Home Office

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

Version 2.0

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, extract and retain digital devices from suspects 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 digital devices from suspects in criminal investigations and their obligations under the Data Protection Act (DPA) 2018 and the Criminal Procedure and Investigations 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 they obtain personal digital devices – most often mobile phones – from suspects and then process data 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 should have when obtaining and handling sensitive personal information, in accordance with obligations under data protection legislation.

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

- Attorney General's Guidelines on Disclosure 2020 Annex A – Digital Material
- Criminal Procedure and Investigations Act Code of Practice 2015
- Criminal Procedure and Investigations Act 1996 Code of Practice 2020
- Investigatory Powers Act 2016
- APP Extraction of material from digital devices (college.police.uk)
- Information Commissioner's Office Report – Mobile Phone Data Extraction
- Data Protection Act (DPA) 2018

This guidance deals with the principles applicable to acquiring digital devices extracting data and the retention of such devices.

For further information see: Search of person.

For officers in Scotland and Northern Ireland also see Part 3 Immigration Act 1971 Sections D to H:

- 28D entry and search of premises
- 28E entry and search of premises following arrest
- 28F entry and search of premises following arrest under s25, 25a, 25b
- 28FA Search for personnel records: warrant unnecessary
- 28FB Search for personnel records: with warrant
- 28G Searching arrested persons
- 28H Searching persons in police custody

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 Stephen Blackwell.

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 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 also see: Home Office data protection guidance held on Horizon.

Publication

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

- version **2.0**
- published for Home Office staff on **23 September 2022**

Changes from last version of this guidance

- new guidance
- for the old version of this guidance see: Immigration Enforcement digital device extraction policy

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.

Investigators will need to consider the practicalities of 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 for law enforcement purposes 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

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 Annex A-Digital Material of 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 Part 2 of the Criminal Justice and Police Act 2001 apply.

Related content
Contents

Statutory powers to seize digital devices

This section tells criminal investigators in Immigration Enforcement and suitably trained and accredited criminal investigators within the Home Office 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.

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

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 applies a number of statutory seizure powers in the Police and Criminal Evidence Act 1984 to immigration officers carrying out criminal investigations.

As a matter of policy and following a Parliamentary undertaking to that effect, this limited subset of PACE powers can be exercised only in relation to investigations carried out by immigration officers, and by those immigration officers who are suitably trained and accredited to use them. The circumstances in which these powers can be exercised include:

- Section 18 Police and Criminal Evidence Act 1984 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 of seizure and retention. see CFI officers, power of entry, search and seizure under s18 PACE
- Section 8 Police and Criminal Evidence Act 1984 Subject to the issuing of a relevant warrant, powers of seizure and retention are exercisable for the purposes of that warrant. see CFI officers, search and seizure under s8 PACE
- Section 19 Police and Criminal Evidence Act 1984 general powers, when an immigration officer is lawfully on a premises, to seize anything on that premises 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, lost altered or destroyed.
    - All three of these powers 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 (section 20 of PACE adds this power to sections 8 and 18).
- Section 32 Police and Criminal Evidence Act 1984 where a person has been arrested other than at a police station, search powers are conferred in relation

to, amongst other things, anything which may be evidence relating to an offence, alongside power to seize and retain anything found, see: CFI officers, search a seizure under s32 PACE

CFI officers' powers of entry, search and seizure under Section 8 of the Police and Criminal Evidence Act (PACE) 1984

Under Section 8 Police and Criminal Evidence Act 1984 CFI officers can apply to a justice of the peace for a section 8 warrant to enter and search premises for evidence likely to be of substantial value to an investigation of an indictable immigration offence. There must be reasonable grounds for believing that there is evidence relating to that offence, or to another connected or similar indictable offence, on the premises. Section 8(2) PACE provides that immigration officers may seize and retain anything for which a search has been authorised under the warrant.

For more information about what should be considered by all CFI officers when submitting Police and Criminal Evidence Act (PACE) warrant applications and production orders in the course of a criminal investigation see: Search warrants and production orders.

If you are an immigration officer in **Scotland and Northern Ireland**, you use the same Part 3 powers under the Immigration Acts as immigration officers in other parts of the UK. These remain the main powers you use to apply for a warrant. In **Scotland** for offences, such as trafficking, contained within section 14 of the Asylum and Immigration (Treatment of Claimants, etc.) Act 2004 general evidence warrants for investigations may be obtained from a Sheriff with the application submitted by the procurator fiscal. Immigration officers may seize and retain anything for which a search has been authorised under the warrant.

CFI officers' powers of entry, search and seizure under Section 9 of the Police and Criminal Evidence Act (PACE) 1984

Under Section 9 Police and Criminal Evidence Act 1984 CFI officers may apply to a judge to order access to excluded or special procedure material under Schedule 1 of PACE if one or more of the sets of access conditions are satisfied. Under paragraph 13 Schedule 1 PACE, CFI officers may seize and retain anything for which entry and search has been authorised by the warrant issued under paragraph 12 of that schedule.

The first set of conditions include:

- An indictable offence has been committed
- that there is material which consists of special procedure material or includes special procedure material and does not also include excluded material on premises specified in the application

- that the material is likely to be of substantial value (whether by itself or together with other material) to the investigation in connection with which the application is made
- that the material is likely to be relevant evidence

The second set of conditions include:

- there are reasonable grounds for believing that there is material which consists of or includes excluded material or special procedure material on premises specified in the application
- but for section 9(2) a search of for that material could have been authorised by the issue of a warrant to a constable under an enactment other than this Schedule
- the issue of such a warrant would have been appropriate

For further information and the full set of conditions see: Schedule 1 Special Procedure Police and Criminal Evidence Act 1984.

CFI officers' powers of entry, search and seizure under Section 18 of the Police and Criminal Evidence Act (PACE) 1984

Under Section 18(1) Police and Criminal Evidence Act 1984 CFI officers have the power to enter and search the premises occupied or controlled by a suspect who has been arrested for an indictable offence. Under Section 18 (1) there must be reasonable grounds for suspecting that there is evidence relating to that offence, or to another connected or similar indictable offence, on the premises. Under section 18(2) PACE immigration officers may seize and retain anything for which they may search under section 18(1) PACE. It should be noted that section 18(3) specifies that the power to search conferred by section 18(1) is only a power to search to the extent that is reasonably required for the purpose of discovering such evidence.

This search must be authorised in writing by a Chief Immigration Officer (CIO) or above. Where the presence of the suspect is necessary at the premises for the effective investigation of the offence, authorisation is not required: see Section 18 (5) PACE. However, an officer of CIO or above must be informed as soon as practicable after the search has been carried out.

CFI officers' powers of, search, seizure and entry under section 32 of the Police and Criminal Evidence Act (PACE) 1984.

Under Section 32 Police and Criminal Evidence Act 1984 CFI officers may search a person upon arrest when the arrest has taken place anywhere other than at a police station. Under section 32(1) CFI officers may search that arrested person if the officer has reasonable grounds for believing that the arrested person may present a danger to himself or others. Under section 32 (2) (a) CFI officers may search the arrested person for anything:

(i) which he might use to assist him to escape from lawful custody; or
(ii) which might be evidence relating to an offence

It does not require any authorisation and the decision to conduct such a search is that of the investigating officer. An immigration officer may seize and retain anything, other than an item subject to legal privilege, they find during a search of person if there are reasonable grounds for believing:

- the person searched might use it to cause physical injury to himself or to any other person [section 32(1) search]
- they might use it to assist him to escape from lawful custody [section 32(2)(a) search]
- it is evidence of an offence or has been obtained in consequence of the commission of an offence [section 32(2)(a) search]

CFI officers also have the power under section 32(2)(b) to enter and search any premises in which the arrested person was when arrested (includes a vehicle) or immediately before they were arrested for evidence relating to the offence if that offence was indictable (this includes either way offences). In all cases where a person has been arrested for an offence the arresting officer should consider whether it is necessary and proportionate to conduct a section 32 premises search.

CFI officers' general power of seizure under section 19 of the Police and Criminal Evidence Act (PACE) 1984

Under Section 19 Police and Criminal Evidence Act 1984 if an immigration officer is lawfully on premises, they may seize anything (other than an item subject to legal privilege) that is on the premises if:

- they have reasonable grounds for believing that it was obtained as a result of the commission of an offence
- it is necessary to seize it to prevent it from being concealed, lost, damaged, altered or destroyed

Under section 19 PACE an immigration officer may seize anything which is on the premises if they have reasonable grounds for believing both:

- that it is evidence in relation to an offence which they are investigating or any other offence
- that it is necessary to seize it in order to prevent the evidence being concealed, lost, altered or destroyed

This is the power used to seize anything relevant to an investigation found during a section 32(2)(b) premises search.

Nothing in section 19 PACE is to be read as authorising the seizure of an item which an immigration officer exercising the power has reasonable grounds for believing to be subject to legal privilege.

Human Rights Act

Search, seizure and retention powers relating to persons and premises under the PACE powers set out above are likely to engage an individual's human rights under Article 8 (respect for private and family life) and Article 1 and Protocol 1 (protection of property) see: Article 8 Human Rights Act 1998. Before any such search is carried out those conducting and/or authorising must be satisfied that the search is both necessary and proportionate to the offence under investigation.

It is essential that officers have a sound knowledge of their powers of entry and search and if necessary should refer to PACE Code B (accessible) GOV.UK to refresh their knowledge

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.

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

Additional powers of seizure available

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 (accessible) GOV.UK 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.

Where material is removed under Section 50 or Section 51, a written notice under Section 52 (counterfoil copy from the Property Search Book (PSB)) should be

provided to the occupier or person from whom the material has been seized, setting out:

- what has been seized
- grounds for seizure
- how a person with relevant interest can apply under Sections 59 to 61 Criminal Justice and Police Act 2001 for the material to be secured or returned

Officers must also ensure the requirements of Section 53 Criminal Justice and Police Act 2001 are satisfied, including that seized property is assessed promptly for relevance and material for which there is no power to retain must be separated and returned as soon as is practicable.

Due regard should be given to allowing the person with an interest in the property to be present or represented at the examination Section 53(4) Criminal Justice and Police Act 2001 See PACE Code B (accessible) GOV.UK paragraph 7.12.

CFI Officers must only exercise these powers when it is essential to do so. Officers must not remove more material than is necessary. Where practicable, copies should be taken, rather than originals removed.

Under Criminal Justice and Police Act 2001 an initial examination of the material should be carried out as soon as reasonably practicable after the seizure.

The examination should be confined to whatever is necessary to determine how much of the material can lawfully be seized.

Until the material seized under Section 50 or Section 51 of the Criminal Justice and Police Act 2001 has been examined and separated, it must be kept separate from any other material seized under any other power.

If legally privileged material is mixed with other material, and if it is not reasonably practicable to separate the material on the premises, officers are lawfully entitled to seize it under CJPA section 50. This may be where privileged and non-privileged material are mixed together on a phone or computer hard drive. In this case, the examination and separation of the material should be undertaken by independent legal counsel.

Section 10 Police and Criminal Evidence Act 1984 defines legally privileged material when in the possession of a person who is entitled to its possession, as communications between:

- a legal adviser and his client or a person representing his client made in connection with giving legal advice to the client
- a legal adviser and his client or a person representing his client, made in connection with, or in contemplation of, legal proceedings and for the purposes of such proceedings

- a legal adviser or his client or any such representative and any other person and made in connection with, or in contemplation of legal proceedings and for the purposes of such proceedings
- items enclosed with, or referred to in such communications and made:
  - in connection with giving legal advice
  - in connection with, or in contemplation of, legal proceedings and for the purposes of such proceedings

Section 10(2) Police and Criminal Evidence Act 1984 states that Items held with the intention of furthering a criminal purpose are not items subject to legal privilege.

For further information on CFI search and seizure powers see: Search warrants and production orders.

CFI officers retention powers under the Police and Criminal Evidence Act 1984

Section 22 Police and Criminal Evidence Act 1984 provides the power to an immigration officer, having lawfully seized an item in a criminal investigation under the act to retain the item for specified purposes for either:

- use as evidence at a trial for an offence
- forensic examination or for investigation in connection with an offence

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.

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 should be restored to the owner.

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

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 and Digital Capabilities**. See: CFI Specialist Capabilities Team.

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, but only where in the particular circumstances of the individual there are identifiable reasonable lines of enquiry to obtain evidence which justify the request or seizure of the device.

Investigators should be clear if there are identified lines of enquiry, consideration must be given to the following factors in deciding whether seizing the phone is appropriate:

- whether seizure of the phone is 'necessary', as opposed to 'strictly necessary', see: Annex D necessity test Attorney General's Guidelines on Disclosure 2020. - this requires, amongst other matters, an assessment of alternative means of pursuing the lines of enquiry/securing the information
  - some examples of alternative means are but not limited to, Service Provider Data, Open Source, CCTV and Other digital devices already seized using a statutory power
- the practicalities of requesting or seizing devices, in particular, to the number of devices that are to be seized and the current time frame for review and return of the device – if, for example, due to resource constraints or back log it is unlikely to be possible to review or take a copy of the material on the device within a reasonable period of time, this would be a factor pointing against seizure

Requesting a PIN number from a suspect where a device has been seized

A request for a PIN number in order to facilitate the search of a device does not constitute an interview for the purposes of PACE. The request for a PIN number for the purpose of searching a device is similar to requesting a key to access a premises or cupboard, etc. for the purpose of search and, as such, the request does not amount to a PACE interview.

Criminal investigators within Immigration Enforcement **must** familiarise themselves with the guidance outlined in the: Investigation of protected electronic information policy - Section 49 policy. Prior to requesting a PIN number from a suspect.

Retention and Obligations 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 retainsaid 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

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.

The Data Protection Act 2018 outlines six data protection principles which must be followed when processing data for Law enforcement purposes, including when exercising powers under Part 3 of the Data Protection Act 2018 these principals are summarised below:

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).

To Note: 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 principals 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 NFA’d and consequently the device can be returned to the owner.

Full guidance in relation to Data Protection and the General Data Protection Regulation can be found at Data Protection Policy: Criminal and Financial Investigation (CFI), Immigration Enforcement also see: Data protection guidance on Horizon.

Related content

Contents

Digital Device Extraction policy: CFI requirements under ISO17025 Standard

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) standard operating procedures under ISO17025.

Criminal and Financial Investigation (CFI) ISO17025 standard operating procedures dictate that all devices subject to examination or that are in the possession of CFI must be recorded on the Clue case management system. Any request for data extraction must be processed and authorised using the CLUE tasking system.

Official – sensitive: start of section

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

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

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

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.

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
- Attorney General's Guidelines on Disclosure 2020 Annex A - Digital Material
- Disclosure of evidence: Guidance for specialist reporting agencies

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 in England and Wales must be set out in an Investigation Management Document (IMD) to feed into the CPS Disclosure Management Document (DMD).

Related content
Contents