Immigration Enforcement: Digital device extraction policy

Version 1.0

This guidance sets out the powers and obligations on Immigration Enforcement Criminal and Financial Investigators (CFI), Investigators within Immigration Compliance and Enforcement (ICE), Immigration Intelligence (II) and others lawfully charged with seizure and interrogation of digital media under the Data Protection Act 2018 (DPA) and how these interact with Criminal Procedure and Investigation Act 1996 (CPIA), statutory powers of seizure and case law.
Contents

About this guidance ............................................................................................................. 3
Contacts .............................................................................................................................. 3
Publication .......................................................................................................................... 4
Changes from last version of this guidance ........................................................................ 4
General principles for investigators .................................................................................. 5
Criminal Procedure and Investigations Act (CPIA) Code of Practice ............................ 7
Obtaining material from the device of a suspect ............................................................... 9
Police and Criminal Evidence Act 1984 ........................................................................... 9
S48 Immigration Act 2016 - Seizure and retention in relation to offences ................. 10
Investigatory Powers Act 2016 ....................................................................................... 10
DPN forms process ........................................................................................................... 14
How to review material .................................................................................................... 15
How to review the material ............................................................................................... 15
Digital Device Extraction policy: CFI requirements under ISO17025 Standard ........ 17
About this guidance

This guidance tells criminal investigators in Immigration Enforcement Criminal and Financial Investigators (CFI), Immigration Investigators within Immigration Compliance and Enforcement (ICE), Immigration Intelligence (II) and suitably trained and accredited criminal investigators within the Home Office and others lawfully charged with seizure and interrogation of digital media about their powers and obligations under the Data Protection Act (DPA) 2018 and how these interact with the Criminal Procedure and Investigations Act 1996 (CPIA), statutory powers of seizure and case law.

This guidance is not intended to be a detailed operational guide but is intended to set out a common approach to be adopted when seeking to obtain and handle digital material, whether that be from a suspect, victim or witness.

It provides officers with a set of principles to inform them how they obtain personal digital devices – most often mobile phones – from victims, witnesses and suspects for the purpose of an investigation and how they then extract the digital data from those devices.

It also seeks to highlight the considerations investigators and prosecutors should have when obtaining and handling sensitive personal information, in accordance with obligations under data protection legislation.

This document should be read in conjunction with the following documents:

- Criminal Procedure and Investigations Act Code of Practice 2015
- Criminal Procedure and Investigations Act 1996 Code of Practice 2020
- APP Extraction of material from digital devices (college.police.uk)
- Information Commissioner’s Office Report – Mobile Phone Data Extraction
- Data Protection Act (DPA) 2018

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 (Cyber & Digital Capabilities).

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.

The Home Office has a duty to safeguard vulnerable people and promote the welfare of children for more information see: Vulnerable people and children.
Criminal Investigators in Immigration Enforcement must be aware of their obligations under the UK General Data Protection Regulation (UK GDPR) and Part 3 of the Data Protection Act 2018 see: Data Protection Policy: Criminal and Financial Investigation (CFI), Immigration Enforcement also see: Data protection

**Publication**

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

- version 1.0
- published for Home Office staff on 07 July 2021

**Changes from last version of this guidance**

New guidance

**Related content**

[Contents](#)
General principles for investigators

This page tells criminal investigators in Immigration Enforcement and suitably trained and accredited criminal investigators within the Home Office, Immigration Intelligence (II) and others lawfully charged with seizure and interrogation of digital media about the general principles relating to the seizure and extraction of data from digital devices during a criminal investigation.

Investigators will need to consider the practicalities of requesting or seizing digital devices, especially where there are many devices. They will also need to consider the effect that taking possession of or seizure of a digital device will have on a business, organisation or individual; and where it is not feasible to obtain a copy of the digital material, the likely timescale for returning the obtained items. Investigators should outline the strategy to be employed when considering the seizure of digital devices in pre-planned operations in the operational order. Investigators should also outline the rationale for the examination of digital devices in the Investigation Management Document (IMD)

When seeking to obtain digital material, whether from a suspect, witness or victim, any intrusion into the personal and private lives of individuals should be carried out only where deemed strictly necessary and using the least intrusive means possible to obtain the material required, adopting an incremental approach.

The term ‘strictly necessary for the law enforcement purpose’ places a high threshold for processing based on this condition. Investigators need to demonstrate they have considered other, less privacy-intrusive means and have found they do not meet the objective of the processing. In addition, there is a further requirement to demonstrate that the processing meets at least one of the Schedule 8 Data Protection Act 2018 conditions:

- statutory purposes
- administration of justice
- protecting individuals’ vital interests
- safeguarding of children and of individuals at risk
- personal data already in the public domain
- legal claims
- judicial acts
- preventing fraud
- archiving

Strictly necessary in this context means that the processing has to relate to a pressing social need, and Immigration Enforcement cannot reasonably achieve it through less intrusive means. This is a requirement that will not be met if Immigration Enforcement can achieve the purpose by some other reasonable means.

The ‘strictly necessary’ criterion should lead to consideration of whether the objective of the measure pursued is sufficiently important to justify the limitation of a fundamental right, for example the right to privacy see: Article 8 Human Rights Act 1998 (legislation.gov.uk)
For more information see:

- APP Extraction of material from digital devices (college.police.uk)
- Disclosure - A guide to "reasonable lines of enquiry" and communications evidence | The Crown Prosecution Service
- Disclosure - Guidelines on Communications Evidence | The Crown Prosecution Service
- Court of Appeal ruling on Reasonable Lines of Enquiry [R v E 2018 EWCA 2426 (Crim)] | The Crown Prosecution Service

The following general principles, outlined in the Attorney General’s Guidelines on Disclosure 2020, must be followed by investigators in handling and examining digital material:

- no action should be taken which changes data on a device which may subsequently be relied upon in court
- if it is necessary to access original data, then that data should only be accessed by trained and accredited officers who are competent and able to explain the relevance and implications of their actions to a court
- an audit trail should be kept of all processes followed (another practitioner should be able to follow the audit trail and achieve the same results)
- the investigator in charge of the investigation has responsibility for ensuring that the law and these principles are followed

Where an investigator has reasonable grounds for believing that digital material may contain material subject to legal professional privilege then this may not be seized unless the provisions of the Criminal Justice and Police Act 2001 apply.

Related content

Contents
Criminal Procedure and Investigations Act (CPIA) Code of Practice

This page tells criminal investigators in Immigration Enforcement, Immigration Intelligence (II) and suitably trained and accredited criminal investigators within the Home Office about how officers should record, retain and reveal to the prosecutor material obtained in a criminal investigation.

The CPIA Code of Practice provides guidance concerning the duty to pursue all reasonable lines of enquiry, in relation to digital material. The CPIA 1996 Code of Practice 2020 applies where investigations started on or after 31 December 2020.

For more information see:

- Criminal Procedure and Investigations Act Code of Practice 2015
- Criminal Procedure and Investigations Act 1996 Code of Practice 2020

Examination of material held on a digital device may require expert assistance to help extract evidence and assist with unused material.

Generally, material must be examined by the disclosure officer or the deputy but, exceptionally, the extent and manner of inspecting, viewing or listening will depend on the nature of the material and its form.

A record or log must be made of all digital material seized or imaged and subsequently retained as relevant to the investigation.

In cases involving large quantities of data where the person in charge of the investigation has developed a strategy setting out how the material should be analysed or searched to identify categories of data, a record should be made of the strategy and the analytical techniques used to search the data, including the software used. The record should include details of the person who has carried out the process and the date and time it was carried out. In such cases the strategy should record the reasons why certain categories have been searched for.

For example, it might be reasonable to examine digital material by using software search tools. The methodology of the examination must be described on the disclosure schedules accurately and as clearly as possible. The extent and manner of its examination must also be described together with justification for such action and this forms part of a digital forensic strategy.

The suspect (defendant) should also be asked if there is any material on the device(s) that may assist their case.

The digital strategy must be set out in an Investigation Management Document (IMD) to feed into the CPS Disclosure Management Document (DMD).
Obtaining material from the device of a suspect

This page tells criminal investigators in Immigration Enforcement and suitably trained and accredited criminal investigators within the Home Office, Immigration Intelligence (II) and others lawfully charged with seizure and interrogation of digital media about the legal obligations and powers in relation to the seizure and retention of digital devices from a suspect under the Police and Criminal Evidence Act 1984 (PACE) and the Immigration Act 2016.

Police and Criminal Evidence Act 1984

In cases where the device user is a suspect, the Police and Criminal Evidence Act 1984 and The Police and Criminal Evidence Act 1984 (Application to immigration officers and designated customs officials in England and Wales) Order 2013 provides a number of statutory seizure powers. This limited subset of PACE powers can be exercised only by those immigration officers suitably trained and accredited to use them. The circumstances in which these powers can be exercised include:

- where a person is under arrest for an indictable offence, powers of entry and search are conferred in relation to any premises occupied or controlled by that person alongside powers to seize and retain anything found:
  o this includes a power to require any information stored in any electronic form and accessible from the premises to be produced in a form in which it can be taken away and in which it is visible or legible
- when lawfully on premises (for example, under warrant), general powers of seizure are exercisable, including powers to seize anything if there are reasonable grounds for believing it is evidence relating to an offence and it is necessary to seize it in order to prevent the evidence being concealed:
  o this includes a power to require any information stored in any electronic form and accessible from the premises to be produced in a form in which it can be taken away and in which it is visible or legible
- where a person has been arrested other than at a police station, search powers are conferred in relation to:
  o amongst other things, anything which may be evidence relating to an offence, alongside power to seize and retain anything found

Where an investigator has reasonable grounds for believing that digital material may contain material subject to legal professional privilege then this may not be seized unless the provisions of the Criminal Justice and Police Act 2001 apply.
S48 Immigration Act 2016 - Seizure and retention in relation to offences

Section 48 Immigration Act 2016 provides the power to an immigration officer lawfully on any premises to seize evidence which the officer finds in the course of exercising a function under the Immigration Acts and it is necessary to seize it in order to prevent it being concealed, lost, damaged, altered or destroyed. The power is not intended for use by those officers who are trained and accredited to use PACE powers.

Those officers who use the section 48 power should also be aware of the considerations under Section 49 Immigration Act 2016.

Digital material may be seized from suspects using these statutory powers, but this material may be obtained from suspects and witnesses with their cooperation as well. See: Obtaining material from the device of a witness.


The Investigatory Powers Act (IPA) 2016 makes provisions about the interception of communications and how intercepted material is handled. These powers are subject to oversight by the Investigatory Powers Commissioner’s Office (IPCO).

Under the IPA, an interception can occur while a communication is being transmitted or by accessing communications stored before or after transmission. Under s4(4)(b) of the IPA, accessing the contents of a communication stored in or by a telecommunication system (whether before or after its transmission) constitutes interception, irrespective of whether it has already been accessed by the intended recipient. This has significance in the context of digital device extraction if accessing “stored communications”.

Section 6 of the IPA provides for “lawful authority” to carry out the interception of communications. A person has lawful authority to carry out an interception if it is carried out in accordance with a targeted interception warrant. “In the case of a communication stored in or by the telecommunications system”, a person also has lawful authority to carry out an interception if it is carried out in accordance with a targeted equipment interference warrant, in the exercise of any statutory power that is exercised for the purpose of obtaining information or taking possession of any document or other property, or in accordance with a court order.

The most commonly encountered requirements for the lawful interception of communications without a warrant can be summarised as including (but not limited to) where:

- the sender and the intended recipient have consented to the interception
- either the sender or intended recipient has consented and a concurrent directed surveillance authority is in place under Part 11 Regulation of Investigatory Powers Act 2000
• it takes place as a result of the exercise of a statutory power exercised for the purpose of obtaining the information, for example the Police and Criminal Evidence Act 1984
• it is carried out in accordance with a court order

Related content
Contents
Obtaining material from the device of a victim/witness

This page tells criminal investigators in Immigration Enforcement and suitably trained and accredited criminal investigators within the Home Office, Immigration Intelligence (II) and others lawfully charged with seizure and interrogation of digital media about the legal obligations in relation to seizure, relevance and retention from a witness/victim.

Digital devices should not routinely be obtained from victims and witnesses. There must be a properly identifiable basis for forming the belief that specific material is required from the device. Devices should not be sought based on mere conjecture or speculation. The same requirements apply to requests for searches by the defence. Their requests must be sufficiently precise to enable targeted searching of devices for relevant material.

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

___________________________________________________________

The request to inspect digital material, in every case, must have a proper basis, namely that there are reasonable grounds to believe that it may reveal material relevant to the investigation or the likely issues at trial – it must be a reasonable line of enquiry.

CFI officers need to familiarise themselves with the Court of Appeal Judgment in R v Bater-James and Mohammed [2020] EWCA Crim 790.

In the above case the court considered the various issues relating to the retention, inspection, copying, disclosure and deletion of the electronic material held by prosecution victims and witnesses and gave extensive guidance in relation to the following 4 heads of principle:

1. **Identifying the circumstances when it is necessary for investigators to seek details of a witness's digital communications.**

Investigators must only review material if it is a reasonable line of enquiry on the facts of the case. The court stressed that mobile telephones or other devices should not be obtained as a matter of routine. There is no automatic right or presumption that the material is reviewed.
2. When it is necessary, how should the review of the witness's electronic communications be conducted?

Investigators need to take a staged approach. First, to consider whether review can happen without recourse to the device. Second, whether it is sufficient simply to view limited areas (for example, an identified string of messages/emails or particular postings on social media). Only if a more extensive enquiry is necessary should the contents of the device be downloaded with the minimum inconvenience to the witness. Enquiries should be focussed using search terms and date parameters.

3. What reassurance should be provided to the witness as to ambit of the review and the circumstances of any disclosure of material that is relevant to the case?

The witness should be kept informed as to any decisions that are made in relation to examination of the device and resulting disclosure. They must be reassured that any content within the device will only be copied or inspected if there is no other appropriate method of discharging the prosecution's disclosure obligations and any material meeting the disclosure test will be appropriately redacted prior to disclosure.

4. What is the consequence if the witness refuses to permit access to a potentially relevant device or if material is deleted?

It is important to look carefully at the reasons for a refusal. The court must assess the impact of the absence of the particular missing evidence and whether the trial process can sufficiently compensate for its absence. An application can be made for a witness summons for the mobile telephone or other device to be produced. If the witness deletes material, although each case will need to be assessed on its own facts, the court noted the potential utility of cross-examination and carefully crafted judicial directions.

If the device owner does not permit the device to be taken, the officer must:

- explain why it is needed and stress the safeguards that will be in place for handling the extraction, storage and management of the data
- explain the potential implications of not providing the data
- make a record of all actions and conversations about the device owner’s refusal

For further information see: [APP Extraction of material from digital devices (college.police.uk)](http://college.police.uk)

If the responder thinks it is necessary to have access to the data, a Chief Immigration Officer (CIO) will be consulted to decide whether the matter under investigation and/or prosecution is so significant or serious that it is necessary for CFI to have access to the data.

The CIO may authorise a legal power such as section 19 [Police and Criminal Evidence Act 1984](http://PACE) (PACE) to obtain the device. The owner of the device will need to
be informed that deletion of data might lead to undermining the investigation to the extent that it cannot continue.

**DPN forms process**

A Digital Processing Notice (DPNa) **must** be completed in all cases. Within this document the witness endorses their agreement to allow staff to take possession of the device and process the data. The form used to request data extraction must also be authorised at a minimum of Chief Immigration Officer (CIO) level, who will record the rationale why this was believed to be strictly necessary.

The witness must also be provided with a DPNb ‘witness information sheet in their preferred language.

For further information on completing the form see: Guidance for officer completing the DPNa form – FAQs

**Related content**

[Contents](#)
How to review material

This page tells criminal investigators in Immigration Enforcement and suitably trained and accredited criminal investigators within the Home Office, Immigration Intelligence (II) and others lawfully charged with seizure and interrogation of digital media about how to review material on devices.

For the purposes of this guidance unless there is an intention to investigate and prosecute a migrant for the offence of illegal entry under Section 24 (1) (a) of the Immigration Act 1971 or they are suspected of being involved in facilitating the illegal entry of others, they are to be treated as victims/witnesses.

How to review the material

Identify that it is a reasonable line of enquiry, and the victim/witness has agreed through fully informed consent to provide their device, then consider carefully what specific material is needed from the device and how to review it.

This should be an incremental approach, starting with the least intrusive method where appropriate. Reduce the inconvenience to the victim/witness by keeping the device for the minimum time possible. Consider:

- can the material be reviewed without taking the device from the victim or witness?
- has the same material from the suspect’s device already been obtained and if so, is this enough and there is no need to examine the witness’s device
- manual examinations of devices, including screen shots, may be considered in certain circumstances
- seek forensic advice about the method of capture

Consider a manual examination, including screenshots, without taking the device away only when:

- there is minimal material, which is unlikely to be of significant evidential value
- material on devices may be lost if not captured immediately
- volatile material is present, for example: data that might be lost if the device is turned off
- having obtained the informed consent of the victim/witness to provide their device, reassured them of its handling and explained to them the potential consequences of refusing to provide it, they still will not do so, leaving screenshots as the only available option to secure some record of the material (this might be the case if the witness will not allow the device to be taken but will allow screenshots)

If the conditions for manual examination are not met and Mobile Phone Extraction (MPE) is required, then the contents should be extracted with minimum inconvenience to the owner and the device returned without unnecessary delay.
Only trained and accredited officers should extract and/or search for the material believed to be relevant to the case. For example, decide on the time-frame that is likely to be relevant within specific applications or datasets and set specific start and end dates accordingly before searching for and/or extracting material. Advise the witness that these parameters have been set, together with your rationale.

Whatever technology is used to extract material from digital devices, officers should only search for material that allows them to review what is strictly necessary as identified on this form and agreed with the witness.

Consider the implications of the IPA 2016. For further information see: Investigatory powers Act 2016 if necessary, to view stored electronic communication content on the device.

Wherever possible, any material extracted from a device that is not relevant to the investigation should be deleted. This includes material that has not been reviewed following the deployment of search tools. Do not retain this material in anticipation of it possibly being relevant later.

CFI officers need to be aware that the data which the officer seeks to review is only that pertaining to the ongoing investigation forming part of a reasonable line of enquiry. If the data is not potentially linked to the crime/offence under investigation it will not be reviewed.

Further, consideration should also be given to whether the extraction of material from the device and the intrusion and inconvenience this would cause the individual is proportionate to the offence being investigated.

If further searches are required, a further Digital Processing Notice (DPNa) should be completed with the witness.

Investigators and disclosure officers must be fair and objective and must work together with prosecutors to ensure that disclosure obligations are met. Investigators and disclosure officers should be familiar with the CPIA Code of Practice in particular their obligations to retain and record the relevant material, to review it and to reveal it to the prosecutor see paragraphs 3-7 of the Criminal Procedure and Investigations Act 1996 (section 23(1)) Code of Practice, and Attorney General’s Guidelines on Disclosure 2020 Annex A – Digital Material

Related content
Contents
Digital Device Extraction policy: CFI requirements under ISO17025 Standard

This page tells criminal investigators in Immigration Enforcement and suitably trained and accredited criminal investigators within the Home Office, Immigration Intelligence (II) and others lawfully charged with seizure and interrogation of digital media about Criminal and Financial Investigation (CFI) standard operating procedures under ISO17025

Criminal and Financial Investigation (CFI) ISO17025 standard operating procedures dictate that an IE22 form must be completed prior to any extraction. This is clearly contained within the guidance.

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

This is a requirement under ISO regulations to ensure that the kiosk operator is aware of their objectives and that the quality manager is notified that an extraction has been recorded.

Where there is specific evidence believed to be contained within a device, a review should focus tightly around the investigative objectives. This should be subject to advice from a digital media advisor (DMA) and a digital media strategy recorded on an Investigation Management Document (IMD) must be prepared to support the IE22.

An IMD should also be completed to ensure that a full record of what has been and just as importantly what has not been viewed has taken place. This is a requirement of the Criminal Procedure and Investigations Act 1996 and a recommendation of the Information Commissioner's Office (ICO) principles.

The digital strategy should indicate the requirement, necessity and proportionality for the search and ensures that only relevant data is extracted or reviewed.

CFI staff are required to make a declaration when undertaking phone downloads and producing MG11s with their examination findings as CFI/IE do not have ISO 17025 accreditation and have not been accredited to the Forensics Regulators Codes of Conduct.

Official – sensitive: start of section