Organisations](#)” guidance and direct the LEO to use the template in the guidance when making a request to HMPO and/or IFB to search a facial image, should the LEO want a facial image to be searched against the passport or immigration facial image databases.

Any sharing of information provided by IFB must be processed in accordance with section 21 of the Immigration and Asylum Act 1999. In respect of passport data, it can be shared under common law powers. In both cases, any sharing must comply with data protection legislation and the European Convention on Human Rights.

Official – sensitive: start of section

The information in this section has been removed as it is restricted for internal Home Office use.

Official – sensitive: start of section

Vulnerable people and sharing data outside of the Home Office

Where the officer needs to share the information with another LEO and they consider the person to be vulnerable, they must seek authorisation from a Senior Officer grade or equivalent where they work before the information can be shared elsewhere and follow the approach on vulnerable people set out in “[Handling facial image search requests from Law Enforcement Organisations](#)”.

Related content

[Contents](#)

Request template

This is the form officers must use to request HMPO and / or IFB to process a search on a facial image they want to check. A single form must be used for each individual investigation regardless of the number of images the officer wants HMPO and / or IFB to search.

Official – sensitive: start of section

The information in this section has been removed as it is restricted for internal Home Office use.

The information in this section has been removed as it is restricted for internal Home Office use.

The information in this section has been removed as it is restricted for internal Home Office use.

The information in this section has been removed as it is restricted for internal Home Office use.

The information in this section has been removed as it is restricted for internal Home Office use.

The information in this section has been removed as it is restricted for internal Home Office use.

The information in this section has been removed as it is restricted for internal Home Office use.

The information in this section has been removed as it is restricted for internal Home Office use.

The information in this section has been removed as it is restricted for internal Home Office use.

The information in this section has been removed as it is restricted for internal Home Office use.

The information in this section has been removed as it is restricted for internal Home Office use.

The information in this section has been removed as it is restricted for internal Home Office use.

Official – sensitive: end of section

Related content

[Contents](#)