Home Office

Immigration Enforcement Criminal and Financial Investigations: Digital devices – seizure and retention, and data extraction policy

Version 4.0

This guidance tells criminal investigators in Immigration Enforcement (IE) and suitably trained and accredited criminal investigators within the Home Office about their statutory powers to seize, obtain, extract and retain digital devices from suspects, witnesses and victims in criminal investigations, and their obligations under the Data Protection Act 2018 (DPA) and the Criminal Procedure and Investigation Act 1996 (CPIA).

Contents

About this guidance

This guidance tells criminal investigators in Immigration Enforcement (IE) and suitably trained and accredited criminal investigators within the Home Office about their statutory powers to seize and obtain digital devices from suspects, witnesses and victims in criminal investigations, and their obligations under the Data Protection Act (DPA) 2018 and the Criminal Procedure and Investigation Act 1996 (CPIA)

This guidance is intended to give an overview of powers available to criminal investigators when seeking to seize and handle digital material from a suspect in a criminal investigation.

It provides officers with a set of principles to inform them how to:

- devise an effective digital investigation strategy
- obtain personal digital devices – most often mobile phones – from suspects, witnesses and victims
- extract the digital data from those devices
- process data for the purpose of a criminal investigation, including sensitive personal information, in accordance with data protection legislation

Further information is available on dealing with digital material, disclosure and data protection obligations from the following sources:

- Attorney General's Guidelines on Disclosure 2024 Annex A – Digital Material
- Criminal Procedure and Investigations Act Code of Practice 2015
- Criminal Procedure and Investigations Act 1996 (section 23(1)) Code of Practice 2020
- Investigatory Powers Act 2016
- Authorised Professional Practice - Extraction of material from digital devices
- Information Commissioner's Office Report – Mobile Phone Data Extraction
- Investigation of protected electronic information policy

The Home Office has a duty to safeguard vulnerable people and promote the welfare of children for more information see: Vulnerable adults 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: IE CFI Data protection policy.

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 Reviews, Atlas and Forms team.

Publication

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

- version **4.0**
- published for Home Office staff on **17 October 2025**

Changes from last version of this guidance

- updated sections on data protection responsibilities, Privacy Information Notices, and use of consent for processing data
- new section on obtaining devices from witnesses and victims via The Police, Crime, Sentencing and Courts Act 2022
- updated procedures for deletion of device data when there is no lawful basis for retaining it
- new section on handling devices during search and seizure and manual reviews
- housekeeping changes

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, about the general principles relating to the seizure and extraction of data from digital devices during a criminal investigation.

What are digital devices?

Digital devices are any electronic device capable of storing data. For example, a mobile phone, tablet, laptop, hard drive, server. Such devices are capable of storing a wide variety of personal data relating to their owners, with clear implications for their right to privacy if that data is accessed by others.

What do I need to consider before seizing digital devices?

Investigators will firstly need to be sure they have the power to seize or otherwise obtain the item. They will then need to consider the practicalities of obtaining digital devices, especially where there are many. 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 by less intrusive means, the likely timescale for returning the obtained items.

Investigators should outline the strategy to be employed when considering the obtaining 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).

To what extent can digital devices be searched?

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 to the extent strictly necessary allowed by the power you have used to seize it, or to the extent voluntarily agreed to.

Any intrusion must only be to the extent strictly necessary for law enforcement purposes and using the least intrusive means possible to obtain the material required, adopting an incremental approach. Unnecessary intrusion could be considered a breach of Article 8 of the European Convention on Human Rights (Respect for private life).

Investigators need to demonstrate they have considered other, less privacy-intrusive means and have found they do not meet the objective of the processing. This is a requirement that will not be met if Immigration Enforcement can achieve the purpose by some other reasonable means.

ACPO guidelines

Any examination of any digital device must always be carried out in accordance with the ACPO guidelines.

The following 4 general principles, first outlined in the Association of Chief Police Officers Good Practice Guide for Digital Evidence, and reinforced the Attorney General's Guidelines on Disclosure must be followed by **all** investigators in handling and examining ALL digital material:

1. No action should be taken which changes data on a device.

2. 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.

3. An audit trail should be kept of all processes followed, such that another practitioner should be able to follow the audit trail and achieve the same results.

4. The investigator in charge of the investigation has responsibility for ensuring that the law and these principles are followed.

Identifiable reasonable lines of enquiry considerations

CFI officers must be aware that digital devices should not as a matter of course be requested or seized from suspects, victims or witnesses. This should only be where in the particular circumstances of the investigation, there are identifiable reasonable lines of enquiry to obtain evidence which justify the request or seizure of that device.

Investigators should be clear if there are identified lines of enquiry when seizing or examining a device. Consideration must be given to the following factors in deciding whether seizing the device is appropriate:

- personal devices are highly likely to contain sensitive personal data: collecting and / or processing personal or private material can only be done when in accordance with the law, strictly necessary, and proportionate
- in order to be in accordance with the law and strictly necessary, an investigator must be pursuing a reasonable line of inquiry in seeking to obtain the material
- what constitutes a reasonable line of inquiry may be informed by others, including the prosecutor and the defendant: seeking the personal or private information of a complainant or witness will not be a reasonable line of inquiry in every case – an assessment of reasonableness is required
- the assessment of reasonableness must be made on a case-by-case basis and regard may be had to:
  - the prospect of obtaining relevant material
  - what the perceived relevance of that material is, having regard to the identifiable facts and issues in the individual case

- if, by following a reasonable line of inquiry, it becomes necessary to obtain personal or private material, investigators will also need to consider:
  - what review is required
  - how the review of this material should be conducted
  - what is the least intrusive method which will nonetheless secure relevant material
  - are particular parameters for searching best suited to the identification of relevant material
  - is provision of the material in its entirety to the investigator strictly necessary; or alternatively, could the material be obtained from other sources, or by the investigator viewing and / or capturing the material in situ? - an incremental approach should be taken to the degree of intrusion
- the rationale for pursuing the reasonable line of inquiry and the scope of the review it necessitates should be open and transparent - it should be capable of articulation by the investigator making the decision - it should provide the basis for:
  - consultation with the prosecutor
  - engagement with the defence
  - the provision of information to the witness about how their material is to be handled

Digital Investigation Strategy

All investigations should have a Digital Investigation Strategy which is reviewed regularly, and subsequent actions dealt with promptly. Seizure of devices is one of several possible digital enquiries available to investigators.

For serious and complex investigations, this must be a formal document, completed by the Officer in the Case (OIC) in conjunction with a Digital Media Advisor and agreed by the Investigation Supervisor.

For volume and priority investigations, a formal Digital Investigation Strategy is advisable, but this may also be recorded using the decision register on Clue. This decision needs to be linked to any future forensic tasking.

For instruction on how to do this, see CLUE Crime Case Management System (BAU) - Home and Clue: Criminal investigation case management system standards

The digital evidence investigation strategy should indicate the requirement, necessity and proportionality for the search and seizure of any digital device, and ensure that:

- digital devices are only seized where less intrusive methods of obtaining the same information are unavailable
- only relevant data is extracted or reviewed from such devices

The only reason a digital evidence investigation strategy should not be developed is if there is no possibility of any digital evidence being sought or used in an investigation. If this occurs, the reasoning not to produce a digital evidence investigation strategy should be recorded as a decision on Clue.

The digital strategy in England and Wales should be referenced in an Investigation Management Document (IMD) which then informs the Crown Prosecution Service's Disclosure Management Document (DMD).

Law enforcement are no longer routinely extracting all the data from mobile devices, as this is rarely proportionate and necessary. Consider focussing extractions along the following lines:

- where and what evidence you believe to be on the device
- what timeframe do you believe encompasses the offence
- what communication you believe to be on the device
- relevant search terms, file, and application types

Legal Professional Privilege

Documents subject to legal professional privilege (LPP) are exempt from search or seizure, unless specified with an explicit power.

Official sensitive: start of section

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

Official sensitive: end of section

Items capable of being subject to LPP are contained in section 10 of Police and Criminal Evidence Act 1984 (PACE) (and equivalent legislation in Scotland and Northern Ireland) and include:

- confidential communications between a professional legal adviser and their client, or any person representing their client, made in connection with the giving of legal advice to the client (this includes instructions from the client) - this is often referred to as 'Legal Advice Privilege'
- confidential communications between a professional legal adviser and their client, or any person representing their client, made in connection with or in contemplation of legal proceedings - this is often referred to as 'Litigation Privilege' and can also include confidential communications with third parties where the dominant purpose of the communication is in the context of litigation
- items, which are enclosed with, or referred to, in the communications set out above

It should be noted that officers should not attempt to decide of whether or not an item is subject to LPP. If material appears to be privileged (in that it is looks like a

solicitor's letter), or an individual asserts that it is, officers should not attempt to read or seize it.

Where evidence is seized and material has been identified as potentially containing LPP, it must be isolated and reviewed by a lawyer independent of the investigating or prosecuting authority. No member of the investigative or prosecution team involved in either the current investigation or, if the LPP material relates to other criminal proceedings, in those proceedings, should have sight of or access to the LPP material. Strict rules apply to the search and sift of digital material which may contain LPP material.

Official sensitive: start of section

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

Official sensitive: end of section

For more information see:

- 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

Related content
Contents

Statutory powers: digital devices

This section tells criminal investigators in Immigration Enforcement (IE) and suitably trained and accredited criminal investigators within the Home Office about the legal powers and obligations in relation to digital devices.

Official – sensitive: start of section

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

Official – sensitive: end of section

All powers under Police and Criminal Evidence Act (PACE) 1984

The Police and Criminal Evidence Act 1984 (Application to immigration officers and designated customs officials in England and Wales) Order 2013 extends certain powers under PACE to be used by Immigration Officers (IOs) carrying out criminal investigations in England and Wales.

This limited subset of PACE powers can be exercised only in relation to investigations carried out by IOs who are suitably trained and accredited to use them. Specifically, these powers are:

Section	Power
s.8(1) to (6)	Warrant to enter and search
s.9(1)	Warrant to enter and search for 'excluded material' or 'special procedure material'
s.15	Search warrants - safeguards
s.16	Execution of warrants
s.17(1)(a)(i), (1)(b), (1)(cb)(i),(1)(d), (2) and (4)	Entry for purpose of arrest
s.18	Entry and search after arrest
s.19	General Power of seizure
s.20	Extension of powers of seizure to computerised information
s.21	Access and copying
s.22(1) – (4) and (7)	Retention
s.24(1) to (5)(c)(iii) and (5)(d) – (5)(f)	Arrest without warrant
s.29	Voluntary attendance at police station
s.30(1) to (4)(a) and (5) to (13)	Arrest elsewhere than police station
s.31	Arrest for further offence
s.32(1) to (9)	Search upon arrest
s.46A(1) and (1A) to (3)	Power of arrest for failure to answer police bail
s.51(b)	Savings

Section	Power
s.107(2)	Police officers performing duties of higher rank

'Excluded material': This is material which is any of the following:

- personal records which a person has acquired or created in the course of any trade, business, profession or other occupation or for the purposes of any paid or unpaid office and which he holds in confidence
- human tissue or fluid taken for the purposes of diagnosis or medical treatment which the person holds in confidence
- journalistic material which a person holds in confidence

'Special Procedure material': Material acquired or created in the course of a trade, business, profession, occupation, or office that is held subject to an express or implied undertaking to hold it in confidence, or subject to a statutory restriction on disclosure or obligation of secrecy.

All of the above search and seizure powers include 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.

Before any search or seizure is carried out, those conducting and/or authorising must be satisfied that it is both necessary and proportionate to the offence under investigation, in accordance with Article 8 Human Rights Act 1998 (Respect for private and family life).

Entry, search, seizure and retention

Legislation provides separate powers for entry, search, seizure and retention so you must be sure you have the power to execute each of them. Each search power will also have relevant connected power of seizure and retention. These 2 powers, whilst they may seem similar, are entirely separate:

'Seizure' allows you to take an item into your possession that you have found either on the person or the premises you are searching. What are you are legally allowed to seize will usually correlate with the power that allows you to search. You must be sure you have the power to seize an item before taking it.

'Retention' is the power to keep hold of the item you have taken. A power to retain will usually determine how long you may keep something. Again, you must be sure you have the appropriate power to keep an item you have taken.

Retention of digital devices under the Police and Criminal Evidence Act 1984

In accordance with Section 22 PACE, anything seized for the purposes of a criminal investigation may be retained so long as is necessary in all the circumstances.

Anything may be retained in order to establish its lawful owner, where there are reasonable grounds for believing that it has been obtained in consequence of the commission of an offence.

Anything seized may be retained for evidence in a trial or for forensic examination / investigation.

However, nothing may be retained where a photocopy or a copy would suffice. Investigators should therefore consider at the point where relevant material has been extracted from a device, whether the device itself should be restored to the owner.

Officers will need to consider and record rationale for the continued retention of a device where material has been extracted.

Computers and related storage devices may be capable of being forensically imaged, whereby a bit for bit copy can be made of the device. This is not the same in the case of mobile phones. Mobile phones use solid state memory chips with processors built into them. This means it's not possible to directly access or copy the memory bit for bit.

Everything must be done via an embedded controller in order to translate the data into tangible data. Specific advice should be considered on a case-by-case basis and advice can be sought by contacting Cyber Digital Capabilities.

Seizure and retention under S48 Immigration Act 2016

Section 48 Immigration Act 2016 provides the power to an Immigration Officer lawfully on any premises while exercising a function under the Immigration Acts to seize evidence they find, if seizure is necessary, it in order to prevent it being concealed, lost, damaged, altered or destroyed.

Official – sensitive: start of section

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

Official – sensitive: end of section

Seize and sift powers

Under the Criminal Justice and Police Act 2001 Section 50 and Section 51, CFI officers can remove items from premises or people for the purpose of sifting or examination elsewhere (for example, a large bulk of mixed material, or where a laptop may hold bulk material). This is also known as 'seize and sift'.

See PACE Code B 2023 Paragraph 7.7.

Sections Section 50 and Section 51 apply to a range of search powers, which are set out in the Criminal Justice and Police Act 2001 Part 1 and Part 2 of Schedule 1.

Following HM, R (On the Application Of) v Secretary of State for the Home Department [March 2022] it is now accepted that officers can treat a mobile device as a single item, and can seize it under the general powers of seizure mentioned previously.

Officers are advised to use their judgement when utilising powers, and to employ them as they see fit to suit the circumstances encountered. Although 'seize and sift' powers under section 50 and 51 of the CJPA 2001 are not required in all situations they may still apply - for example where officers have reasonable grounds for believing legally privileged material could be stored on a device.

For more information see Search powers, and obtaining and executing search warrants | College of Policing.

Encrypted devices

Often it will be apparent when seizing a device that it features encryption, where data cannot be accessed without an encryption key such as a swipe pattern, passcode or Personal Information Number (PIN).

Encryption may apply separately to the device's operation system as well as individual applications or files.

Officers should ask the owner of device where possible for any passcodes. Requesting a passcode for the purpose of searching a device is equivalent to requesting a key to access a premises for the purpose of search and, as such, the request does not amount to a PACE interview. Officers should test any provided passcode to determine its veracity, and if verified record the passcode on the tamper-proof evidence bag, pocket notebook, or search record.

Device owners are under no legal obligation to supply the passcode at this point.

If device owners refuse, and the offence under investigation meets the definition of 'serious' under the Regulation of Investigatory Powers Act (RIPA) 2000, then Section 49 of that Act may be used to compel subjects to disclose passcodes.

Official – sensitive: start of section

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

Official – sensitive: end of section

Retention under section 28ZI and 28I of the 1971 Immigration Act

This section applies to CFI officers in Scotland and Northern Ireland only when using seizure powers under Part 3 of the Immigration Act 1971.

For devices seized under Part 3 of the 1971 Immigration Act investigators may retain said items under Section 28ZI. This section applies to anything seized by an immigration officer under this part for the purposes of the investigation of an offence or on the basis that it may be evidence relating to an offence. Anything seized as mentioned may be retained so long as is necessary in all the circumstances and in particular:

- for use as evidence at a trial for an offence
- for forensic examination or for investigation in connection with an offence
- in order to establish its lawful owner, where there are reasonable grounds for believing that it has been obtained in consequence of the commission of an offence

However, nothing may be retained for a purpose mentioned above if a photocopy or a copy would be sufficient for that purpose.

Investigators must also consider their obligations under Section 28I of the 1971 Act which states amongst other things that:

- if the device owner / occupier of the premises asks for a record of what was seized, the officer must provide the record to that person within a reasonable time
- if the relevant person, asks the officer for permission for access to the seized material, the officer must arrange for him to have access to the material under supervision
- there is no duty under this section to arrange for access or provide copies of the seized material, if the officer has reasonable grounds for believing it would prejudice the investigation or any criminal proceedings

For more information, particularly in relation to criminal powers of seizure used by Immigration Officers in Scotland and Northern Ireland, see:

- CFI Guidance on Searches
- Criminal investigation guidance to the PACE (1984) Order 2013
- PACE Code B

Official – sensitive: start of section

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

Official – sensitive: end of section

Related content

Contents

Handling devices during search and seizure

This section tells criminal investigators in Immigration Enforcement (IE) and suitably trained and accredited criminal investigators within the Home Office how seized personal electronic devices should be handled during search and seizure, in order to preserve evidence.

A wide range of device types, models and operation systems may be encountered, with varying capabilities. New hardware and software are constantly coming to market. Furthermore, devices can be encountered in several different states, depending on whether they are:

- powered on or not
- encrypted via passcode or biometrics or not
- connected to any networks or services

All these factors ultimately influence the amount of material that may be retrieved from the device as evidence.

As such, every potential circumstance of device seizure cannot be covered in this guidance, and you should seek advice from CFI Cyber and Digital Capabilities whenever necessary.

Any interaction between an officer and a device has the potential to alter or destroy data. Therefore, any interactions with a device should only occur where strictly necessary, should be recorded to a standard where they can be replicated by an independent third party, and should only be done by officers with the appropriate level of competence.

Officers should be aware of the following broad instructions for handling devices, which apply in the most common search and seizure circumstances, and are permitted for officers without specialist training:

Official – sensitive: start of section

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

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

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

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

Official – sensitive: end of section

Related content
Contents

Obtaining devices from victims and witnesses: The Police, Crime, Sentencing and Courts Act 2022

Section 37 of the Police Crime Sentencing and Courts (PCSC) Act 2022 now provides a standard legal basis for immigration officers to lawfully take possession of, and access the data from, digital devices belonging to victims or witnesses – including those who are potentially vulnerable - with their agreement.

Both immigration officers and external digital forensic services under instruction from an immigration officer may exercise powers under this section.

Immigration officers may use the power under s.37 PCSC for the purposes of:

- preventing, detecting, investigating, or prosecuting crime
- helping to locate a missing person
- protection a child or an at-risk adult from neglect or physical, mental or emotional harm

When using this power for the prevention and detection of crime, you must reasonably believe that information on the device is relevant to a reasonable line of enquiry. Extraction of that information must be necessary and proportionate to that aim. An effective and up to date digital strategy document will help with this.

The device user's right to privacy must be respected as much as possible. Where you think that there is a risk of obtaining excess information, the exercise of s.37 PCSC Act powers will only be proportionate if you are satisfied that:

- there are no other means of obtaining the information sought which avoid that risk
- there are such other means, but it is not reasonably practicable to use them.

This is in accordance with the principles set out in the ruling Bater-James & Mohamed v R [2020] EWCA Crim 790. Less intrusive means may include, for example, a user providing screenshots or exporting data from their device and providing that to investigators.

For further information see: Disclosure - A guide to "reasonable lines of enquiry" and communications evidence (cps.gov.uk).

When utilising this power, officers must comply with the relevant statutory Code of Practice issued by the Home Office - Extraction of Information from electronic devices: code of practice.

This agreement to take possession of a device for the purpose of investigating or preventing crime, and the agreement to extract data, is distinct and separate from

the lawful basis under which personal data will subsequently be processed under Part 3 of the Data Processing Act 2018. Such processing will be on the basis of 'strict necessity' rather than 'consent' in most cases – see Legal basis for processing.

You cannot use these powers where the intention is to extract confidential information from a device. You should use your professional judgement to assess whether there is a risk of obtaining confidential information. In some cases, the device user may not know whether they have confidential information on their device, but you should consider asking every person providing agreement whether there is likely to be confidential information on their device.

In all cases, you must ensure information extraction is not excessive, minimising intrusion into the device user's privacy and the privacy of others. In some cases, it may be necessary to extract a larger subset of information to understand the context of it. For example, viewing the conversation immediately before and after a relevant comment.

In all cases, where a user has provided agreement to extract information authorised persons should aim to return a device as quickly as possible.

Requirements for voluntary provision and agreement

The device user must have made a fully informed and conscious decision to volunteer the device and have freely given their agreement to the extraction of information from it. The device user must not have had any undue pressure placed on them or been coerced by anyone to provide the device or agree to the extraction of information from it.

You must provide a Digital Processing Notice to a device user. This forms the basis of the agreement and must be signed by the person providing the device. The person must also be given a copy of the agreement. The Notice must include the following:

- the information that is sought
- the reason why the information is sought, for example how it may answer a reasonable line of enquiry, and how this meets the necessity and proportionately requirements
- how the information will be dealt with once it has been extracted, for example who it will be shared with and how long it may be retained for
- that the person may refuse to provide the device or agree to the extraction of information from it
- that the enquiry will not be brought to end merely because of this refusal
- that the person may withdraw their agreement any point before the extraction takes place, but where the extraction has already taken place, the requirements of disclosure may mean that some of the information obtained with their agreement may be disclosed to the CPS or the defence where it is relevant
- how long the device user is expected to be without their device

- if an additional extraction is required, what action will be taken to obtain further agreement
- any other, less intrusive methods, the authorised person has considered to obtain this information and if any were identified, why they have not been followed
- how any collateral information obtained will be managed
- how to challenge a request, both at the point it is made, and at a later date
- the person has voluntarily provided the device to an immigration officer
- the person has agreed to the extraction of information from the device

The relevant notices for Immigration Enforcement, are known as Data Processing Notice (DPNa) and Witness Information Sheet (DPNb).

Official – sensitive: start of section

The information on this page has been removed as it is restricted for internal Home Office use.
Official – sensitive: end of section

You must keep a completed copy of the DPNa for your records and supply the device user with a copy of the relevant sections of the DPNa. You must also supply the user with a DPNb for their information.

Separate DPNa forms must be completed and provided for each device seized.

If new lines of enquiry are subsequently identified which would require further extractions beyond those originally agreed to, this would require a new agreement with the device user, recorded on a new DPNa.

Extractions of devices obtained via section 37 PCSC Act powers must be authorised by a sanctioning officer, at least one rank higher than the first authorising officer, and of the minimum rank of Chief Immigration Officer. This authorisation is recorded in writing on the DPNa.

Vulnerable victims and witnesses

The PCSC Act includes safeguards for vulnerable witnesses and victims to ensure they can make a fully informed and conscious decision to volunteer their device for extraction.

For example, witnesses or victims in Immigration Enforcement investigations may be experiencing temporary shock when encountered, may not be able to read or write, or may require an interpreter.

See Extraction of Information from electronic devices: code of practice for guidance on how to identify various vulnerabilities and put in place the necessary safeguards and support.

Related content

Contents

Responsibilities under the Data Protection Act

This page tells criminal investigators in Immigration Enforcement and suitably trained and accredited criminal investigators within the Home Office about criminal investigators' obligations under Part 3 of the Data Protection Act (DPA) 2018 and how they relate to data obtained from seized electronic devices.

The amount, depth and quality of data held on nearly every personal digital device seized from an individual in the course of a criminal investigation clearly constitutes 'personal data' as defined in DPA Section 3.

Processing that personal data for law enforcement purposes is permitted under DPA Part 3. That processing must be in accordance with the following 6 principles:

1. The processing of personal data for any of the law enforcement purposes must be lawful and fair.
2. The law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.
3. Personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.
4. Personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.
5. Personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.
6. Personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, 'appropriate security' includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

CFI officers need to be aware of the obligations under Section 39 Data Protection Act 2018 to regularly review the necessity to retain data during an investigation rather than just assessing the retention principles at the conclusion of an investigation. This is especially relevant regarding the retention of digital devices once the evidential data has been extracted or the case has been discontinued and consequently the device can be returned to the owner.

Data subject rights

Part 3, Chapter 3 of the DPA provides the following individual rights to data subjects:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure or restrict processing
- the right not to be subject to automated decision-making

Section 43(4) DPA sets out that subject access rights and the rights to rectification, erasure and restriction do not apply to the processing of 'relevant personal data' in the course of a criminal investigation or criminal proceedings.

'Relevant personal data' means personal data contained in a judicial decision or in other documents relating to the investigation or proceedings which are created by or on behalf of a court or other judicial authority.

For more information see Data Protection Policy - Criminal and Financial Investigation, Immigration Enforcement

Privacy Information Notice (PIN)

The purpose of a PIN is to inform the data subject why their data is being processed, what is being done to their data, by whom it is being processed, what their rights are, how they can exercise their rights, and if need be, how they can make a complaint. Provision of or access to the PIN directly supports compliance with the principle of fairness.

As a principle, data subjects, whether they are suspects, persons convicted of an offence, witnesses or victims should be informed of Home Office processing activity via a PIN at the earliest appropriate opportunity.

For a victim or witness this will usually be at the point at which they are first contacted or spoken to, and we process their data.

For a suspect, informing them of processing at the outset - prior to arrest - might obstruct or impede our investigation. Section 44 (4) Data Protection Act 2018 allows the right to be informed to be restricted in such cases. Therefore, it is likely that the first appropriate opportunity to inform them of their rights and our processing will be following their arrest, interview, or when a device or other property belonging to them is seized.

The Home Office has a PIN which covers data processing activity across Borders and Enforcement, including processing undertaken by CFI for law enforcement purposes. This can be accessed online at Borders, immigration and citizenship: privacy information notice.

All owners of seized devices must be issued with, or signposted to, the above PIN at the point of seizure, unless it has already been issued. This must be recorded on Clue, in the 'Privacy Info Notice given' field on the person record.

Criminal and Financial Investigation have additionally produced a series of Short PINs for service as a hard copy, to data subjects whose digital devices are seized in

circumstances where they would reasonably be viewed as vulnerable, given the manner in which they have been detected or encountered. This is likely to be relevant to those migrants identified as suspects or whose devices are otherwise seized when encountered in the back of lorries, or who arrive on small boats, or by other dangerous means.

The shortened PIN has been translated into the main languages of those nationalities which are encountered entering by clandestine means. Service of this shortened PIN supports compliance with the principle of fairness, given that a digital device, such as a phone is considered to contain information which is sensitive, and any loss of access to a device may have a significant impact on the owner.

Official – sensitive: start of section

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

Official – sensitive: end of section

Legal basis for processing

The processing of such data will be in accordance with section 35 of the Data Protection Act. Section 35 sets out that ‘consent’ or ‘strict necessity’ are the only lawful bases for law enforcement processing.

Due to the stringent conditions required for processing by ‘consent’ to be valid and legally defensible, it must **not** be relied upon in the context of data processing by CFI. Processing should **only** be undertaken on the basis of strict necessity for a law enforcement purpose.

For full guidance in relation to Data Protection, see:

- Data Protection Policy (CFI)
- Managing and protecting information and data.

Data breaches

To comply with the sixth data protection principle (security), CFI investigators must follow Home Office policy on reporting data breaches. This includes any incident involving the loss of confidentiality, integrity, or availability of personal data, whether on seized digital devices, in other records (for example, pocket notebooks), or during handling and extraction.

Investigators must report any potential breach as soon as it is identified, using the Home Office's Data and Security Incident Reporting process. This applies to both suspected and confirmed breaches. For more information see Report a data breach or incident.

Related content
Contents

Extraction and review process

This section tells criminal investigators in Immigration Enforcement and suitably trained and accredited criminal investigators within the Home Office about Criminal and Financial Investigation (CFI) how to lawfully extract data from digital devices.

Official – sensitive: start of section

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

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

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

Official – sensitive: end of section

Related content
Contents

Retention and deletion of data

This section tells criminal investigators in Immigration Enforcement and suitably trained and accredited criminal investigators within the Home Office about Criminal and Financial Investigation (CFI) about retaining and deleting data that has been lawfully extracted from digital devices during the course of a criminal investigation.

Data retention

NPCC Guidance on Management of Physical and Digital Evidence states that 'evidence' refers to 'physical property or digital data / media downloaded / recovered which could potentially form part of the evidence of a criminal offence and which may become a court exhibit in any judicial proceedings', and as such, downloads of mobile phones and other devices should be considered as evidence for the purpose of retention, and subject to the requirements of the Criminal Procedure and Investigations Act (1996) and Police and Criminal Evidence Act 1984 (in England and Wales).

Official – sensitive: start of section

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

Official – sensitive: end of section

Deletion of data

Where there is no lawful basis to retain data extracted from a seized digital device – following a 'no further action' outcome of a case, for example - then the investigation team must ensure that all copies of that data they hold are promptly marked for deletion.

Official – sensitive: start of section

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

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

Official – sensitive: end of section

Related content
Contents

Criminal Procedure and Investigations Act (CPIA) Code of Practice

This section tells criminal investigators in Immigration Enforcement 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, particularly when dealing with large volumes of data obtained from seized digital devices.

The CPIA Code of Practice provides guidance concerning the duty to pursue all reasonable lines of enquiry, in relation to digital material. The Criminal Procedure and Investigations Act 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
- Attorney General's Guidelines on Disclosure 2024 Annex A - Digital Material

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 investigation strategy.

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

For more information see Disclosure (CPIA).

Related content
Contents