Home Office

Handling facial image search requests from Law Enforcement Organisations

Version 1.0

This guidance tells Home Office staff how to consider and handle requests from UK law enforcement organisations to conduct searches against the Passport and Immigration facial image databases.

Contents

About this guidance

This guidance sets out the policy on how HM Passport Office (HMPO) and UK Visas and Immigration (UKVI) should treat requests from UK law enforcement organisations (LEOs) to conduct searches against the Passport and Immigration facial image databases (facial image search).

In particular, 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 caseworker within the Immigration Fingerprint Bureau (which is the team in UKVI that processes requests from LEOs to search facial images)
- a passport counter fraud officer

'UK Law enforcement organisation' (LEO) means a UK organisation designated as a law enforcement competent authority under the Data Protection Act 2018, which includes the following:

- UK Police Forces, including Counter Terrorist Policing
- National Crime Agency

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 process 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 UKVI 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 Review, Atlas 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 **15 September 2025**

Changes from last version of this guidance

This is new guidance.

Related content
Contents

Introduction

There are circumstances in which UK law enforcement organisations (LEOs) need to request that the Home Office carry out searches of facial images held on Home Office databases, using a facial image of a person the LEO considers to be of interest to them.

Policy intent

Facial images 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.

The passport and immigration facial image databases can also provide value for LEOs, including for law enforcement investigations and national security purposes, through the carrying out of searches of images against them. 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 human rights, data protection and equalities legislation. Any requests from LEOs to HMPO and / or UKVI to conduct searches against the HMPO or UKVI 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.

This guidance seeks to ensure that Home Office staff understand and comply with the legal requirements. When they consider a request from a LEO to search a facial image, they must be satisfied there is a legal basis for performing the search, and that the search is both necessary and proportionate. Data Sharing Agreements (DSA) between Home Office and LEOs are in place to formalise the framework set out in this policy.

Requirements

The LEO must use the request template when making a request to HMPO and / or UKVI to search a facial image. To enable HMPO and / or UKVI to undertake a search the LEO should adhere, as far as possible, to the specifications about the quality requirements of images to be searched, which includes information and about the size and format of the facial image to be searched.

Related content
Contents

Basis for searching facial images

This section sets out the basis for Home Office staff to consider requests from UK law enforcement organisations (LEOs) to search facial images they provide against the passport and / or immigration facial image databases.

Legal basis

HMPO process facial images supplied with passport applications under the Royal Prerogative. Furthermore, it may perform searches and share data with LEOs under the Royal Prerogative and common law powers, including where it is in the interest of national security, for the purposes of preventing or investigating crime, or for the purposes of preventing serious risk to life.

Immigration staff may share facial image data with the police and other LEOs under section 21 of the Immigration and Asylum Act 1999, Regulation 8 of the Immigration (Provision of Physical Data) Regulations 2006, or Regulation 9 of the Immigration (Biometric Registration) Regulations 2008.

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. This requires anyone performing 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 the search.

To assist Home Office staff to consider whether to search a facial image provided by a LEO 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

Types of checks

This section sets out the types of searches and sharing that HMPO and UKVI may undertake.

Searches by HMPO and UKVI

HMPO and UKVI can undertake a comparison of a facial image provided by a UK law enforcement organisations (LEO) against the facial images stored on the HMPO and / or UKVI databases where it meets all the criteria set out in this guidance. This can include facial images captured in a supervised environment, such as at a police station, or can be from unsupervised camera sources, such as from CCTV or from other devices. However, the images must adhere to the requirements in the criteria to reduce the risk of incorrect identification.

HMPO and UKVI may only share facial images and associated biographical information resulting from the search, where they are satisfied the facial images relate to the person in the image which the LEO requested that they search. All matches against facial images held on the passport and / or immigration databases must be reviewed and confirmed by at least two members of Home Office staff, before any matched images can be returned to the LEO.

Related content
Contents

Submitting and processing requests

This section sets out how UK law enforcement organisations (LEOs) must submit any requests to HMPO or UKVI, and how Home Office staff must process them.

LEOs

The LEO must confirm on the request template they will ensure any actions taken in respect of information provided are in accordance with this guidance, data protection legislation and the Human Rights Act 1998. Requests that are not submitted on the template or are incomplete will be rejected.

LEOs must direct their requests to HMPO or UKVI based on whether they consider the person to be a British national (HMPO) or a foreign national (UKVI). Where the LEO is unsure of the person's nationality, they need to make separate requests to HMPO and UKVI. If the person is a foreign national and the LEO has their fingerprints, the LEO must run the fingerprints checks against the IABS database and only submit a request to UKVI to process a facial image if the fingerprint checks have not identified the individual. The LEO may be able to identify the person if they were issued with a visa, claimed asylum or were encountered by Immigration Enforcement.

LEOs must make requests via secure official email using the specified template form. It is the responsibility of the LEOs to ensure that any requests submitted comply with the framework of the relevant Data Sharing Agreements (DSA) between the Home Office and the LEO.

Prioritisation

Where the requesting LEO considers their request to be urgent, they should state this on the request template, so Home Office staff can flag it up for prioritisation. Home Office staff will endeavour to process urgent requests as quickly as possible, but this will be dependent upon demand and resource availability. LEOs need to be aware they must avoid making urgent requests, unless it is absolutely necessary as this could adversely affect processing of urgent requests.

Completing the template

The requesting LEO must confirm on the request template that they have exhausted all other reasonable avenues to identify the person of interest, including making checks against their own national and local databases, 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 adheres to the LEO's own searching policy and has been approved at the appropriate level, which is normally the equivalent of a police Inspector rank.

The request template sets out the information required, which includes information about the person of interest and specifications of the facial image the LEO wants

HMPO and / or UKVI to search. The officer submitting the requests should include as much information on the request template as possible, to improve the prospects of confirming an accurate match.

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.

Official – sensitive: end of section

Home Office staff will check the images for matches and should only send facial images and accompanying biographical information to the LEO, where they are satisfied that the image matches the facial image or images provided by the LEO. This is to reduce the risk of images of other people being incorrectly shared.

Related content
Contents

Criteria for a search

HMPO and UKVI have the power to conduct facial image searches in the circumstances set out in the section that sets out the basis for agreeing to search a facial image provided by the UK law enforcement organisations (LEO). However, they may only conduct such a search where it is necessary and proportionate to do so.

Necessary and proportionate

Home Office staff must satisfy themselves the request from the LEO to search a facial image is both necessary and proportionate, by considering the request against each of the four requirements set out below, which the LEO must meet before HMPO and / or UKVI will agree to conduct a facial image search.

Importance

Home Office staff must satisfy themselves that the need to carry out a facial image search fulfils an important objective in the public interest.

Law enforcement objectives including preventing, investigating or prosecuting crime, protecting life and protecting national security will typically be considered sufficiently important to meet this requirement. However, Home Office staff must satisfy themselves that the search is being requested for one or more of these purposes.

Achievement of the purpose

Home Office staff must satisfy themselves that running a facial matching search is reasonably likely to achieve the purpose of the search. This includes checking:

- whether there is a rational connection between the search and the stated purpose
- whether the facial image provided by the LEO is useable and meets the facial image requirements
- any biographical information before undertaking an image search, which might indicate whether the person's facial image is likely to be stored on either the HMPO or UKVI facial image databases

Exhausting other options

The LEO must confirm they have exhausted all other reasonable options available to them before requesting HMPO and / or UKVI undertake a facial image search. LEOs must confirm on the request template they have checked any law enforcement databases available to them, including international, national and regional or local, and completed other enquiries before approaching HMPO and / or UKVI to undertake a facial image search. If there is a less intrusive way of identifying the person, the LEO must use that option first to try and identify the person of interest.

Balancing privacy rights

When a search is undertaken, the privacy of every person whose facial image is on the HMPO and / or UKVI facial image databases could be impacted because of their facial image being searched, even if their facial image is not matched. Therefore, the need for any request to search a facial image against the passport and / or immigration databases needs to outweigh any infringement upon other people's rights to privacy.

To balance the right to privacy against the need to conduct a facial image search, Home Office staff must consider whether the benefits of undertaking a facial image search outweigh the intrusion on the right to privacy of persons on the database. To assist staff with this decision making, the Home Office has set a threshold of seriousness, below which a search will not be run. Before agreeing to a search Home Office staff must therefore be satisfied that the search is either:

- 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

A serious crime for the purpose of this policy means either (a) any sexual offence, or (b) any act which if planned, attempted or carried out by a person would normally be capable of resulting in a sentence of imprisonment for a term of at least 2 years and either involves the use of violence, grooming, online criminality or could result in substantial financial gain.

Home Office staff must consider the extent of the alleged crime or incident in terms of the number of people affected and the level of harm that has been caused or could be caused by the person of interest, against the level of intrusion sharing the information would have into a person's right to privacy, and be satisfied that the public interest is sufficient to share the information.

Related content
Contents

Vulnerable people

HMPO and UKVI will 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 UKVI and the UK law enforcement organisations (LEO) 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. Where the LEO needs to share the information with another organisation, it must seek authorisation from the Home Office staff member or another officer where they work before the information can be shared elsewhere.

Home Office staff must review section 8 of the request template to check whether the LEO has flagged they suspect the person in question may be vulnerable.

Related content
Contents

Response protocol

HMPO or UKVI 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 UKVI cannot establish any matches to the image provided - this does not mean the subject's facial image is not held on either of the HMPO or UKVI databases, but simply means the image could not be matched
- **report a match and return data in one of two ways**:
  - **where the UK law enforcement organisation (LEO) provides an image of a person who they cannot identify,** HMPO or UKVI will provide details of the match - to provide an image and associated biographical information, you must be satisfied that the image provided by the LEO matches the image or images held on the databases
  - **where the LEO knows to whom the image relates** but is seeking to establish whether the individual has any other identities, HMPO or UKVI will provide details of the person or persons it holds, including any facial image to enable the LEO to confirm whether the identities relate to the same person

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

Any matches will be returned to the requesting LEOs to be used only for the purposes for which the request was made; namely, as above, for the prevention, investigation or prosecution of a serious crime, in the interests of national security, or for the prevention of serious risk to life.

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

HMPO	UKVI
• name • date of birth • nationality • sex marker • passport number	• port / local reference: • person nationality code • passport nationality code: • passport number • Home Office reference • biometric recording officer • biometric recording date • biometric recording location

Last known address, other contact or biographical details may also be provided to the LEO, where available.

Official – sensitive: start of section

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

Official – sensitive: end of section

Matches

The decision that an image provided by the LEO matches an image on the database involves a judgement that the images stored on the passport and / or immigration databases are very similar to the facial images provided by the LEO. Where matches are produced after carrying out a search following a request from a LEO, of the person of interest and / or unconnected people, HMPO and UKVI will only share the results where Home Office staff are satisfied the facial image or images are a match to the facial image of the person of interest. Where there are multiple matches Home Office staff will only share those images where they are satisfied that they are a possible match to the facial images provided by the LEO.

All matches against facial images held on the passport and / or immigration databases **must** be reviewed and confirmed by at least 2 members of Home Office staff, who must also take account of any other information provided by the LEO that would assist them to decide whether the results are a match. To do this, they will undertake a visual comparison of the returned facial images to ensure that they are a match, which will avoid sharing facial images of people who do not relate to the person of interest with LEOs.

Law enforcement retention of any information shared

The Home Office expects LEOs to use the information shared by HMPO and / or UKVI for the defined purposes, which are either:

- the prevention, investigation and prosecution of "serious crime"
- in the interest of national security
- for the purposes of prevention of serious risk to life

They must store it securely, in a manner that is set out in their respective Data Sharing Agreement (DSA) with the Home Office. It cannot be processed for other purposes, and it may only be retained so long as it is necessary for the purposes for which the facial image request was made. Where the LEO no longer needs the information, it must be destroyed.

Personal information must be 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.

Sharing information with third parties

Where LEOs need to share the facial image with another organisation, the LEO must ensure that any decision to share the information with another organisation is lawful and in line with the overall intent of this policy and their respective DSA with the Home Office.

Non-relevant information

Where, despite the checks outlined above, HMPO or UKVI provides an LEO with images and details of a person whom the LEO ascertains is not relevant to its investigation, the LEO must take steps to delete such information immediately.

Rejected requests

Home Office staff must inform the LEO when it has rejected a request to undertake a facial search. Where the LEO wants that decision to be reviewed, they should 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.

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.

Audit and assurance

A record of the requests and decisions must be made and retained 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 that UK law enforcement organisations (LEOs) and Home Office staff adhere to the Data Sharing Agreements (DSA) and this policy guidance.

Related content
Contents

Assurance

The process for considering requests from UK law enforcement organisations (LEOs) to search facial images against the HMPO and / or UKVI facial databases is subject to internal and external assurance procedures.

Internal assurance

The Senior Information Asset Owners (SIAO) for HMPO and UKVI are responsible for ensuring requests submitted by LEOs are made in accordance with the Data Sharing Agreements (DSAs) between the signing organisations and that Home Office staff adhere to the policy guidance and associated training. The roles can be delegated to a manager to perform.

Compliance checks include periodically providing management information to the SIAO about the number of requests and the responses and sampling some cases to ensure they followed the DSA and policy guidance. This information will be provided to the SIAO at least annually.

External assurance

The Information Commissioner's Office (ICO) is the UK regulator for personal data. It has regulatory responsibility for biometrics captured, retained and used by HMPO and / or UKVI.

Biometric data is a type of personal data whose processing is designated as sensitive processing, meaning that it carries additional protection under data protection legislation. The ICO has powers to enable it to take regulatory action if personal data is processed in a way which does not comply with the applicable legislation, set out in either the UK General Data Protection Regulation (GDPR) (GDPR Article 57), or the Data Protection Act (DPA) 2018 (DPA 2018, Section 116; Schedule 13). This action can include prohibitions on processing, fines, and other measures depending on the seriousness of the non-compliance and the level of risk to individuals. These actions are supported by further powers to compel data controllers to co-operate with its investigations by providing information on request.

The ICO's key tasks are set out in legislation1, 2, and include:

- advising parliament and others
- promoting awareness of controllers and processor
- promoting awareness of the public
- monitor and enforcing compliance with data protection legislation

Related content
Contents

Request template

This is the form UK law enforcement organisations (LEOs) must use to request HMPO and / or UKVI to process a search on a facial image against facial images held on their databases. A single form must be used for each individual investigation regardless of the number of images the LEO wants HMPO and / or UKVI to be searched.

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.

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.

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.

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.

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.

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