



Home Office

Identity management (Enforcement)

Version 5.0

Contents

Contents.....	2
About this guidance	4
Contacts	4
Publication.....	4
Changes from last version of this guidance	4
Identity management: background and purpose	5
Biometrics (enforcement cases)	7
Powers to check or take biometrics	7
Summary: when to use each power	8
Procedures for the taking of biometrics	10
Capturing biometrics.....	10
Immigration bail.....	11
Ink and paper	11
Electronic scans	12
Checking fingerprints to establish identity	12
Attendance for photographing and fingerprinting	12
Taking biometrics from dependants	13
Capturing biometrics from children: safeguards.....	15
Age dispute	15
Previous age assessment.....	16
Reasonable belief	16
Additional safeguards	17
Taking of biometrics from vulnerable adults	19
Police ‘appropriate adult scheme’	19
Use of reasonable force when taking biometrics	19
Fingerprinting of corpses	20
Fingerprints: requests for expert statements	20
Establishing identity with fingerprints and data sharing	21
Five Country Conference (FCC) Data Sharing Protocol	22
Storage of fingerprints	23
Using Mobile Biometric Devices (MBD).....	24
Use of Mobile Biometric Devices (MBD): exploratory examination.....	24
Use of Mobile Biometric Devices (MBD): administrative interviews.....	25
Security and safe storage of Mobile Biometric Devices (MBD).....	26
Additional identity checks.....	27

Additional checks	29
Document verification and forgeries	30
Examination of documents	30
Template: IS86	31

About this guidance

This guidance tells Immigration Enforcement officers about how they may determine an encountered person's identity. This includes taking, storing, and sharing the person's biometrics (facial image and up to 10 fingerprints).

In this guidance:

- 'people / person' means applicants, claimants, individuals, and dependants

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 Policy 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 **5.0**
- published for Home Office staff on **30 September 2026**

Changes from last version of this guidance

Significant updates across the guidance include:

- references to mobile biometric devices (MBD) removed
- updated to reflect the addition of all biometrics
- references to CID replaced with Atlas
- the addition of a section on [reasonable belief](#)

Related content

[Contents](#)

Identity management: background and purpose

Identity management means organising and looking after the biometric and biographical information we have about people, so we can find the data we have on a person in one place. It helps us to know exactly who someone is whenever they are in contact with the Home Office and enables us to handle them appropriately.

This means we can identify the person accurately without having to reestablish their identity on each encounter. Identity management across the Home Office is underpinned by the use of biometrics, in the form of fingerprints and facial images, to support identity assurance and suitability checks on foreign nationals who are subject to immigration control.

By confirming a person's identity accurately, we are able to prevent and detect identity abuse by people attempting to enter or stay in the UK without permission to do so. Identity abuse can be for a range of purposes, such as illegal immigration, or to facilitate crime or terrorism. This is why it is important that we check and / or capture a foreign national's biometrics and associated biographics whenever they are encountered.

When you need to check a person's identity, you **must** always consider either checking or taking their biometrics.

Official - sensitive: start of section

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

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

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

Official - sensitive: end of section

For more information about biometrics, see: [Biometrics information – introduction guidance](#).

Related content

[Contents](#)

Biometrics (enforcement cases)

This page tells Immigration Enforcement officers who they may take biometrics from for immigration purposes, and the procedures to follow when doing so.

Home Office ministers **expect** biometrics to be taken whenever a person meets one of the conditions set out in the [Powers to check or take biometrics section](#) below, unless a person is exempt or excused. Furthermore, where you consider a person is also likely to be, subject to extended fingerprint retention because they are a risk of high harm to border security or public safety, you **must** capture their biometrics. See the guidance on Retention and usage of biometric information for more information.

We take and use biometrics, in the form of a facial image and fingerprints, to fix and confirm the identities of all foreign nationals who are required to apply for entry clearance or are applying to extend their stay in the UK for over 6 months and then from those applying to become British citizens. In addition, we capture facial images of non-visa nationals who apply for an Electronic Travel Authorisation (ETA).

Biometrics enable us to conduct comprehensive checks against immigration and criminality records to prevent permission being granted to illegal immigrants and foreign nationals who are a public protection threat or use multiple identities. For example, enrolling fingerprints from people who apply for a visa has helped us to identify people who have stayed in the UK unlawfully and have sought to disguise their identity.

Powers to check or take biometrics

The powers relevant to Immigration Enforcement, to take biometrics for immigration purposes arise from:

- [Paragraph 18\(2\) of Schedule 2 to the Immigration Act 1971](#) ('1971 act') – this is for identity purposes only, and only in relation to a person who is detained, or liable to be detained, under paragraph 16 - it allows immigration officers (IOs) to check a person's biometrics (face and fingerprints) where they suspect the person to be unlawfully in the UK and are unable to ascertain their identity
- [Section 141 of the Immigration and Asylum Act 1999](#) (the 1999 act) and [Regulation 2 of the Immigration \(Collection, Use and Retention of Biometric Information and Related Amendments\) Regulations 2021](#) (the 2021 regulations) enable officers to capture a facial image and fingerprints from a person who:
 - on arrival to the United Kingdom, fails to produce a valid passport with photograph or some other document satisfactorily establishing their identity and nationality or citizenship
 - has been refused permission to enter the United Kingdom but has been granted immigration bail subject to a residence or reporting condition, if an immigration officer reasonably suspects the person might break the condition
 - the Secretary of State is considering whether to make, or has decided to make, a deportation order; or a person in respect of whom the automatic deportation regime applies, or has decided that it applies

- requires permission to enter or stay in the United Kingdom but does not have it, which includes illegal entrants and overstayers
- has been detained under paragraph 16 of schedule 2 to the 1971 act (10) or arrested under paragraph 17 of that schedule
- has made a protection claim
- is a family member of any of these categories (except those subject to a deportation order or the automatic deportation scheme) where that family member does not have a right of abode in the UK or indefinite leave to enter or remain
- is the dependant of a person subject to a deportation order, where the dependant does not have a right of abode in the UK, indefinite leave to enter or remain

Fingerprinting under the 1999 act and photographing under the 2021 regulations include [safeguards for taking fingerprints from children](#). Although not included in the legislation, similar approaches apply to [vulnerable adults](#).

The policy for the retention and usage of such data is set out in the Retention and usage of biometric information guidance.

Summary: when to use each power

The table below summarises, which of the fingerprinting powers should be used within some of the main immigration actions (this list is not exhaustive):

Scenario	Paragraph 18(2) of schedule 2 to the 1971 act	Sections 141-143 of the Immigration and Asylum Act 1999 (For fingerprints)	The Immigration (Collection, Use and Retention of Biometric Information and Related Amendments) Regulations 2021 (For facial images)
To check an identity	Yes	No	No
To raise a new immigration record	No	Yes	Yes
To process an existing immigration record	No	Yes	Yes
To require attendance for biometrics	No	Yes	Yes
To take biometrics from family members and/ dependants	No	Yes	Yes
To retain the biometrics after positive identification has been made	No	Yes	Yes

Scenario	Paragraph 18(2) of schedule 2 to the 1971 act	Sections 141-143 of the Immigration and Asylum Act 1999 (For fingerprints)	The Immigration (Collection, Use and Retention of Biometric Information and Related Amendments) Regulations 2021 (For facial images)
To take biometrics for re-documentation purposes	No	Yes	Yes

Related content

[Contents](#)

Procedures for the taking of biometrics

Those authorised to take biometrics (known as an 'authorised person') are:

- a police constable
- an immigration officer
- a prison officer
- an officer of the Secretary of State authorised for the purpose (a civil servant or customs officer, if authorised and trained)
- a person who is employed by a contractor, in connection with the discharge of the contractor's duties under a detention centre contract (Immigration Removal Centre)
- from 6 October 2026, a person who is employed by a contractor in connection with the discharge of the contractor's duties under a short-term holding facility contract

Official - sensitive: start of section

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

Official - sensitive: end of section

Capturing biometrics

You must take biometrics as soon as possible after establishing that a person and any family members or dependants is / are liable to have their biometrics taken.

Official - sensitive: start of section

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

Official - sensitive: end of section

Ink and paper fingerprinting must be conducted exclusively on original IFB1 forms. The use of printed or photocopied IFB1 forms is prohibited due to the risk of reduced fingerprint quality and compromised search results. If original IFB1 forms are not available, officers must either use livescan or rearrange the enrolment.

Where you have taken biometrics from a person under any of the powers in the 1971 act, or the 1999 act, and the 2021 regulations, officers must comply with the relevant parts of the codes of practice provisions on biometrics as modified by the [Immigration \(PACE Codes of Practice No 2 and amendment\) Direction 2000](#) and the [Immigration \(PACE Codes of Practice\) Direction 2013 \(Code D – 4.10\)](#).

Details such as missing digits or hands should be recorded on a person's Atlas biographical page.

Immigration bail

Where a person has been refused permission to enter the UK, but you are going to grant them immigration bail, under Schedule 10 to the Immigration Act 2016 and you reasonably suspect the person might break any condition imposed on them relating to their residence or as to reporting to a police or an immigration officer, you may require them to provide their biometrics (face and fingerprints). This must be authorised by a chief immigration officer (CIO) beforehand. If a person is already subject to a Deportation Order, requires immigration permission or there is another reason that allows an officer to take the person's biometrics, this does not apply.

Ink and paper

If you take fingerprints on an IFB1 form (using the ink and paper method), you must:

- tell the applicant they are to be fingerprinted and explain that it is normal procedure
- where prints are being taken under the 1999 act, give the applicant form IS.86 which explains:
 - their liability to be fingerprinted
 - why they are to be fingerprinted
 - when the fingerprints will be destroyed
- fully complete the written details on form IFB1 (do not use any other form) including the reason for taking fingerprints
- check fingerprint quality and that form IFB1 has been completed correctly - if fingerprint quality is inadequate, destroy the form and take another set
- do not make or keep copies of the IFB1 form

Official - sensitive: start of section

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

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

Official - sensitive: end of section

Electronic scans

Fingerprints taken using police livescan units should be solely for the searching or verification against fingerprints already recorded on the IABS. Scan results are not recorded or saved on the IABS.

Information on how to take fingerprints via livescan / cardscan can be found at the Biometric Recording Station (BRS) User Guide section 5.3.1.

Home Office livescan units are non-mobile units (generally office based) and are suitable for taking fingerprints for immigration purposes under the 1999 act. Fingerprints taken on these units are saved and recorded on the IABS once the scan has been transmitted. All biographic details must be completed in full before electronically transmitting the scans to the immigration fingerprint bureau (IFB).

Checking fingerprints to establish identity

Fingerprints taken to establish the identity of a person under the 1971 act, must be taken on either form IFB1 or a [Mobile Biometric Device \(MBD\)](#), which is a device that can be connected to a smartphone to enable checks on fingerprints. The police reporting and notebook organiser (PRONTO) digital pocket notebook (DPNB) must be fully updated to the effect that a search has taken place and the result.

If you do use a form IFB1, you **must** send it to IFB for searching, with a clear indication that fingerprints have been taken under the 1971 act so that they can be processed appropriately and deleted immediately after checks have been made.

Attendance for photographing and fingerprinting

The relevant legislation for attendance is set out in the [1999 act for fingerprinting](#), and the [2021 regulations for facial images](#).

Normally, those subject to fingerprinting are fingerprinted immediately so that the results are known when considering service of papers and detention.

However, a person may be required to attend at a specified place for fingerprinting and photographing. The person must be given a period of at least 7 days in which to

attend. Where this is necessary, BAIL201 must be used. Those who fail to comply may be arrested without warrant by a police constable or immigration officer (IO), unless the requirement has ceased to have effect. Before such a person is released, their biometrics can be taken, if necessary, by moving them first to an appropriate place to do so.

In family cases, with a child under the age of 5 years, a note must be placed on Atlas to remind the reporting centre officer that once the child has reached 5 years of age, they must be fingerprinted as soon as possible. In these circumstances, officers must bear in mind Home Office policy on children and reporting. If it is possible for members of the local family team to fingerprint the child during an invited family returns process meeting or a welfare visit, using a mobile fingerprinting kit, this is to be preferred to the setting up of a required one-off reporting event.

Should the family be reported and confirmed as missing at a later stage, IFB fingerprint records will be the best means of identification for the Missing Persons Bureau, who will lead the investigation to trace the family.

Official - sensitive: start of section

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

Official - sensitive: end of section

Taking biometrics from dependants

Our legislation allows for the fingerprinting and photographing of a person who is a family member of, or dependant of, someone who is a family member of a person who lacks ID at the border, is likely to breach bail, does not hold the required immigration permission, has been detained under paragraph 16 of schedule 2 of the 1971 act or arrested under paragraph 17 of the same schedule, or has claimed asylum, or is a dependent of a person subject to a deportation action (see below for further details).

A 'family member' is defined as a person who does not have a right of abode, indefinite leave to enter or remain in the UK and they are either:

- the person's partner
- the person's child
- any other child who is living in the same household and under the care of the person
- the parents of the person, where the person is a child
- an adult dependant relative of the person

For the purposes of those subject to a deportation order, a dependant person is someone who does not have a right of abode in the United Kingdom or indefinite leave to enter or remain in the United Kingdom, and they are either:

- the person's spouse
- the person's child (child is defined here as under 18)

If any family members or dependants are aged under 18, or have been recognised as being vulnerable, you must refer to the guidance on [Fingerprinting children](#) and [Fingerprinting vulnerable adults](#) respectively.

Related content

[Contents](#)

Capturing biometrics from children: safeguards

For the purposes of this guidance, a child is any person below 18 years of age.

Children aged under 5 years old are exempt from having to provide their fingerprints but must still provide a facial photograph. Facial photo should meet the HM Passport Office standards which are set out here: [Digital Image](#) and [Printed Image](#).

A responsible adult (RA) must be present when taking biometrics from anyone under the age of 16 unless the statutory reasonable belief exception applies. Those aged between 16 and 18 should have a RA provided if one is available, unless they choose not to have one. An RA may be:

- the child's parent
- the child's guardian
- a person who, for the time being, takes responsibility for the child, such as a Local Authority worker authorised to take charge of the child but who is not:
 - an officer of the Secretary of State, (who is not an authorised person)
 - an authorised person (see [Procedures for the taking of biometrics](#) for the definition of an authorised person)

If a 16–17- year-old declines an RA, officers must explain the safeguarding purpose of the RA, confirm the person understands this, and make a written record that:

- an RA was offered
- the person's decision to decline
- the explanation provided
- the officer's assessment that the refusal was voluntary, informed and presents no safeguarding concern

The RA's function is to observe the biometric process, communicate with the young person and ensure the process is safe. The RA does not represent the person in interviews or decision making. See the [Police 'appropriate adult scheme'](#), which sets out safeguards. This should be recorded on an IS86 form, the template for which can be found at the bottom of this document.

Age dispute

The purpose of this section is to help officers decide whether a RA is required for the purpose of taking biometrics. It is not a formal age assessment and does not determine a person's age for any other immigration, asylum or safeguarding purpose.

Previous age assessment

Where a person has previously been assessed as an adult (over 18) through a local authority Merton compliant age assessment or through the Assessing Age guidance, officers should normally treat that person as an adult for the purposes of biometric enrolment unless there is credible evidence to suggest the assessment should no longer be relied upon.

Reasonable belief

Reasonable belief is a decision made on the age of a person based on the information available to officers at the point they are dealing with the person, and it is not intended to be a formal age assessment. Any decision based on reasonable belief for the purposes of taking biometrics forms no part of the decision making when conducting an age assessment for other purposes, for example, asylum. It is solely for the purpose to enable officers to decide whether they need a RA present while the person is having their biometrics taken. Reasonable belief should be fair, with regard to the circumstances and based on observations and facts that can be evaluated by other people (such as another officer, senior officer, or child safeguarding officer).

Where a person is known, or reasonably believed, to be aged 16 or over, officers may take their biometrics without a RA being present. A person aged 16 or 17 must first be offered a RA and may proceed without one only where they decline that support voluntarily and on an informed basis, in accordance with the safeguards above.

When officers encounter a person who claims to be either under 16 years old or over 16 years old, but officers have a reasonable belief that this claim is not the case, the officers must decide at the point of encounter whether a RA is required for biometric enrolment. This is a safeguarding measure intended to support the welfare of children and to ensure that biometric enrolment is conducted appropriately. Where officers are aware the person has previously had their age assessed in accordance with the Assessing Age guidance, they must take account of that assessment when exercising reasonable belief.

For the purposes of biometric enrolment, any individual believed to be under 16 **must** be treated as under 16, even if they claim to be an adult. This requirement is intended to provide additional safeguarding during the biometric enrolment process.

Where 2 officers reasonably believe that a person who claims to be a child is aged 18 or over for the purposes of biometric enrolment:

- they must continue to be treated as a child for all safeguarding and operational purposes, unless and until:
 - they are assessed to be an adult in accordance with the Assessing Age guidance even if their biometrics are obtained as if the person was an adult

Biometrics may only be taken without a RA where 2 officers must each consider the available information, and both conclude that the person is clearly aged 16 or over. A

chief immigration officer (CIO), who may also be one of the 2 officers, authorises proceeding without a RA being present. Where the person is aged under 16, any decision to take biometrics **must** be authorised by a CIO. The CIO does not need to be present to authorise the taking of biometrics without an RA, if another 2 officers believe the person is aged over 16.

When exercising reasonable belief, officers must have regard to:

- whether there is credible and clear documentary evidence to show the person's age
- whether the person gave a date of birth that would contradict any claimed age before being told about providing their biometrics
- the person's physical appearance and / or demeanour which very strongly suggests that they are not the age they are claiming to be

Officers must record in PRONTO:

- the information and observable indicators relied upon
- any date of birth statements made
- any documentary evidence considered
- the names of the 2 officers and times of their assessment
- the name and time of the CIO authorisation
- the reasoning for proceeding without a RA

The Assessing Age guidance sets out the policy and procedures that must be followed when those subject to immigration control, do not have sufficient evidence to demonstrate their age, and either their claim to be children is doubted or they claim to be adults but are suspected to be children. This includes guidance determining whether a person's physical appearance and demeanour very strongly suggests they are significantly over 18. Home Office systems must be updated to reflect this using the IS86 template.

Additional safeguards

The exception to this is for vulnerable persons who are reasonably believed to be over the age of 16, who require authorisation to have their biometrics taken and the presence of a RA, irrespective of age, in line with [Fingerprinting vulnerable adults guidance](#).

In most circumstances, force must not be used to take the fingerprints of a pregnant woman, child or young person under the age of 18. See also: [Use of force when taking fingerprints](#) and guidance on use of force and restraint.

The fingerprints of all asylum seekers over the age of 5 are routinely searched against the police database IDENT1, although the check requires this to be manually verified on livenesscan or cardscan at enrolment. If the search results in a positive match against the police database, an automatic email response will be sent to the generic mailbox associated with the location code used to enrol the biometrics onto IABS.

Officers must apply the above safeguards for all biometrics

In this policy, the taking of biometrics may only be excused in exceptional circumstances, as set out in the 'Who is excused section' of the biometric enrolment guidance.

Where a deferral of fingerprinting is made, arrangements must be made to fingerprint the child as soon as possible thereafter.

Related content

[Contents](#)

Taking of biometrics from vulnerable adults

For the purpose of this guidance, a vulnerable adult, is defined as a person:

‘who is or may be in need of community care services by reason of mental or other disability, age or illness; and who is or may be unable to take care of themselves, or unable to protect themselves against significant harm or exploitation’

In line with standard Home Office policy, a person is considered an adult once they reach 18 years of age.

While our legislation and codes do not cover the taking of biometrics from vulnerable adults for immigration purposes, officers are expected to take reasonable action, within their powers, to safeguard the rights of people who may be at risk.

As part of the Home Office duty of care towards vulnerable adults, it is policy to apply the same procedure when taking biometrics from vulnerable adults as when taking biometrics from children under 16 (and over the age of 5 for fingerprints).

Biometrics may not be taken from a vulnerable adult unless in the presence of an adult (18 years or older) who is that person’s parent or a family member, guardian, care worker or other person who, for the time being, takes responsibility for the care of that person. In the latter case, that person may not be a person authorised to take biometrics, see [procedures for taking biometrics](#).

Police ‘appropriate adult scheme’

The police maintain a local list of appropriate adults, and it may be possible to arrange for a person listed under the appropriate adult scheme to attend a local police station in the following circumstances:

- where a lone vulnerable adult or child is unexpectedly encountered during an enforcement operation and needs to have their biometrics taken for immigration purposes, in addition to an initial welfare interview being held at the local police station
- where the police have detained a vulnerable adult or child without Immigration Enforcement presence and inform the Home Office that there is an immigration interest and that person needs to have their biometrics taken for immigration purposes

See also the [‘Being an appropriate adult’ on GOV.UK](#).

Use of reasonable force when taking biometrics

For any of the biometric powers referenced in this guidance, you may, if necessary, use reasonable force.

However, immigration officers (IOs), constables, prison officers and contractors working in detention centres or short-term holding facilities must be trained in the use of force, they must only use it if the person has already been arrested or detained, and when using it they must only exercise their power in line with the Use of force guidance.

Only those IOs designated to exercise the existing power of arrest, and the powers of entry, search and seizure are suitably trained.

Trained officers must make every attempt to gain compliance of the person before exercising the use of reasonable force. The use of force must only be as far as necessary to obtain the fingerprints, and it must also always remain proportionate.

The use of force against the elderly, infirm, pregnant women or children must only be used in exceptional circumstances, specifically when the use of force will prevent the person from causing harm to themselves or to others. Please refer to the Use of Force guidance for more details.

Fingerprinting of corpses

Under no circumstances may officers agree to fingerprint corpses using a Mobile Biometric Device (MBD) or lend the equipment for police officers to use themselves.

Police officers who require postmortem prints to be checked against the IABS database must take them themselves, using ink and card or a police digital unit, and submit them to IFB. They must contact IFB before they submit the fingerprints.

Fingerprints: requests for expert statements

In cases where a person is suspected of having multiple identities, an expert statement may be required to confirm that suspicion, especially where the decision may be taken to prosecute.

For Immigration Tribunals where it is suspected an individual has multiple identities, you must make a request for an expert statement by email to IFB mailbox giving full details of all identities used by the suspect. IFB will arrange for fingerprint experts to prepare and forward to the relevant crime intelligence team expert witness statements for all prosecution cases. For statements which enter the criminal justice system, this will need to be completed by the prosecuting force.

Related content

[Contents](#)

Establishing identity with fingerprints and data sharing

This section tells Immigration Enforcement officers about the power to take fingerprints for identification purposes, use of a Mobile Biometric Device (MBD), how to record that fingerprints have been checked and who they may share fingerprint data with and the processes for doing so.

For general guidance and standards for sharing data with other agencies, see Data sharing in enforcement cases: standards of operational practice.

[Section 20 of the 1999 act](#) allows for information held by the police to be supplied to the Secretary of State for the purposes of immigration control. It has been agreed with the police that immigration officers can check the police fingerprint databases (IDENT1) for such purposes.

Fingerprints of foreign nationals routinely taken under the [1999 act](#) for immigration purposes must be searched through IDENT1 where one of the following criteria is met:

- anyone who has made an asylum claim in their own right
- a dependant, aged at least 5 years of age, of a person who has made an asylum claim
- anyone who has had an enforcement decision served on them (for example, service of a Notice of Liability)
- anyone who requires permission to enter and does not have it
- anyone who arrives at the border without a passport or other acceptable proof of identity,
- anyone who is required to enrol their biometric when granted immigration bail
- anyone who is arrested under paragraph 17 or detained under paragraph 16 of [Schedule 2 of the 1971 act](#)

The fingerprints of foreign nationals that can be checked under paragraph 18(2) of [schedule 2 of the 1971 act](#) because they are a person:

- who is detained under paragraph 16 of [schedule 2 of the 1971 act](#)
- is liable to be detained under paragraph 16 of [schedule 2 of the 1971 act](#)

can also be checked against the police fingerprint databases (IDENT1) under [section 20 of the 1999 act](#).

Official - sensitive: start of section

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

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

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

Official - sensitive: end of section

Five Country Conference (FCC) Data Sharing Protocol

[The Five Country Conference \(FCC\) Data Sharing Protocol](#) is an agreement between the UK, Australia, Canada, New Zealand and United States of America to share and match data in certain circumstances. See there for more information regarding the sharing of biometrics.

Related content

[Contents](#)

Storage of fingerprints

This page tells Immigration Enforcement officers how to store fingerprint data and their responsibility to keep the data secure.

All hardcopies of fingerprints must be sent to the Immigration Fingerprint Bureau (IFB). Originals or copies of prints must not be attached to the Home Office file.

If you find original or copies of prints attached to a file, you must send these to IFB in a sealed envelope for correct filing, enclosing a covering note explaining where they were found.

Biometrics taken under the 1971 act are primarily aimed at confirming a person's identity and should be deleted as soon as they are no longer needed. Where you intend to retain the biometrics, you should use the powers in the 1999 act and the 2021 Regulations, where appropriate. See [Taking fingerprints to establish identity](#).

Guidance on the usage and retention of biometric information is available at: [Retention and usage of biometric information](#).

Related content

[Contents](#)

Using Mobile Biometric Devices (MBD)

This page tells Immigration Enforcement officers about the use and storage of MBDs.

The guidance in this section must be followed as a matter of course and applied firmly but not rigidly. All decisions need to be made on a case-by-case basis so there is scope for departing from this guidance at officers' discretion in limited exceptional circumstances. Officers must not forget their obligation to act in a proportionate and reasonable way consistent with human rights principles.

Establishing identity is a key objective on enforcement operations, and a mobile fingerprint device, which is a form of MBD, allows for biometric checks to be completed, enhancing the quality of investigations. Biometric information allows officers to make more accurate and informed decisions about a person's identity and immigration status.

MBDs do not store fingerprints. Templates of fingerprints are transmitted to the Immigration Asylum Biometric System (IABS) database, and a search is made against existing records. A response is transmitted back to the unit indicating whether a possible match has been found. A fingerprint expert does not verify the results of these searches.

There are 2 typical scenarios in which a MBD can be used during an enforcement operation:

- [use of Mobile Biometric Devices \(MBD\): exploratory examination](#)
- [use of Mobile Biometric Devices \(MBD\): administrative interviews](#)

Use of Mobile Biometric Devices (MBD): exploratory examination

When officers arrive at any premises or location, they may seek the voluntary cooperation of members of the public to explore provisionally whether they are related to the immigration enquiry they are conducting. Officers must identify themselves and the purpose of their enquiry from the outset.

The general purpose of inviting people to cooperate with exploratory questioning (see Exploratory examination interviews) is to eliminate them from enquiries. As part of this exploratory examination, officers may, with the fully informed consent of the person concerned, use a MBDs to confirm the person's identity, where it has not been possible to use other means.

You must explain that:

- fingerprints will be checked against Home Office records to confirm their identity
- the person does not have to give their consent

- they can withdraw their consent until such time as the check is made
- the person's fingerprints will not be retained

Officers must fully record details of this consent in their digital pocket notebooks contained in PRONTO (police reporting and notebook organiser). (see Record keeping during enforcement visits).

Use of Mobile Biometric Devices (MBD): administrative interviews

If, because of an officer's initial enquiries, they have formed a reasonable suspicion that the person is liable to be detained as an immigration offender potentially liable for removal from the UK because they, for example (this is not an exhaustive list):

- cannot readily and easily confirm the person's identity to their satisfaction
- suspect the person has provided false information
- suspect the person has provided false documentation

officers may, as part of their administrative interview (see Administrative enforcement interviews), exercise a power to take reasonable steps to establish identity, including by fingerprinting, photographing or other means of measuring them.

Officers must attempt to use the mobile fingerprint device with the cooperation of the person, explaining fully the power to obtain fingerprints. Provided that the person has been, or is liable to be, arrested or detained, and the officers are designated to use reasonable force (see [Use of reasonable force when taking fingerprints](#)), officers may [use force](#) to obtain the fingerprints. Officers must include in their reports:

- their reasons for suspecting the person to be potentially liable for removal from the UK
- the fact that fingerprints will not be retained
- whether reasonable force was required to take the fingerprints

This will allow the person an opportunity to quickly eliminate themselves from further enquiries and give officers certainty as to their identity by checking against central records held about that person.

If necessary, officers may request the person accompanies them to a location where the mobile device can obtain the required signal and successfully send and receive information relating to the fingerprints; this is provided that the officer in charge (OIC) is informed and neither the officer taking the fingerprints or the rest of the team is put at risk as a result.

In all cases, officers must record the full circumstances of the request, including all checks and their results and the related transmission identifier, in their digital pocket notebooks contained in PRONTO (police reporting and notebook organiser) (see Record keeping during enforcement visits).

Officers must also record which [power](#) the fingerprint check was conducted under and details of any [use of force](#) and why they considered it to be reasonable at the time given the particular circumstances.

Where there is no match on the mobile fingerprint device, officers may continue with their investigations to confirm the person's identity and immigration status.

Security and safe storage of Mobile Biometric Devices (MBD)

Storage of units must be in line with the generic physical security guidance (see Clear desks and screens).

In addition, there are several security points that are specific to the MBDs:

- devices must be stored in a secure area or office when not in use
- every team must have a list recording all the units they hold
- each team must have a designated officer responsible for the equipment and updating the log
- the log must be checked at the end of every shift to account for all units
- the log must detail the movement of each device on operations, noting the officer responsible on the day
- passwords must not be visible under any circumstances; this includes not sticking passwords to units and not leaving them under workstation keyboards
- the devices must not be used in situations where theft or risk to personal safety is increased
- the devices must not be visible in any vehicle or left unattended in public places

Related content

[Contents](#)

Additional identity checks

This page tells Immigration Enforcement officers which additional Home Office systems can be checked for biographical details, to help determine a person's identity.

Official – sensitive: start of section

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

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

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

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

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

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

Additional checks

In cases of claimed British or Irish nationality where that identity cannot be established see: Common Travel Area and British nationality issues.

DVA (Data Validation Application) is the HM Passport Office database that can be searched in relation to a British national identity where a trace has not been found on the above systems or when there is suspicion of forged documents or imposters.

Once you have completed all checks, you must record this in PRONTO (see Record keeping during enforcement visits), together with any results received.

Related content

[Contents](#)

Document verification and forgeries

This page tells Immigration Enforcement officers what to do if they suspect encountered documents are fraudulent or forged.

Examination of documents

If you suspect identity documents or marriage certificates are forgeries, contact your local forgery expert in the first instance.

Official - sensitive: start of section

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

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

Official - sensitive: end of section

Related content

[Contents](#)

Related external links

[Public Register of Authentic travel and identity Documents Online \(PRADO\)](#)

Template: IS86

This section contains the IS86 template which must be completed and issued to the person when officers take their biometrics under Section 141 of the Immigration and Asylum Act 1999 and the Immigration (Collection, Use and Retention of Biometric Information and Related Amendments) Regulations 2021.

Official - sensitive: start of section

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

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

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

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

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

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

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

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

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

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

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

Official - sensitive: end of section

Related content

[Contents](#)