



Home Office

Disclosure and confidentiality of information in asylum claims

Version 2.0

Contents

Contents.....	2
About this guidance.....	4
Contacts	4
Clearance and publication	4
Changes from last version of this guidance	4
Introduction	5
Background	5
Policy intention.....	5
Application in respect of children.....	6
Safeguarding	7
Mental capacity	7
Signposting to support services	7
Relevant legislation	8
International conventions and treaties	8
The 1951 Refugee Convention.....	8
European legislation	8
UK legislation	8
Immigration Rules.....	10
Asylum claims: confidentiality	12
When do asylum claims enter the public domain	13
Asylum claims: supporting evidence.....	15
Foreign and Commonwealth and Development Office (FCDO) advice	15
Police reports	15
Document verification	15
Transfer of information between cases.....	17
Inappropriate disclosure: steps to take	19
Disclosure for appeals and Courts.....	20
Judicial Reviews	21
Other Courts.....	21
Family Court.....	21
Disclosure of information to other parties	23
Requests by the claimant (or their representatives or MP) for details about their own case	24
Routine enquiries	24
Non-routine requests.....	24

Pending prosecutions	24
Telephone requests	25
Right to work check	25
Police.....	25
Other government departments and local authorities.....	25
Foreign and Commonwealth and Development Office (FCDO).....	26
International organisations	26
Family tracing.....	27
Authorities in the claimant’s own country and other countries	27
Serious criminal charges.....	27
Disclosure of identity for re-documentation purposes.....	28

About this guidance

This guidance tells you about obtaining and handling information in asylum cases. It provides specific guidance on disclosure and confidentiality for asylum claims due to the potential risks to the claimant and their family if asylum information is not handled appropriately.

This guidance also applies when considering settlement protection or revocation to ensure that the UK's obligations under the Refugee Convention and European Convention on Human Rights (ECHR) are met where there is a continuing need for UK protection.

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 Asylum 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.

Clearance and publication

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

- version **2.0**
- published for Home Office staff on **26 August 2022**

Changes from last version of this guidance

- updated caselaw included under the Document verification and Family Court sections

Related content

[Contents](#)

Introduction

This guidance explains what you must consider when:

- obtaining information in relation to an asylum claim
- sharing information related to the asylum claimant

This instruction must be read in conjunction with the main asylum policy instructions, in particular:

- Assessing credibility and refugee status
- Asylum interviews
- Dependants and family members

and where relevant:

- Asylum screening and routing
- Processing children's asylum claims
- Family tracing
- Gender identity issues in the asylum claim
- Sexual identity issues in the asylum claim
- Exclusion (Article 1F) and Article 33(2) of the Refugee Convention

See asylum decision making guidance for further asylum instructions. You must also refer to the relevant country policy and information notes which include country specific guidance. For family and private life applications see family leave instructions.

Background

You are required to obtain information in order to carefully consider asylum claims and you must be aware of the confidentiality rights of those who seek asylum. Information received about an asylum claimant whilst processing their claim could put those concerned at risk if disclosed and so it must not be shared except in certain circumstances where there is a legitimate need to do so.

Policy intention

The policy intention in considering disclosure and confidentiality of information in asylum claims is to ensure that:

- legal obligations regarding what information can be obtained and shared in relation to asylum claims are understood, including what can be disclosed at appeal and to third parties
- the rights of those seeking asylum are respected and they are given the opportunity to disclose, at the earliest opportunity, all evidence relevant to their asylum claim

- proportionate and necessary information is obtained to carefully and sensitively consider all asylum claims

Application in respect of children

[Section 55 of the Borders, Citizenship and Immigration Act 2009](#) requires the Secretary of State to make arrangements for ensuring that immigration, asylum and nationality functions are discharged having regard to the need to safeguard and promote the welfare of children in the UK. The section 55 duty applies whether the child applies in their own right or as the dependant of a parent or guardian.

The statutory guidance, [Every Child Matters – Change for Children](#), sets out the key principles to take into account in all actions concerning children. All decisions must demonstrate that the child's best interests have been a primary (albeit not necessarily the only) consideration. Disclosure and confidentiality is one of the factors to take in account when working with a child and their family.

You must carefully and sensitively consider cases involving unaccompanied children and whether and when it is appropriate to share information, for example in the interests of safeguarding or family tracing. You must also be aware that there may be individual protection needs or safeguarding concerns for children who are part of a family seeking asylum. Therefore, depending on the individual circumstances, it may be appropriate to share information with third parties in the best interests of the child. You must be vigilant that a child may be at risk of harm and be prepared to refer cases immediately to the Asylum Safeguarding Hub for referral to a relevant safeguarding agency where child protection issues arise.

For further information, see also the Processing children's asylum claims instruction and Family Court section.

Related content

[Contents](#)

Safeguarding

You do not have to stop making the asylum decision whilst a safeguarding issue is investigated. However, you must speak to your senior caseworker to check whether service of the asylum decision is appropriate, or if the safeguarding issue needs to be considered together with the asylum claim. You must make a referral to the Asylum Safeguarding Hub in order for safeguarding staff to liaise with the statutory authorities.

If you become concerned that a claimant may be in danger, you need to take immediate action to ensure their safety. Where there are child welfare or protection concerns that may involve safeguarding issues within the family unit the case must be referred immediately to the Asylum Safeguarding Hub, who will refer the case to the relevant local authority. There is no requirement to obtain the consent of any adults involved as safeguarding the child is our primary responsibility. In an emergency the case must be referred to the police without delay. The Safeguarding Advice and Children's Champion (SACC) can also offer specialist safeguarding and welfare advice on issues relating to children, including family court proceedings and complex child protection cases.

There are some circumstances where consent is not needed from adults before sharing information with statutory authorities for safeguarding purposes, you should engage the Asylum Safeguarding Hub who can assess whether consent is needed before sharing.

This government guidance provides information for [safeguarding practitioners on information sharing](#).

Mental capacity

In situations where informed consent would be required from an adult claimant to share their information in relation to their asylum claim, it is important to consider if there are any exceptional circumstances which may mean they would be unable to provide informed consent, for example due to, but not limited to, a disability, being detained under the [Mental Capacity Act 2005](#) or if they lack capacity to make such a decision. You must engage the Asylum Safeguarding Hub in these situations.

Signposting to support services

The asylum claimant receives the [information leaflet for asylum applications](#) which includes information on support services and you can refer them to the contacts for appropriate support which are detailed in this leaflet.

Related content

[Contents](#)

Relevant legislation

International conventions and treaties

The 1951 Refugee Convention

The [Refugee Convention](#) provides the framework for international refugee protection. It has been supplemented by the progressive development of international human rights law, and in the European Union (EU) by a subsidiary protection regime.

European legislation

This is for background information only – following the UK's exit from the European Union, the UK is no longer bound by the following directives but relevant aspects have been transposed into UK law, see [UK legislation](#) and [Immigration Rules](#), in particular Immigration Rule 339IA.

The [Council Directive 2004/83/EC \(the Qualification Directive\)](#) lays down provisions and criteria for interpreting the Refugee Convention to be adopted across the EU. It has been transposed into UK law through [The Refugee or Person in Need of International Protection \(Qualification\) Regulations 2006](#) and the [Immigration Rules](#). The Qualification Directive article most relevant to this instruction is:

- Article 36 which concerns the confidentiality principle

[Council Directive 2005/85/EC](#) (the Procedures Directive) sets minimum standards for Member States for granting and withdrawing refugee status and has been transposed into UK law via the [Asylum \(Procedures\) Regulations 2007](#) and the [Immigration Rules](#). The Procedures Directive articles most relevant to this instruction are:

- Article 22 Collection of information on individual cases
- Article 41 Confidentiality

UK legislation

Every person has data protection rights under UK law. The law does not prevent the sharing of sensitive, personal information either within or between organisations when there is a legitimate need to share this data, as set out in data protection legislation.

The common law duty of confidentiality is an important principle of UK law which enables people to feel safe in sharing their concerns and asking for help. The common law duty of confidentiality recognises that some information has a quality of confidence, which means that the individual or organisation that provided the information has an expectation that it will not be shared with, or disclosed to, others.

It is generally accepted that information has a quality of confidence if it: is not 'trivial' in its nature; is not in the public domain or easily available from another source; has a degree of sensitivity; and has been communicated for a limited purpose and in circumstances where the individual or organisation is likely to assume an obligation of confidence - for example, information shared between: a solicitor and their client, or a health practitioner and their patient.

However, the right to confidentiality is not absolute. The law permits the disclosure of confidential information where there is an overriding public interest or lawful justification for doing so, for example, for child protection or the prevention of crime.

Domestic courts have also recognised that a duty of confidence under common law is owed to a person claiming asylum in respect of the information they provide in support of their claim. In particular, the courts have recognised that the confidentiality of the asylum process is intrinsic to the operation of both the asylum system generally and the proper discharge by the UK of its obligations under the Refugee Convention. See in particular, [F v M and another \(Joint Council for the Welfare of Immigrants intervening\) \[2017\] EWHC 949 \(Fam\)](#), and [Re H \(a child\) \[2020\] EWCA 1001](#).

The [Human Rights Act 1998](#) (HRA) gives effect in UK law to the human rights set out in the European Convention on Human Rights (ECHR) and applies to everyone in the UK regardless of their immigration status. Under section 6(1) of the HRA, a public authority is bound to act in a way which is compatible with the ECHR. Under Article 8, any consideration of the ECHR must take into account, not only the potential impact of disclosure on the individual but also the potential consequences for their family members.

Article 8(1) of the ECHR states that 'Everyone has the right to respect for his private and family life, his home and his correspondence.' However, Article 8 is a qualified right, rather than an absolute right, and Article 8(2) states:

There should be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

When making a decision to disclose information on an individual, you must have regard in every case to Article 2 (right to life), Article 3 (prohibition of torture or inhuman or degrading treatment or punishment) and Article 4 (prohibition of slavery and forced labour). These are unqualified rights and you will need to consider whether any of these rights would be engaged as a result of the disclosure of this information.

The [Data Protection Act 2018](#) (DPA) achieved Royal Assent on 23 May 2018. It replaced the Data Protection Act 1998 updating data protection laws for the digital age. The DPA applied the EU General Data Protection Regulation (GDPR) standards. The DPA is a complete data protection system and includes a number of agreed modifications to the GDPR to make it work for the UK. The [Borders](#),

[immigration and citizenship: Privacy Information Notice](#) reflects individuals' rights under data protection legislation including the DPA and states how the Home Office looks after and uses personal information within the borders, immigration and citizenship system. It also explains how individuals can request a copy of their information.

In principle, you could be personally liable to prosecution for breaches of data protection legislation. However, you will not commit an offence where you act in good faith and follow this guidance on disclosure and confidentiality. If disclosure made in accordance with published guidance is later found to be in breach of the data protection legislation, the Home Office will be the subject of enforcement action not individual members of staff.

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

The [Freedom of Information Act 2000](#) (FOIA) took effect on 1 January 2005 but does not affect the rights of an asylum claimant to access their personal data. The FOIA defers to the DPA in the area of Subject Access Requests. The FOIA does not give individuals who are not connected to a case the right to access personal information held in an asylum claimant's immigration records. Information may be provided, though not through access to personal records, on general asylum issues (for example on government policy or process), subject to the exemptions laid down in the FOIA.

Immigration Rules

[Part 11 of the Immigration Rules](#) sets out the provisions for considering asylum claims and reflects our obligations under the Refugee Convention and the ECHR.

[Paragraph 339IA of the Immigration Rules](#) transposed Article 22 of [Council Directive 2005/85/EC](#) (the Procedures Directive) into UK law and states:

For the purposes of examining individual applications for asylum

- (i) information provided in support of an application and the fact that an application has been made shall not be disclosed to the alleged actor(s) of persecution of the applicant, and
- (ii) information shall not be obtained from the alleged actor(s) of persecution that would result in their being directly informed that an application for asylum has been made by the applicant in question and would jeopardise the physical integrity of the applicant and their dependants, or the liberty and security of their family members still living in the country of origin.

This paragraph shall also apply where the Secretary of State is considering revoking a person's refugee status in accordance with these rules.

Related content

[Contents](#)

Asylum claims: confidentiality

This section tells you about the statement of confidentiality that is provided to the asylum claimant and what this means in terms of treating information in confidence and when disclosure is appropriate.

When asylum claims are made, the claimant is informed that we may share certain information but that their own country, from whom they are claiming they are fleeing persecution from, will not be informed about their asylum claim and no information will be shared that would put them or their family at risk. This is the statement that is provided to the asylum claimant:

Your information may be shared with other UK government departments or agencies including the National Health Service, local authorities, asylum authorities of other countries, international organisations and other bodies. Any information shared is to enable us and other organisations to carry out functions, including the prevention and detection of crime. If another country has responsibility for considering your claim you will be informed.

We will not inform your own country that you have claimed asylum or the reasons. We will not share any information if doing so would put you or your family at risk. However we may share some of the information you have given us with them. For example, to help us get travel documentation if your claim is refused.

The fact that this statement has been made is documented on the initial contact and asylum registration questionnaire (also known as the screening questionnaire). This questionnaire also says where the claimant can find the Privacy Information Notice:

The [Data Protection Act 2018](#) governs how we use personal data. For details of how we will use your personal information and who we may share it with please see our Privacy Notice for the Border, Immigration and Citizenship system at <https://www.gov.uk/government/publications/personal-information-use-in-borders-immigration-and-citizenship>. This also explains your key rights under the 2018 Act, how you can access your personal information and how to complain if you have concerns.

You must treat all information provided by a claimant in support of their asylum claim in confidence and in accordance with [legislation](#). Data protection applies to all living people. If a claimant has died since making their asylum claim, data protection provisions may no longer apply. However, we must continue to ensure that any personal information about other living family members is treated in line with data protection legislation, and that family members are not put at risk in breach of [Immigration Rule 339IA](#). If you are unsure about what information you can legitimately share you must refer to a senior caseworker.

The UNHCR has published an [Advisory Opinion](#) on the rules of confidentiality regarding asylum information. It sets out the principles of confidentiality in asylum claims and stresses the importance of these principles. The following summarises relevant points of the UNHCR advisory opinion to be aware of:

(paragraph 2): Effective measures need to be taken to ensure that information concerning a person's private life does not reach the hands of third parties that might use such information for purposes incompatible with international human rights law.

(paragraphs 4 and 5): The right to privacy and its confidentiality requirements are especially important for an asylum-seeker, whose claim inherently supposes a fear of persecution by the authorities of the country of origin and whose situation can be jeopardized if protection of information is not ensured. It would be against the spirit of the 1951 Convention to share personal data or any other information relating to asylum seekers with the authorities of the country of origin until a final rejection of the asylum claim.

(paragraph 5): Bearing these concerns in mind, the State that receives and assesses an asylum request must refrain from sharing any information with the authorities of the country of origin and indeed from informing the authorities in the country of origin that a national has presented an asylum claim.

(paragraph 8): The authorities must therefore seek in advance the written consent of asylum seekers to check their personal data in the country of origin.

(paragraph 10): There may also be questions as to whether the confidentiality requirements continue to apply in situations where an asylum-seeker has voluntarily disclosed his or her identity and the fact that s/he has sought asylum through statements to the media. In UNHCR's view, while there might be a possibility that such information has come to the knowledge of the country of origin, this may not be interpreted as an explicit waiver of confidentiality. The country of asylum remains bound by the principle of confidentiality and personal data on the individual asylum claim must not be disclosed to the country of origin.

(paragraph 14): Overall, it would be against the spirit of the 1951 Convention to share personal data or any other information relating to asylum-seekers with the authorities of the country of origin.

When do asylum claims enter the public domain

Appeals against the refusal of asylum are usually heard in an open appeal hearing. All matters discussed in open court, which are likely to include the appellant's basis of claim and any representations made by the different parties to the appeal (for example those presenting the appeal, representatives of the claimant, expert witnesses) are considered to have entered the public domain during the hearing. As the matters discussed in open court have entered the public domain they can, where relevant, be included in decisions (including the Reasons for refusal letter) of other claimants, for example where the case reasoning is the same.

In cases where claims for asylum have been refused and the Appellate Authority have upheld the decision, this information can usually be considered to be in the public domain and therefore to that extent is no longer covered by our obligations of confidentiality. However, you must consider whether the disclosure of that information is necessary in the light of the enquiry received. If you have any doubts

about whether or not information should be given you must seek advice from a senior caseworker.

Determinations which have been reported are also considered to be in the public domain (determinations which have not been reported are not public documents). They may contain information which is relevant to other asylum claims and, in these circumstances, they can be referred to in a decision letter. Case law can be used in decision letters where relevant and in accordance with relevant Asylum policy guidance and country policy and information notes.

If an appeal is outstanding, but has not yet been heard, details about the case are not in the public domain and no reference to that claim can be made in a decision letter relating to other claims.

If an appeal is heard 'in camera', the evidence is heard in a closed court which is not open to the public. This means that the matter has not passed into the public domain and details of those claims must not be disclosed or mentioned in relation to other cases, as the information will still be protected by our obligations of confidentiality - unless there are specific facts that justify the disclosure under overriding public interest or lawful justification. When an appeal has been heard 'in camera' this will normally be noted on the determination. Any request for this information should be considered under the Freedom of Information Act 2000 (FOIA) but in such cases it may be appropriate to rely on exemptions of the FOIA. There will also be cases where the court or tribunal orders anonymity and this must be abided by. Breaching an anonymity order is a contempt of court. Therefore, if information covered by an anonymity order needs to be disclosed an application would have to be made to the Court for the order to be lifted.

An asylum claimant may choose to make details of their own asylum claims public before their appeal has been heard, for example to make allegations in the press about the way the Home Office has considered their claims. Publication of details relating to claims may lead to interest from other media outlets and attract the attention of MPs, members of the public and interested stakeholders. Usually it is inappropriate for the Home Office to comment on individual cases. However, in these circumstances, and only in response to individual inquiries, the Home Office may be able to give information to set the record straight and to prevent unfounded rumours from spreading. If you are contacted by a media outlet, care must be taken to avoid being drawn into any discussion on the specifics of a case or the details of allegations or statements made in the media. You must always direct them to contact the Home Office Press Office. Journalists should be directed to call 0300 123 3535 and you should notify the Press Office to make them aware of this.

Related content

[Contents](#)

Related external link

[Policy on the Protection of Personal Data of Persons of Concern to UNHCR](#)

Asylum claims: supporting evidence

This section tells you about handling supporting evidence and disclosure of information in asylum cases and decision letters.

You must refer to the Assessing credibility and refugee status instruction, in particular the section on Obtaining evidence and the relevant country policy and information notes.

You must ensure that only relevant and disclosable information is used in asylum decision letters. For example, police interviewing officers and MPs must not be referred to by name in asylum decision letters.

Foreign and Commonwealth and Development Office (FCDO) advice

Evidence provided by the FCDO which is used in deciding asylum claims will normally be provided in the form of a disclosable letter which can be referenced in the decision letter. If there is any doubt, the FCDO must be consulted before using their evidence in the letter.

Police reports

Information contained in police reports may be paraphrased for inclusion in the decision letter. A police force's interviewing officers must not be mentioned by name. It is important to accurately record the details (including any relevant dates) and particular care must be exercised when interpreting the sequence of events outlined in police reports. The appropriate wording for incorporating such information in a decision letter is "The police informed the Home Office that...". You must bear in mind that evidence relied upon in the decision letter will probably have to be disclosed if there is an appeal. The Tribunal has arrangements for handling sensitive evidence, and it is for the judge, not the Home Office, to decide whether or not they apply in the particular case.

Document verification

When you are considering the weight to be attached to an overseas document it is for the claimant to show that those documents can be relied on (as established in [Tanveer Ahmed v Secretary of State for the Home Department \(Pakistan\) UKIAT 000439 \(19 February 2002\)](#)). To assert that a document is a forgery shifts the burden of proof to you as the decision maker. See the Assessing credibility and refugee status for details on which types of evidence this principle applies to and for the guidance to be followed on obtaining and considering evidence.

You must check relevant country policy and information notes for available information on country specific documents. The Asylum screening and routing instruction provides guidance on security checks, travel document and identity verification. There is also guidance available on Biometric data-sharing.

Any document verification must not breach our obligations under [Immigration Rule 339IA](#). You must ensure that no personal information about an asylum claimant is shared with the authorities in their country of origin without written consent of the claimant. There must also be no direct contact with the alleged actor of persecution in the country of origin in a manner that might alert them to the likelihood that a protection claim has been made, or in a manner that might place the claimant or their family members in the country of origin at risk.

You must take into account the caselaw in [VT Sri Lanka \(Article 22 Procedures Directive; confidentiality\) \[2017\] UKUT 368](#) when considering whether document verification is necessary (this judgment referred to Article 22 of the Procedures Directive which is transposed into UK law in Immigration Rule 339IA):

- (i) There is no general duty of inquiry upon the examiner to authenticate documents produced in support of a protection claim. There may be exceptional situations when a document can be authenticated by a simple process of inquiry which will conclusively resolve the authenticity and reliability of a document.
- (ii) There is a general duty of confidentiality during the process of examining a protection claim, including appellate and judicial review proceedings. If it is considered necessary to make an inquiry in the country of origin the country of asylum must obtain the applicant's written consent. Disclosure of confidential information without consent is only justified in limited and exceptional circumstances, such as combating terrorism.
- (iii) The humanitarian principles underpinning Article 22 of the Procedures Directive prohibit direct contact with the alleged actor of persecution in the country of origin in a manner that might alert them to the likelihood that a protection claim has been made or in a manner that might place applicants or their family members in the country of origin at risk.
- (iv) The humanitarian objective of the Refugee Convention requires anyone seeking to authenticate a document produced in support of a protection claim to follow a precautionary approach. Careful consideration should be given to the duty of confidentiality, to whether an inquiry is necessary, to whether there is a safer alternative and whether the inquiry is made in a way that does not give rise to additional protection issues for applicants or their family members. Disclosure of personal information should go no further than is strictly necessary. Whether an inquiry is necessary and is carried out in an appropriate way will depend on the facts of the case and the circumstances in the country of origin.
- (v) Failure to comply with the duty of confidentiality or a breach of the prohibitions contained in Article 22 does not automatically lead to recognition as a refugee, but might be relevant to the overall assessment of risk on return.

Further to VT Sri Lanka, [PA Bangladesh \(Respondent's enquiries, Bias\) \[2018\] UKUT 337](#) clarified, at paragraph 55, that consent is not a legal necessity in all circumstances and that Immigration Rule 339IA (which transposed Article 22 into the

Immigration Rules) can still be breached even where consent is given. The legal obligations that prohibit enquiries being conducted in a manner that would result in alleged persecutors being informed of asylum claims also apply where consent is obtained.

If document verification is considered necessary, then overseas officers must ensure that no personal details are shared. Verification must be carried out by the overseas officers simply introducing themselves as being from the British High Commission and they must not take any identifiable paperwork with them. Overseas officers must ask to see the records from the courts rather than the police if the authorities are the alleged actors of persecution. Overseas officers must ensure that any computer checks which are made do not enable the claimant or their family to be identified or traced.

The Assessing credibility and refugee status guidance must be followed with regards to obtaining evidence. The section on documentary evidence includes that you should be aware of [QC \(verification of documents; Mibanga duty\) \[2021\] UKUT 33 \(IAC\)](#), which advises there are certain limited circumstances where you are required to make enquiries to verify the authenticity of a document. However, this requirement will only arise in exceptional circumstances where all of the following apply:

- • the document forms a central part of the claim
- • the document can be easily authenticated (taking into consideration issues such as costs and technical and logistical concerns)
- • the authentication is unlikely to leave any “live” issue as to the reliability of its contents

This duty to authenticate a document will therefore arise rarely and if you need further advice on whether to consider making further enquiries you should consult a SCW for advice.

For information on document verification checks in cases where false documents have been submitted in support of an application for entry clearance, leave to enter or leave to remain see the Document verification checks guidance.

Redocumentation for removal purposes is separate from document verification and is covered in the Returns Logistics guidance.

Social media

Any social media checks must only be carried by those who have received specialist training and have access to the appropriate units for undertaking social media investigation. This is to avoid placing those undertaking any investigations at risk (for example by inappropriately using or revealing their own personal details during a check), as well as the claimant and their family.

Transfer of information between cases

When dealing with asylum claims, for example in interviews, decisions or other communications, you must not refer to information provided in confidence by other claimants unless: informed consent has been given by the relevant claimant to whom the information belongs for that information to be shared, or the information is already in the public domain or is available in other disclosable sources (in which case you must rely on those sources alone) and in each case the information must be relevant to the claim in question.

This applies even where details which specifically allow the other person to be identified are left out. This also applies to claimants who are related but have made separate asylum claims.

Informed consent requires an individual's freely given and explicit consent for a specific piece of information to be used for a specific, known purpose. For consent to be informed, the individual must have been made aware of the risks involved in giving consent as well as the consequences of not giving consent.

These principles also apply to claimants who are related but have made separate asylum claims. There may be cases where the accounts of family members differ or even contradict one another. It is nevertheless inappropriate to disclose information relating to other family members' claims as sharing of any information could potentially put family members at risk of harm.

In terms of providing informed consent to share information, you should be aware that family members may have legitimate reasons not to consent to information being disclosed, such as a fear of abuse, so careful consideration needs to be given to the evidence before citing failure to give consent as a credibility issue.

A claimant, whilst applying in their own right, may seek to rely on the details given in family members' claims which are not in the public domain. In this situation, the claimant must give their own account of events relevant to their claim unless either informed consent has been given by the other family member for their information to be used, or that information is available in other disclosable sources.

Where a dependant later decides to claim asylum in their own right, no mention must be made to them of details from the earlier asylum claim where they are not already aware of this information. Information from the earlier claim which is not in the public domain must not be referred to in the decision letter. This applies even where there are clear discrepancies. Although not strictly a third party to the original claim, dependants are not asked to confirm the main claimant's account and so discrepancies do not necessarily indicate dishonesty on the part of the former dependant. Dependants are not necessarily aware of the details given by main claimant and our undertaking not to disclose such information to third parties in this instance extends to dependants. See Dependants guidance for further information.

Related content

[Contents](#)

Inappropriate disclosure: steps to take

This section tells you about what steps to take if it comes to light that information disclosed or relied upon as part of the decision-making process should not have been disclosed.

It is important to ascertain that the information was wrongly used and had not, in fact, entered the public domain through another channel.

If the information was incorrectly disclosed, then you must not continue to rely on that information. The case must be reviewed to ensure that the decision will stand without the non-disclosable information and whether further consideration or investigation is necessary.

If you consider that the decision will stand then the decision letter must be amended to remove the incorrectly disclosed information. The revised decision letter should be dated as the date of the new revised letter and not the date of the original letter. A covering letter must be sent with the amended decision letter making it clear that the original decision still stands. The amended decision letter does not have to follow the original. It can strengthen existing arguments and refer to information received after the original decision was made, if this is relevant.

If you consider that the decision will not stand without the non-disclosable information, then you must refer to a Senior Caseworker and carefully consider whether to make further enquiries.

Where cases have already reached the appeals stage when it comes to light that information disclosed, or relied upon as part of the decision-making process, should not have been disclosed, the Withdrawing decisions guidance must be followed.

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

Related content

[Contents](#)

Disclosure for appeals and Courts

This section tells you about disclosure of information for asylum appeals, Judicial Reviews, other Courts requesting asylum information and provides links to further guidance to be followed.

When making asylum decisions you must consider not only that the information you are including will be seen by the claimant and their representative, but also that asylum decision letters may enter the public domain if decisions are appealed. As evidence used to make the decision would be required by the Court for considering the appeal against the asylum decision, it is important to consider how information is used, as generally information relied on when making asylum decisions must be disclosable in appeals and Judicial Reviews. For example:

- some evidence used in decision making will already be in the public domain for example:
 - country information which is published on GOV.UK is disclosable - see the [Assessing credibility and refugee status and country policy and information notes](#) for further details on using country information
- other information obtained as part of the asylum claims or provided by the claimant may need to be redacted accordingly for example:
 - to remove individuals' personal details and contact information
- information which forms part of the case file but which is not relevant to the matters in the decision must not be disclosed, for example:
 - particular care must be taken in respect of any Border Force reports which may contain information that is operationally sensitive or personal information about the claimant's travelling companions, for example, which will itself be subject to exemption from disclosure under the Data Protection Act
- visa application information must be considered as part of any asylum decision, in line with all other information:
 - the visa match may not be determinative or significant in every case, but it must be mentioned in any grant minute or refusal letter when addressing the immigration history and or credibility issues, see [Visa match guidance](#) for further information concerning disclosure in decisions and appeals

If you have any doubt whether to include certain information in asylum decisions, you must seek senior caseworker advice and authorisation or consent, where appropriate, from the source of the information.

An appellant is entitled to know the case against them, and the Home Office will usually be expected to disclose any and all documents on which the decision under challenge is based. Appeal hearings are normally open to the public so particular care must be taken not to include any information which is not for public disclosure, for example information provided to the Home Office in confidence which the provider has not consented to disclose. Any disclosure of such information could be unlawful under the [Data Protection Act 2018](#). The courts and tribunals can make special arrangements for dealing with sensitive information, but this is at the discretion of the judge. If you have information which is essential to your decision but

which you cannot disclose, you should discuss your options with a senior caseworker or presenting officer or contact appeals policy.

Pro-formas (PF1) and supporting documents, including the Reasons for Refusal Letter (RFRL), are generated by the Home Office and made available to the Immigration and Asylum Chamber (IAC), the appellant and their legal representative. They may also be provided to UNHCR where they have given notice that they wish to participate in the appeal. See Appeal bundles guidance for further information and details on what to include in the appeal bundles. Generally, if information can be relied on when making an asylum decision, you should be able to disclose it at appeal and not withhold evidence.

Judicial Reviews

In the course of judicial review proceedings please see [Administrative Court judicial review guide](#) for guidance on duty of candour and disclosure.

Other Courts

There are instances when a court may order disclosure of information related to asylum claims. The bar to disclosure arising from [Immigration Rule 339IA](#) applies only in respect of an alleged actor of persecution. Therefore, this and the domestic law of confidentiality do not prohibit disclosure of information from pending asylum claims where a court order requires it. Court Orders must be complied with unless the issue of Public Interest Immunity (PII) arises. A claim for PII invites the court to conduct a balancing exercise between two competing public interests - the public interest that, in the fair administration of justice, the courts should have the fullest possible access to all relevant material; and the need to maintain the confidentiality of information whose disclosure would be damaging to the public interest. The PII process is not applicable in circumstances where the Secretary of State is not a party to the proceedings and the asylum seeker or refugee who is a party has access to, or can request as of right, the relevant documents from the Secretary of State. In some cases, a closed rather than open judgment will be appropriate.

Family Court

In family proceedings, while the context will differ from case to case, as will the status of any asylum claims, [Re H \(a child\) \[2020\] EWCA 1001](#) is now the starting point for any question of disclosure of asylum records in family proceedings, setting out the procedure to be adopted and the test to be applied. Where there is an application for the disclosure of asylum documents from the Secretary of State directly, you must seek appropriate legal advice (if these applications are received outside of litigation casework units you must refer to your senior caseworker). It is possible for such disclosure to be made directly by the party who claimed asylum, meaning that the Secretary of State does not have to take an active role, as the asylum claimant will be able to share the information themselves.

Where there is an ongoing asylum claim, the Court of Appeal in *Re H* stated that 'absolute confidentiality' applies and disclosure to an alleged persecutor cannot be

ordered (see Phillips LJ at section 58 and Peter Jackson LJ at section 68(3)). However, the UK Supreme Court (UKSC) in [G \(Appellant\) v G \(Respondent\) \(UKSC 2020/0191\)](#) departed from this position, stating that Article 22 and Immigration Rule 339IA 'do not prevent a court from ordering disclosure nor is it necessary to postpone disclosure until the asylum process has concluded' (para 170). The UKSC did, though, still approve the 'balancing exercise' outlined in Re H (a Child) to be undertaken to decide whether to order disclosure. The UKSC also noted that 'In carrying out the balancing exercise a relevant factor will be whether the left-behind parent in the 1980 Hague Convention proceedings is "the alleged [actor] of persecution of the applicant for asylum"' (paragraph 171). This is a factor which will mitigate against disclosure (to the alleged persecutor) and tip the scales towards confidentiality.

The procedure to be adopted on application for disclosure from asylum files is that set out in [Family Procedure Rules 21.3](#). That means that the first question is one of relevance: are the documents potentially relevant to the issues the court has to determine? This is a low threshold, since the issue of relevance is primarily a matter for the court not for the Secretary of State. A detailed examination of the issue of relevance is not required at this stage, but at least some connection to the issues must be established. You must ensure when requested to disclosure information, that the only minimum information necessary is provided. For example, initially this may simply be to confirm that an asylum claim has been made and then, if ordered by the court, provide other basic aspects such as dates and whether any dependants have the same protection needs. It will depend on the case whether minimal information is sufficient or whether further will be ordered by the court.

The Family Court may carry out a balancing exercise to determine whether asylum information should be disclosed. The way the court applies the balancing exercise will vary depending on the nature of the family proceedings, and the status and details of the asylum claims but should be conducted by reference to rights under the European Convention on Human Rights (ECHR). The best interests of the child are also, as always in Children Act 1989 proceedings, a paramount consideration (Children Act proceedings differ to [Section 55 of the Borders, Citizenship and Immigration Act 2009](#), see [Application in respect of children](#)). It is for the court, not the Secretary of State, to conduct the balancing exercise but those acting on behalf of the Secretary of State will be required to make appropriate redactions to reduce the harm to the public interests and rights involved, as well as for personal data reasons.

You must not use any Family Court documents or information unless there is express consent from the Family Court. Reference to or use of any information without consent could amount to a contempt of court and potentially constitute a criminal offence. See Appeal bundles guidance.

Where there are concurrent asylum claims and 1980 Hague Convention proceedings, you must follow the Operating instruction on Hague Convention cases.

Related content

[Contents](#)

Disclosure of information to other parties

This section tells you how to handle requests from a claimant and others on their behalf, and how to approach sharing information with public bodies, international organisations and other countries.

Given the very nature of claims for asylum, in many cases it would be contrary to the public interest to reveal details of claimant's asylum claims as it could put them and or their family at risk. In any event, in many instances a sufficient degree of information can be disclosed to satisfy the enquirer without revealing that the individual has claimed asylum.

There will be some instances when information can be shared with certain public bodies where they have a legitimate reason to request the immigration status of an individual for example:

- the NHS to assist in determining whether or not an individual should be liable to charging for treatment
- local authorities and Department for Work and Pensions to establish benefit entitlement
- the police for crime prevention and detection purposes

When information is disclosed to other public bodies for a legitimate reason in order to enable them to carry out their functions, only the required information must be shared, going no further than is strictly necessary, and the disclosure must not breach our obligations under data protection legislation and our duty of confidentiality. The information remains confidential and it must be made clear that it is not to be further disclosed without first obtaining prior consent from the Home Office (this consent does not need to be sought when the information is required to be disclosed as part of a Subject Access Request). Where the sharing of personal data is for a legitimate purpose and government function it would meet the lawful basis of being shared for public task, as set out in the relevant data protection legislation. It must, though, be ensured that what is provided is proportionate to the stated aim.

In the majority of pre-appeal cases where the asylum claims are still under consideration, our obligations of confidentiality will usually prevent disclosure to a non-public body. The only exception is where there is an overriding public interest in the disclosure on the facts of the particular case, for example where the disclosure is necessary for the purposes of safeguarding national security, or where the disclosure is required in legal proceedings. If you have any doubts about whether or what information should be disclosed, you must seek advice from your senior caseworker.

All requests for personal data which are not from the data subject (individual) should be considered in line with the Freedom of Information Act 2000 (FOIA). For many requests, it may be appropriate to refuse disclosure under FOIA exemptions.

Where FOIA exemptions are not relevant, you must consider whether sharing information is prohibited under data protection legislation (DPA). Under the DPA, the Home Office must have a specific legal basis to share any personal data. If in doubt, you must seek advice from your senior caseworker and data protection lead.

Requests by the claimant (or their representatives or MP) for details about their own case

All individuals have the right to access personal data held on them under data protection legislation. Information about Subject Access Requests is publicly available on [GOV.UK](https://www.gov.uk).

You must ensure that information management standards are followed when managing information and documents.

Routine enquiries

Routine enquiries from a claimant about the progress of their case or requests for copies of correspondence or interview records must be responded to. You can disclose the requested information if it is clear that the request has come from the claimant. If the request comes from representatives or MPs, you must be sure that they are acting on behalf of the claimant. Any request made by a person claiming to act on behalf of an asylum claimant must be accompanied by authorisation from the claimant where we have not previously been made aware that they have permission to act on behalf of the claimant.

Non-routine requests

Non-routine requests, for example when a claimant asks for all personal data on our files or every minute sheet in which their name is mentioned, are considered to be Subject Access Requests under the data protection legislation and must be referred to the relevant Subject Access Request Unit.

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

Pending prosecutions

You may be asked the reason for delay in cases where asylum claims are awaiting the outcome of pending prosecutions prior to deciding the case. Where the claimant is aware of their pending prosecutions, this reason for delay in decision making may be shared with them, their legal representatives and the Courts in line with data protection legislation, see Pending prosecutions guidance.

Telephone requests

You must not generally disclose information in response to a telephone call. You must ask the caller to put the request in writing unless the caller is the claimant or their representatives (including MPs). The claimant or their representatives must not be given any information about the case until the caller's identity has been established beyond reasonable doubt.

For requests received from other government departments or third parties, again you must ensure you are confident of the caller's identity and that they are entitled to receive the requested information.

You must be aware that your calls may be recorded and that these recordings could be used in legal representations.

Right to work check

If you receive a request from a potential employer for confirmation that a claimant has permission to work, you must refer them to the [Employers Checking Service](#), which is publicly available on GOV.UK.

Police

You may disclose a claimant's immigration status to the police when the information is required for police investigations. Where an enquiry is not received via Status Verification, Enquiries and Checking (SVEC) it must be ensured that the enquirer is genuine, and records must be clearly minuted with the name, rank, location and telephone number of the enquirer.

Details of asylum claims must not be passed to the police without senior caseworker approval, and no more details than are necessary for the police investigation must ever be disclosed. Requests for copies of documents from Home Office files from the police or other government bodies are usually dealt with by SVEC (which is part of Immigration Checking and Enquiry Services) as they will be aware of Memorandums of Understanding or disclosure agreements.

Other government departments and local authorities

A number of government departments, local authorities, housing and social services departments may have a legitimate interest in the information contained in Home Office case files. HM Revenue and Customs and the Department for Work and Pensions, for example, are routinely forwarded relevant personal details of recognised refugees and those granted Humanitarian Protection or Discretionary Leave so that they can use these to issue National Insurance numbers. When another government department requests information that is necessary for it to be able to carry out its functions, disclosure is usually permitted.

Other government departments are unlikely to contact you directly. However, in the event that a request for information is received, advice must be sought from SVEC

who act as the central point of contact and can advise on disclosing information to other government departments.

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

Foreign and Commonwealth and Development Office (FCDO)

You must ensure that care is taken when passing personal information about refugees, asylum seekers or their families to posts abroad. Information must only be passed via secure means to those in FCDO posts abroad for legitimate government function.

International organisations

The statement of confidentiality refers to the possibility of passing information about the asylum claimant to international organisations without their express permission. In this instance, the term international organisations refers to recognised and respected organisations concerned with the welfare of asylum seekers such as the United Nations High Commissioner for Refugees (UNHCR), the Red Cross or the International Organization for Migration (IOM). Information must only be given on the understanding that it is treated in the strictest confidence and in a manner which would not pose risk to the individual or their family.

Information about a claimant's actual asylum claims must only be given where the organisation already knows that asylum claims exist and provided that the claimant consents to disclosure.

If there is any doubt about whether or not information should be given to such an organisation, you must seek advice from a senior caseworker. If it is not clear if the

sharing of information would be in compliance with data protection legislation you must ensure that your data protection lead is consulted.

Family tracing

Family members may become separated and wish to trace other family members. There may be safeguarding concerns to consider or reasons why some family members do not wish to be reunited. Therefore, if someone wishes to trace family members you can refer to the family tracing contact details found in the [information leaflet](#) provided to the asylum claimant.

You must refer to the Family tracing Asylum Instruction for specific guidance on sharing information for tracing family members of unaccompanied children. SVEC assists the Red Cross with fulfilling their family tracing duties.

Authorities in the claimant's own country and other countries

The claimant is informed that information they give us will be treated in confidence and the details of their asylum claims will not be disclosed to the authorities of their own country. This applies equally where consideration is being given as to whether to revoke a person's refugee status and or leave.

You must not disclose any information about individual's asylum claim to the authorities of their country of origin while claims are under consideration, including confirming that asylum claims have even been made. To do so would be unlawful and could put the claimant and or members of their family at risk. You must ensure that any request for information made to the authorities would not directly or indirectly alert them to the likelihood that asylum claims have been made. If you become aware that a legal representative or anyone else may have disclosed information, this must be reported to your data protection lead.

See Biometric data-sharing process guidance for information on which cases may be checked through international biometric data-sharing.

When asylum is granted, you must not return any passports to the refugee's embassy.

Serious criminal charges

There may be circumstances where it may be inappropriate to withhold the fact that a person is in the UK if, for example, the other country produces evidence that they are wanted on serious criminal charges and extradition proceedings are being contemplated. In each case, the decision to disclose must be authorised by a senior caseworker or above. Any decision to refuse to provide such information should be taken in consultation with Asylum Policy. Despite potential criminality, due to risk of harm to the individual or their family, you can neither confirm nor deny if asylum claims have been made.

Disclosure of identity for re-documentation purposes

When asylum claims are unsuccessful, it may be necessary to provide information about the claimant's identity to the authorities in their own country in order to obtain travel documentation.

The information disclosed must be limited to that which is necessary for re-documentation purposes. Details of the asylum claims must not be shared and no reference should ever be made to the fact that claims for asylum were made in the UK, see Returns Logistics guidance. Arranging removals guidance provides information on not sharing immigration history with third parties.

Related content

[Contents](#)