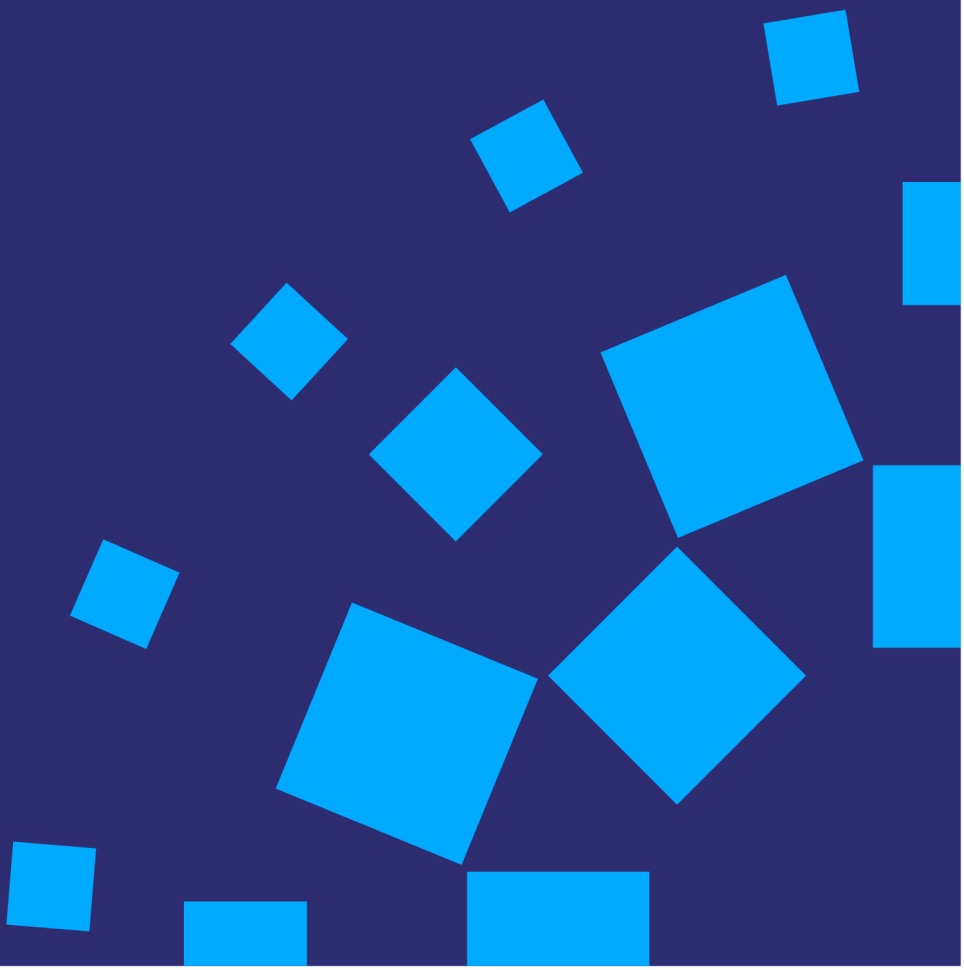
College of Policing

Working together to keep people safe

Authorised Professional Practice: The extraction of digital data from personal devices

Draft version 3.0 October 2020



college.police.uk

This publication is available for download at **beta.college.police.uk/article/consultation-extracting-data-electronic-devices-released**

If you have any enquiries regarding this publication, please email **Vulnerability@college.pnn.police.uk**

This document has been created with the intention of making the content accessible to the widest range of people, regardless of disability or impairment. To enquire about having this document provided in an alternative format, please email **Vulnerability@college.pnn.police.uk**

Contents

Introduction

Background

In recent years, mobile phones and other digital devices have come to play an increasing part of daily life. They are being used for a wide range of functions in addition to communication – from personal banking to recording health and fitness data and storing photographs. As a consequence of their prevalence, data from digital devices is increasingly used as evidence in criminal investigations and prosecutions. Concerns have been raised by interest groups and privacy campaigners that the extraction of data from these devices is excessive: amounting to a 'digital strip search'. **Privacy groups** and others representing **victims of rape and sexual violence** who are disproportionately affected by the intrusion, called for an urgent review of police use of mobile phone data.

In August 2018, the Information Commissioner's Office (ICO) launched an investigation into the use of data extracted from mobile phones of victims, witnesses and suspects by law enforcement agencies during the course of a criminal investigation. The ICO **concluded** that the police have not been abiding by the obligations of the DPA 2018 in their extraction of data from these devices as part of investigations.

Recommendation 1 of the **ICO report** states:

> 'Given the complexity of this area, the Commissioner is calling for the introduction of better rules, ideally set out in a statutory code of practice, that will provide greater clarity and foreseeability about when, why and how the police and other law enforcement agencies use mobile phone extraction.'

In addition, the Court of Appeal considered the issues in the case of R v Bater-James and Mohammed [2020] EWCA Crim 790. Police practice must now reflect both this **Court of Appeal judgement,** and the recommendations of the ICO.

Aims of the Authorised Professional Practice (APP)

This APP sets out the powers and obligations on the police under the Data Protection Act 2018 and how these interact with other relevant legislation and case law. It provides police officers and staff with a set of principles to inform 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 will also help the public to understand the responsibilities of the police to gather evidence, access devices and the data held on them.

The powers to acquire a device are different to those that apply to the data on the device. Acquisition of the device would be under common law consent. In most investigative circumstances, officers or staff will be intending to take the device for the purposes of extracting data. Investigators should be considering and explaining the power to acquire the device and the power to acquire the data at the same time, therefore officers and staff should apply both the common law consent to the physical device and DPA 2018 requirements for the data. Consequently officers and staff will:

- seek consent for the acquisition of the device

  and

- believe acquisition of the data to be **strictly necessary** to satisfy a reasonable line of enquiry

  and

- consider all other less intrusive means and decide that they are not able to provide the evidence in a way that will support the investigation of a reasonable line of enquiry

  and

- seek informed, freely given permission to acquire the data

The **Code of Practice to the Criminal Procedure and Investigation Act 1996 (CPIA 1996),** makes clear that all reasonable lines of enquiry should be pursued, whether they point towards and away from a suspect[1]. The criminal justice system seeks to establish fair and just outcomes for victims, witnesses and suspects.

This APP aims to ensure that, where possible, obtaining evidence from mobile phones and other digital devices is done with permission, complies with the relevant legislation and balances the individual's rights to privacy with the rights of all individuals to a fair trial. In a small number of cases, evidence may be obtained from a victim or witness without their permission. This may happen when it is in the public interest, for example, where it is vital to prevent a dangerous offender committing further offences. The police will need to obtain a court order in these cases. See **Principle 4** for further information.

The College has developed an Equality Impact Assessment {insert link} and this will help forces in developing their own EIAs for implementation of this APP.

Definitions

Permission – Throughout the APP we refer to 'permission' to acquire data. This is because there is a particular meaning for **'consent'** within the DPA 2018. Consent can only be given when the giver of that consent is fully informed. Advice from ICO is that consent cannot be fully informed in police investigations because it is unlikely that the full use of the data can be known at the point consent is sought. In addition, because of the authority of police in society, there is a power imbalance between the police officer/staff seeking consent and the data owner. Investigators will only seek data from devices when it is 'strictly necessary'. They will also seek permission.

Device owner – Throughout this document the phrase 'device owner' is used to indicate the person from whom permission is to be sought. In some situations the officer/staff may have to get authority from more than one person where for example the device may be owned by one person but the data on it belongs to someone else

[1] A revised Code is before Parliament at the time of writing. The requirement to investigate towards and away from a suspect remains.

eg, parent owner, child user or where an organisation owns a device but an employee uses it or where a device is shared.

Irrelevant material – This is data that may be acquired from a device that has no relevance at all to the investigation. It may be inadvertently acquired when applying searches to material on a device and more data than is required to satisfy the reasonable line of enquiry is returned. Additionally, some search technology cannot be applied to data held on a device and requires a total download of all information into a digital repository. The searching technology is then engaged, using carefully constructed search terms. The data that is not recovered in the search is irrelevant material and should be managed according to the principles in this APP. 'Irrelevant material' is not the same as 'unused material' – See CPIA 1996 for the definition of 'unused material'.

Summary – Principles for the extraction of digital data for the purposes of an investigation

For further detail on each of the principles please click the links provided.

Principle 1 – Strictly necessary and avoiding unnecessary intrusion. Data will only be extracted from a personal digital device if it is strictly necessary for an investigation. Intrusion into the personal or family life of device owners will be avoided wherever possible. Only the minimum data that is strictly necessary will be extracted.

Principle 2 – Provision of information. Where data is extracted from a personal digital device, investigators will provide full and clear details about the data extraction to the device owner.

Principle 3 – Requesting permission. Investigators will ask the device owner for permission to take possession of the personal digital device for the purpose of data extraction.

Principle 4 – The right to refuse. The device owner has the right to refuse permission for digital data to be extracted from their personal digital device. There are some exceptions to this principle.

Principle 5 – Deletion of irrelevant material. Investigators will extract and examine the minimum data required to satisfy the reasonable lines of enquiry. Any information or material irrelevant to the investigation will be deleted without undue delay.

Principle 6 – Safeguarding. Investigators will consider risk of harm and any issues which could have adverse impact on the device owner when deciding how to extract data.

Principle 7 – Updating, reviewing and managing. Investigators will review the retention of digital devices and the extracted data at regular intervals. The storage, retention and disposal of data extracted from a digital device will be managed in line with data protection legislation and will be retained for no longer than necessary. The investigating officer will inform the victim or witness of any proposal

to change the processing of data extracted or the use of that data and request further permission for any such changes.

Principle 8 – Sharing information. Investigators will not disclose personal information unless it is strictly necessary to do so as part of the investigation or prosecution for which the data was extracted.

Principle 9 – Recording actions. All actions including information provided, permission given, decisions and approvals given about the extraction of data from a personal digital device will be recorded including any changes and any refusals.

Principle 10 – Implementation. Chief officers are responsible for implementation of these principles and will ensure their officers and staff have the skills and knowledge to implement the principles and that a Data Protection Impact Assessment and Equality Impact Assessment of all relevant investigative processes are undertaken.

Responsibilities by role

The table below sets out, by role, the responsibilities of police officers and staff under the DPA 2018 and other relevant legislation. In some cases – for example volume and priority crime investigations, the first responder will also be the investigator and in this case they will carry out the responsibilities for both roles.

Role	Responsibilities
First responders	Where a first responder seeks to take possession of a personal device in the initial stages of an investigation. They will: ▪ Consider if there are reasonable grounds to believe that a search of a personal device may reveal material relevant to the investigation, ie, is it a reasonable line of enquiry. ▪ Consider whether it is strictly necessary, as **a reasonable line of enquiry**, to take possession of a personal device to extract digital data. Other options will be considered. For example, it may be possible to obtain material from another source, such as communications data for the victim or suspect's mobile phone to indicate the location of an incident. Also consider CCTV, witnesses, or other sources of material. It is important to consider whether a proposed measure fulfils evidential requirements and retains the required evidential integrity. Manual examination, including screenshots, will be considered when: o There is minimal material which would be of significant evidential value. o Material on devices may be lost if not captured immediately. o Volatile material is present, ie, data that might be lost if the device is turned off; or

	○ The device owner does not give permission for the device to be taken, leaving screenshots as the only available option to secure a record of the material. **See also The Attorney General's Guidelines on disclosure Annex A.** ▪ Consider what data is likely to be on the device, and whether there is a less intrusive method to obtain that material while maintaining integrity and continuity of the material and the potential corroborative value, for example, screen shots or screen images. ▪ Consider whether the device owner has capacity to provide permission for the police to take possession of the personal device or is incapacitated, for example: ○ Is the victim/witness injured or traumatised? ○ Is the victim/witness intoxicated ○ Is the victim/witness a child? ○ Does the victim/witness have other impairments that may impact on their capacity, for example, cognitive impairment, neurodiversity issues, experiencing a mental health crisis? Where the device owner lacks capacity or is incapacitated, consider what steps can be taken to support them to fully understand the implications of the request. Seek alternative or additional permission if the person lacks capacity, for example, from a carer, parent/guardian or legal representative. If there are reasonable grounds to believe material may be lost, the device can be retained by the police until permission is obtained. See **here** for a brief guide to capacity and consent in the under 18s.

	▪ Consider any safeguarding requirements for the victim/witness. In particular whether taking their device might further compromise their safety and what safeguards need to be put in place. ▪ Inform the device owner about the following: This could be done by providing a copy of the **NPCC agreed Data Processing Notice** (DPN). o Why data on the device is required o The lawful basis for taking possession of and examining the device o How the data will be extracted/processed o When the device is likely to be returned to them o Their rights to refuse and to make complaints to the ICO; and o Who they should contact if they have any questions or concerns. ▪ Ask permission – taking possession of a personal digital device should be a consensual process (see below for actions that should be taken if permission is not given). ▪ Agree updating arrangements – ask how frequently the device owner would like to be updated on the investigation and how. Ensure updating arrangements are carried out as agreed. Tell the device owner of any changes to the police contacts if the case is passed on. Record this information of the crime report. ▪ Record decisions/actions – The first responder will log the decisions taken and the permission given on the relevant forms for example the NPCC approved DPN and/or body worn video (BWV). ▪ Seek inspectors' authority for the extraction of data for the device.

	▪ Return the device – Where the first responder still has possession of the device, return the device as soon as the required data has been extracted to the device owner. Inform the device owner that it is possible further examination may be required if new lines of enquiry emerge, and advise the device owner that they should not to delete or amend any data that could be relevant to the investigation. When telling owners about data retention you will need to use your professional judgement to determine what might become relevant. This will be based on best available information at the time. Responders and investigators cannot acquire data from a device in anticipation of a future line of enquiry. Device owners, however, may be aware of or become aware of data on their device that may be relevant to the investigation. They should be advised not to delete or alter that data. ▪ Delete extracted irrelevant material – Where the first responder has extracted data that cannot have a bearing on the investigation it should be deleted without undue delay. See **Code of Practice to the Criminal Procedure and Investigative Procedures Act 1996** (CPIA 1996) for further information on unused material.
	If the device owner **does not permit** the device to be taken, the first responder will: ▪ Further 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. If the responder thinks it is necessary for the police to have access to the data, an Inspector will be consulted to decide whether the matter under investigation and/or prosecution is so significant or serious that it is necessary for

	the police to have access to the data. The inspector can then authorise an application for a legal power 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.
Investigators	Investigators will: ▪ Seek authorisation from an Inspector before downloading relevant data from the device. ▪ Provide search criteria to digital forensic practitioners. Investigators will ensure search terms are well defined and appropriately focused to extract only what is necessary and relevant to the line of enquiry. The technical solutions that forces have access to will vary and investigators may be able to undertake a limited extraction themselves where technology will allow. ▪ Review and develop lines of enquiry. If further data is required for example to pursue further lines of enquiry or after a suspect is identified, the investigator will inform the device owner and ask for permission to extract the additional data, as set out in Bater-James.R v Bater-James and Mogammed {202} ECWA Crim 790Delete extracted data that cannot have a bearing on the investigation without undue delay. See Code of Practice to the CPIA 1996 for detail on unused material. ▪ Ensure that all safeguarding risks are identified and mitigated if the victim or witness does not have their personal digital device. Investigators will also consider how the extracted data could increase risk to the victim or witness or may affect their private life or relationships. ▪ Only share data with CJS partners that is relevant to the investigation. If a request for data is received from another CJS organisation or the defence, and the requested data is not supported by a reasonable line of enquiry, the request must be investigated. Liaise with CPS or force solicitors if necessary. If there is no

	reasonable line of enquiry, the request must be refused, in accordance with Bater-James Follow force escalation policies if necessary. ▪ Update the device owner at regular intervals as agreed with them. The investigator will provide updates on the progress of the investigation, in particular significant developments in the case. ▪ Provide support and advice to first responders on how to apply this guidance.
Supervisors	Supervisors will: ▪ Ensure that all reasonable lines of enquiry have been identified and are being followed and that personal digital devices are only requested when strictly necessary to do so and when less intrusive methods have been considered. ▪ Ensure that first responders are aware of and follow the APP and are supported to implement it. ▪ Ensure that failures to follow the APP are reviewed and action is implemented to prevent repeated failures. Supervisors will follow local processes and procedures to develop the knowledge and skills of the first responders.
Inspectors	Inspectors will be responsible for authorising applications to lawfully obtain data from a personal digital device when a device has been taken possession of. They will ensure: ▪ Authority is only given when they are satisfied that the personal digital device, and the data on it, is strictly necessary for reasonable line of enquiry. ▪ Less intrusive methods of obtaining the data have been considered.

	They may also be asked to authorise warrants to obtain devices where permission to take possession of the device has been refused and it is in the public interest to do so. Along with the responsibilities associated with authorising an application for a warrant, they will also consider whether strict necessity and minimal intrusion as described above have been considered. Inspectors will record their decisions, the rationale and the **strictly necessary** criterion.
Staff in Specialist Digital Forensic Units	Specialist Digital Forensic Investigators will: ▪ Ensure that only the minimum data required to satisfy the line of enquiry is extracted, using the least intrusive methods, subject to the capability of the available technology. They will liaise closely with the investigator to ensure that only the minimum data is extracted. ▪ Ensure irrelevant material is deleted without undue delay once the required data has been identified and retained as evidence, relevant or unused material. ▪ Ensure the extraction was carried out in a timely way so that the device is returned to the owner as soon as practicable? ▪ Record how the extraction was undertaken and the methods used. ▪ Ensure the extracted data is stored securely in accordance with the DPA 2018, the **CPIA 1996** and **Management of Police Information (MOPI)**. The extracted data will not be shared with anyone other than the investigator or other authorised persons.

Chief Officers	Chief officers should: ▪ Implement this APP – ensuring all officers and staff are aware of this APP and have the skills and knowledge to implement it. ▪ Ensure an Equality Impact Assessment (EIA) is carried out on all local investigative and data extraction policies. ▪ Ensure that a Data Protection Impact Assessment (DPIA) is carried out on all relevant local investigative policies governing processing data extracted from personal digital devices. See NPCC DPIA template {insert link} ▪ Ensure that the force implements technology that supports staff to follow this APP, taking into account the changing nature of extraction technology, the changes in devices and software and cost. ▪ Ensure that procurement and/or roll out of new hardware or software for data extraction from personal digital devices is undertaken with 'privacy by design' principles in mind. • Ensure that data protection officers are involved in any new projects involving the procurement or use of technology for processing personal data to ensure the force complies with relevant legal obligations. • Ensure that an appropriate policy document for sensitive processing of data is developed and implemented.

Principles for the extraction of digital data for the purposes of an investigation

Principle	Detail
Principle 1 – Strictly necessary and avoiding unnecessary intrusion. Data will only be extracted from a personal digital device if it is strictly necessary for an investigation. Intrusion into the personal or family life of device owners will be avoided wherever possible.	**Victims, witnesses and suspects** Mobile telephones or other digital devices will not be examined as a matter of course. They will only be examined in investigations where there is reason to believe that it is **strictly necessary** to acquire data to pursue a reasonable line of enquiry. However, for an investigation to proceed and be fair to the victim, witness and suspect, all reasonable lines of enquiry must be pursued, whether they point towards or away from the suspect[2]. Where data is required from a personal device only the minimum strictly necessary material will be extracted. The 'strictly necessary' condition can only be satisfied where all other **less intrusive means** of following a reasonable line of enquiry have been explored. Investigators will consider whether it is sufficient simply to view limited areas (for example, an identified string of messages/emails or particular postings on social media) or take screenshots without taking possession of, or extracting data from the device. Alternatively, data may be available on the suspect's device. It is important to consider whether a proposed measure fulfils evidential requirements and retains the required evidential integrity. Manual examination, including screenshots, will be considered when:

[2] This legal duty is found in section 23 of the Criminal Procedure and Investigations Act 1996 and in paragraph 3.5 of the Criminal Procedure and Investigations Act 1996 Code of Practice.

Only the minimum data that is strictly necessary will be extracted.	▪ There is minimal material which would be of significant evidential value ▪ Material on devices may be lost if not captured immediately ▪ Volatile material is present, ie, data that might be lost if the device is turned off; or ▪ The device owner does not give permission for the device to be taken, leaving screenshots as the only available option to secure a record of the material. **See also The Attorney General's Guidelines on disclosure Annex A.** Where a more extensive examination is required this will be done with a minimum of inconvenience and intrusion required to recover the relevant material. Intrusion will be minimised by the following: ▪ Use of defined and focussed searches of the device/data. A search cannot be speculative. The search must support one or more reasonable lines of enquiry. Victims, witnesses and suspects may help to identify reasonable lines of enquiry and/or material within the data on the device. The investigator will then need to apply the 'strictly necessary' test. ▪ Use the least intrusive method available including the most up-to-date techniques, software and equipment available; and ▪ disregard information irrelevant to the search terms and line of enquiry (except where additional serious offences are identified – see Principle 5).

	Suspects/defendants Once a suspect is charged, they are referred to as a 'defendant' and the investigation comes under the jurisdiction of the court and all of the rules and laws of the court process apply. Where police have carried out a search of a device and a suspect has been identified, the police will inform the suspect of the method(s) used to search the device, including the search parameters. The suspect may identify further methods to search the device, including suggesting new search terms. These must be precise so that a reasonable and proportionate search can be undertaken. A search cannot be speculative.
Principle 2 – Provision of information. Where data is extracted from a personal digital device, investigators will provide full and clear details about the data extraction to the device owner.	**Sensitive processing** It is likely that some information on a digital device will be considered sensitive under **Section 35(8) of the DPA 2018**, for example, personal data about; political opinions, religious or philosophical beliefs, trade union membership, information concerning an individual's sex life or sexual orientation. It is also possible that the data may relate to individuals other than the owner of the device. Police practitioners are unable to assess the nature of the data before viewing it, so they will assume that it is sensitive and comply with Part 3 DPA 2018. Sensitive processing applies to data obtained from victims, witnesses and suspects. Chief officers must ensure that an appropriate policy about sensitive processing is implemented.

	Victims, witnesses and suspects/defendants An **NPCC approved Digital Processing Notice** or similar will be provided to the device owner before a device is processed and data extracted. The Inspector's authority will also be noted on the DPN and the Inspector will need to record their rationale including the considerations of the 'strictly necessary' criterion. The notice will explain the following. ▪ **Legislation** – the lawful basis for taking possession of the device and extracting data. This may be different depending on the status of the device owner, ie, victim/witness or suspect. ▪ **Reason** – why the police need to take possession of the device. For example, to examine the device for material about an allegation made by the victim, or to pursue a reasonable line of enquiry. ▪ **Use** – how the information will be used. For example, material from the device may be used to support a prosecution and thereby prevent further offending. ▪ **Searching** – how the device will be searched, for example the parameters which will be used to pursue the line of enquiry and what that means when searching for and extracting data. For example; data will be limited to the time of the offence and to communications between victim and suspect identified by the victim. Searches cannot be speculative. ▪ **Length of time** – how long the device and data are likely to be held by the police. If taking possession of the device causes safety issues for the victim, witness or suspect the police will seek to minimise the impact, including where possible offering an alternative device. Devices will be returned without any unnecessary delay.

	▪ **Contact details** – how to contact the investigator responsible for the device and extracting the data. This will also include how to withdraw consent for having possession of the device and/or extracting data. ▪ **The individual's rights** – how to complain to the ICO and in particular their right to refuse – (See Principle 4 below). ▪ **Technical limitations** – explain how the technology will be used and what its limitations are, and that the police will use the best available technology and techniques to limit their examination of a device only to that strictly necessary for the line of enquiry. Technology is developing, both that used for data extraction and that used within the device. Police forces do not use a single form of technology, so the method of extraction and limitations will vary from force to force, for example, some technology cannot search material while it is on a device, and therefore the data must be downloaded so that a search tool can then be applied.
	Suspects/defendants When managing an individual's personal information the police will be as transparent as possible. However, for suspects and defendants, **S45(4) of the DPA 2018** gives data controllers the right to restrict this information if it is necessary and proportionate to do so, for example to avoid: ▪ obstructing an official or legal enquiry, investigation or procedure ▪ prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties This power will be considered to prevent the device owner tampering with or remotely accessing the device.

<table>
<tr><td rowspan="2">Principle 3 – Request permission
Investigators will ask the device owner for permission to take possession of the personal digital device for the purpose of data extraction.</td><td>Victims and witnesses

The investigator will consider who can give permission in cases where, for example, the device is shared, owned or used by different people. The investigator will also consider if the device owner has the capacity to give permission (see below).

In all cases, where the device and/or data is owned by a victim or witness, an inspector’s authority (or equivalent civilian grade) will be required to extract data from it because of the potential intrusion into a person’s private life.</td></tr>
<tr><td>Capacity to give fully informed permission

Consider whether the victim or witness has capacity to give fully informed permission for their digital device to be taken by the police and data to be extracted or is temporarily incapacitated due to injury, intoxication or trauma for example.

Specifically consider capacity where the device owner is: a child; an adult with cognitive impairment; a person for whom English is not their first language; the victim/witness has experienced trauma; the victim or witness is not present.

Where it is believed that the device owner may lack capacity or be incapacitated the investigator will ensure suitable support is available and where appropriate, contact details are provided so that support can be provided before permission is sought, for example, an appropriate adult, guardian, advocate, interpreter or legal representative.</td></tr>
</table>

	If the device owner is not present, consider whether it is 'strictly necessary' that data is extracted to support a law enforcement purpose. In urgent cases, consideration will be immediate and the decision will be recorded with supporting rationale. In other cases, seek the advice of an inspector or the CPS.
Principle 4 – The right to refuse permission. The device owner has the right to refuse permission for digital data to be extracted from their personal digital device. There are some exceptions to this principle.	Investigators will advise that victims, witnesses or suspects (who have not been arrested) have the right to refuse permission for their digital device to be taken by the police. The police will always seek the permission of the device owner, however, the police do have specific powers to seize material from suspects if they have been arrested. The police also have the power to seize material believed to be evidence when lawfully on premises. Permission is not required in these circumstances. Investigators will provide contact details for agencies and organisations who can advise the device owner.
	If permission is refused – victims and witnesses: ▪ Investigators will explain what will happen to their device if it is made available to the investigator. They will reassure the victim or witness, outline the procedure that will be followed and why the material on their device is important to the investigation. An individual may be vulnerable, for example, because of trauma or factors about their ethnicity, gender, sexuality or immigration status, and this may affect their willingness to share their data. ▪ Investigators will continue to investigate the case, considering alternative sources of material which may support the line of enquiry. The defence may seek to have charges dismissed where relevant evidence is not available.

	▪ Where the offence is so significant or serious, for example, homicide or rape, that it is necessary for the police to have access to the information, the investigator can apply for a warrant to seize the device and relevant data (see for example College of Policing Authorised Professional Practice on **search warrants).** An inspector will authorise applications for any such legal powers. ▪ Investigators will make a record of all actions and conversations about the refusal.
	Suspects The right to refuse permission also applies to suspects who have **not been arrested** and where other powers have been used to seize the device. The device and data may be acquired if a legal power such as a warrant exists.
Principle 5 – Deletion of irrelevant material. Investigators will extract and examine the minimum data required to satisfy the reasonable lines of enquiry. Any information or material irrelevant to the investigation will be	**Victims, witnesses and suspects/defendants** Investigators will only extract the minimum amount of data required to satisfy the line of enquiry. Any of the extracted data that falls outside of the search parameters will be deleted without undue delay. Where material has been extracted, but it is not relevant to the search, it will **not** be examined and will be deleted without undue delay. When data is extracted from a digital device, a copy is created of the data. It is the copied data that will be deleted, the original data will be retained on the device. In some cases this may be difficult because of the limitations of the technology, for example, where the material is protected by encryption or stored on a disc. **Where it is not possible to remove non-relevant data from relevant data, it should be retained securely and not subject to further processing.** Extracted data will fall into three categories:

deleted without undue delay.	▪ Evidence (used material) – this is material that will be used by the prosecution as evidence in the case and will be retained and disclosed under the **CPIA 1996**. See also **Management of Police Information (MOPI)** Code of Practice for information on storage and retention of police information. ▪ Unused, relevant material – although it is relevant to the case, this material will not be used by the prosecution. This may include material that may undermine the prosecution case, or assist the Defence – this material will be disclosed and retained under the **CPIA 1996**. ▪ Unused, non-relevant material – this material is not relevant because it is not capable of having a bearing on the case and is not used either as evidence, or disclosed as unused material and will be deleted as soon as possible. Where the extraction of strictly necessary data identifies material relating to offences not under investigation, this will be disregarded unless it relates to serious harm. For offences that are less serious than the initial investigation, officers will take a proportionate approach to any evidence of unrelated criminal activity found on the device. Before initiating an investigation into such activity consider: ▪ The seriousness of the offence being investigated set against the seriousness of the unrelated criminal activity. It is unlikely to be proportionate, for example, to investigate references to drug use, when dealing with a victim of serious sexual assault. ▪ Whether there is risk of harm to any person because of the unrelated criminality. ▪ Whether there is a risk a witness might disengage if they think they will be prosecuted for a minor offence, and the impact this may have to the current investigation, eg, the risk to public safety if an offender is not brought to justice.

	Where the investigation relates to a sexual assault a Detective Chief Inspector must authorise investigation of the unrelated criminal activity. Where material is recovered during a strictly necessary and proportionate examination of data and it indicates additional offences involving serious harm, it may be necessary to investigate those offences. The investigator will: ▪ seek advice from a supervisor ▪ in cases of doubt, seek advice from a CPS prosecutor or force solicitor. Where evidence of a serious offence is identified, the relevant data may be retained and investigated by the police. This data may be shared with other parties including, for example, other police forces or a court in any criminal proceedings in accordance with relevant data protection legislation.
Principle 6 – Safeguarding. Investigators will consider risk of harm and any issues which could have adverse impact on the device owner when deciding how to extract data.	**Victims, witnesses and suspects** Consideration will be given to any situational or personal factors which may be affected if the device owner permits the police to take possession of their device, in particular an increased risk of harm or impact in their private life. The lack of a mobile phone could, for example, affect the safety of a victim of coercive control and/or stalking. Alternatively, data on the device may highlight confidential personal information, for example, their sexuality, honour-based abuse, threats of violence and intimidation or the privacy of others whose information is included in the data on the device.

	Efforts will be made to mitigate those risks, including: not removing the device and taking screenshots of the relevant material at the time; returning the device to the owner without unnecessary delay; providing an alternative device where a risk assessment suggests it is necessary. All data will be stored securely and only accessed by those with a legitimate reason to do so. Only used and unused material meeting the CPIA 1996 disclosure test will be shared with the defence. Under the DPA 2018 disclosed material will be appropriately redacted so that personal details or other irrelevant information is not disclosed (eg, photographs, addresses or full telephone numbers).
Principle 7 – Updating, reviewing and managing. The retention of digital devices and the extracted data will be reviewed at regular intervals. The storage, retention and disposal of data extracted from a digital device will be managed in line with data protection	**Victims witnesses and suspects/defendants** During an investigation a new line of enquiry may develop and this may change how the data is used or require further data to be extracted and examined. This may include: ▪ Where the investigation has uncovered new material identifying new lines of enquiry, eg, where a suspect is arrested and, for example, an item of clothing is recovered. It may then be appropriate to examine photos on a victim's device to identify pictures of the suspect wearing the item of clothing. ▪ If data extracted from the device has been or will be shown to the suspect. ▪ If there is a decision-point in the case where the device is relevant, eg, a suspect is to be charged. The investigating officer will **inform** the victim or witness or suspect of any proposed changes and, in relation to victims and witnesses, seek renewed **permission** to extract or use the data. The victim/witness has **the right to refuse or withdraw their permission**.

legislation and will be retained for no longer than necessary The investigating officer will inform the victim or witness of any proposal to change the processing of data extracted or the use of that data and request further permission for any such changes.	Investigations can take a long time and a device may be required for a significant period until all relevant data has been extracted. The victim witness or suspect will be kept informed of the progress of the investigation at a period agreed with the victim/witness and using their preferred form of communication. They will also be informed of: ▪ the progress of the investigation ▪ any significant developments in the case, eg, the arrest of a suspect ▪ the use of the data on the device ▪ the likely timescales for return of the device and for the retention of any downloaded data A specific update timetable will be agreed. **Storage –** All data extracted from personal digital devices will be stored with effective safeguards in place to prevent unauthorised access or disclosure (the ICO report expects all extracted data to be stored in encrypted form).
Principle 8 – Sharing information. Investigators will not disclose personal information unless it is	**Victims and witnesses** Material will only be provided to the defence if it is part of the prosecution case or it meets the **test for disclosure**. It will be served in a suitably redacted form to ensure that personal details or other irrelevant information is not unnecessarily revealed (for example, photographs, addresses or full telephone numbers).

strictly necessary to do so as part of the investigation or prosecution.	All reasonable lines of enquiry will be pursued that point toward or away from the suspect. The defence must be shown all disclosable material which can include information extracted from digital devices. Only 'disclosable' material will be disclosed to the defence.
	Suspects/defendants Data from a suspect's device will not be shown to the victim or witness unless it is necessary as part of the investigation. Only data that forms part of a reasonable line of enquiry will be used. There is no obligation on the defence to disclose material to other parties in a criminal case.
Principle 9 – Recording actions. All actions – information provided, permissions given, decisions and approvals given about the extraction of data from a personal digital device will be recorded including any changes and any refusals.	**Victims and witnesses** **Section 62 of the DPA 2018** states that logs will be kept of all processing operations, for example all conversations with the device owner; all decisions made and any approvals given. This record could be in writing on a proforma (for example, the **NPCC approved DPN**) or as a verbal record recorded by body worn video. Where further requests for permission to extract and/or use the data are required because – for example, a new line of enquiry has developed or the use of the extracted data has changed – the response to these requests will also be recorded. If a device owner refuses to allow their device to be seized, or the data extracted, this decision will be logged outlining their reasons and including any associated conversation, and decisions.

	Suspects/defendants Suspects will be told when a new or revised search of their device is needed and how the data recovered will be used. When managing personal information, including a suspect's, the police will be as transparent as possible. **S45(4) of the DPA 2018**, however, gives data controllers the right to restrict information given to suspects if it is necessary and proportionate, for example, to avoid: ▪ obstructing an official or legal enquiry, investigation or procedure ▪ prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties This power will be considered to prevent the device owner tampering with or remotely accessing the device.

Principle 10 – Implementation. Chief officers are responsible for implementation of these principles and will ensure that their officers and staff have the skills and knowledge to	Chief officers will ensure that this guidance is implemented. This includes ensuring:
	
	▪ A data protection impact assessment (DPIA) is carried out on all relevant investigative processes and data processing operations. A DPIA will be completed:
	  ○ before the procurement or roll out of new hardware or software for mobile phone data extraction and processing, including any analytical capabilities
	  ○ for any software used for the extraction of data from mobile phone and other devices, ensuring that privacy by design is maintained and that privacy safeguards are built into any new procurement or upgrade

implement the guidance and that a Data Protection Impact Assessment and Equality Impact Assessment of all relevant investigative processes are undertaken.	○ on any new projects involving the use of new technologies for processing personal data to ensure the force complies with their legal obligations, Data protection officers will be involved in the DPIA ▪ An equality impact assessment (EIA) is completed for all investigative processes and data extraction procedures. ▪ Officers and staff have the required skills and knowledge to implement this guidance. ▪ That supervision and other supporting processes are in place to embed the guidance. ▪ That a sensitive processing policy document is in place.

Glossary of terms

Concept/phrase	Definition
Strictly necessary for a law enforcement purpose	The term 'strictly necessary for the law enforcement purpose' places a high threshold for processing based on this condition. Investigators need to demonstrate that they have considered other, less privacy-intrusive means and have found that 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 DPA 2018 conditions: statutory purposes: ▪ statutory purposes ▪ administration of justice ▪ protecting individual's vital interests ▪ safeguarding of children and of individuals at risk ▪ personal data already in the public domain ▪ legal claims ▪ judicial acts ▪ preventing fraud; or ▪ archiving etc

Reasonable lines of enquiry	**CPIA Code of Practice** states that in conducting an investigation, the investigator will pursue all reasonable lines of enquiry, whether these point towards or away from the suspect. What is reasonable in each case will depend on the particular circumstances. For example, where material is held on a computer, it is a matter for the investigator to decide which material on the computer it is reasonable to inquire into, and in what manner. **2020 EWCA Crim 790, R v Bater James and Mohammed** states that 'It is not a 'reasonable' line of enquiry if the investigator pursues fanciful or inherently speculative searches. Instead, there needs to be an identifiable basis that justifies taking steps in this context. This is not dependent on formal evidence in the sense of witness statements or documentary material, but there must be a reasonable foundation for the enquiry. **The AG Guidelines on Disclosure** states that 'It is not the duty of the prosecution to comb through all the material in its possession (eg, every word or byte of computer material) on the lookout for anything which might conceivably or speculatively undermine the case or assist the defence. The duty of the prosecution is to disclose material which might reasonably be considered capable of undermining its case or assisting the case for the accused which they become aware of, or to which their attention is drawn.' Just because an investigator can search a device does not mean that they should. It is difficult to provide a simple formula to help investigators decide whether a particular line of enquiry is reasonable, but it may be helpful to consider whether, if the data was held in physical form, the investigator would order every document to be searched.

Disclosure test	Material is 'disclosable' if it is capable of undermining the prosecution case or supporting the defence case. If material, including data from digital devices, is disclosable, it will be disclosed to the defence. Redaction will take place when necessary.
Relevant material	**CPIA Code of Practice 2015** states that material may be relevant to an investigation if it appears to an investigator, or to the officer in charge of an investigation, or to the disclosure officer, that it has some bearing on any offence under investigation or any person being investigated, or on the surrounding circumstances of the case, unless it is incapable of having any impact on the case. **https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/447967/code-of-practice-approved.pdf**
Data Protection Act 2018 – Law enforcement purposes	The law enforcement purposes are defined under **Section 31 of the DPA 2018** as: 'The prevention, investigation detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'.
Sensitive processing	Sensitive processing is defined in **Section 35(8) of the DPA 2018** as: ▪ personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership ▪ genetic data, or of biometric data, for the purpose of uniquely identifying an individual

	▪ data concerning health; or ▪ data concerning an individual's sex life or sexual orientation
Data Protection Act 2018 – Personal data	Personal data is defined in section 3 of the DPA 2018 as: Any information relating to an identified or identifiable **living** individual. An identifying characteristic could include a name, ID number or location data. You should treat such information as personal data even if it can only be potentially linked to a living individual.
Serious harm	Serious harm is not defined and investigators and managers will need to use their professional judgement. Some help can be found in definitions for serious crime such as in **section 93(4)** of the Police Act 1997 as: Conduct which: a. involves the use of violence, results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose or b. the offence or one of the offences is an offence for which a person who has attained the age of twenty-one and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more.
Policy document for sensitive processing data strictly necessary	The data controller has an appropriate policy document in place in relation to the sensitive processing if the controller has produced a document which— (a) explains the controller's procedures for securing compliance with the data protection principles (see section 34(1) DPA 2018) in connection with sensitive processing in reliance on the consent of the data subject or (as the case may be) in reliance on the condition in question,

for law enforcement purposes	and (b) explains the data controller's policies as regards the retention and erasure of personal data processed in reliance on the consent of the data subject or (as the case may be) in reliance on the condition in question, giving an indication of how long such personal data is likely to be retained.

References

Attorney General's Office (2013) Attorney General's guidelines on disclosure **https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/868617/AG_Guidelines_on_Disclosure_-_FINAL.pdf**

Criminal Procedure and Investigations Act 1996 (Sections 23 (1)) A Code of Practice (2015) **https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/447967/code-of-practice-approved.pdf**

Information Commissioners Office (2020) Mobile phone data extraction by police forces in England and Wales, Investigation Report version 1.1. **https://ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/**Information

Commissioners Office (2018) A guide to data protection **https://ico.org.uk/for-organisations/guide-to-data-protection/**

Police Act 1997 **https://www.legislation.gov.uk/ukpga/1997/50/contents**

2020 EWCA Crim 790 Bater-James etc Judgment Final **https://www.bailii.org/ew/cases/EWCA/Crim/2020/790.html**

About the College

We're the professional body for the police service in England and Wales.

Working together with everyone in policing, we share the skills and knowledge officers and staff need to prevent crime and keep people safe.

We set the standards in policing to build and preserve public trust and we help those in policing develop the expertise needed to meet the demands of today and prepare for the challenges of the future.

college.police.uk