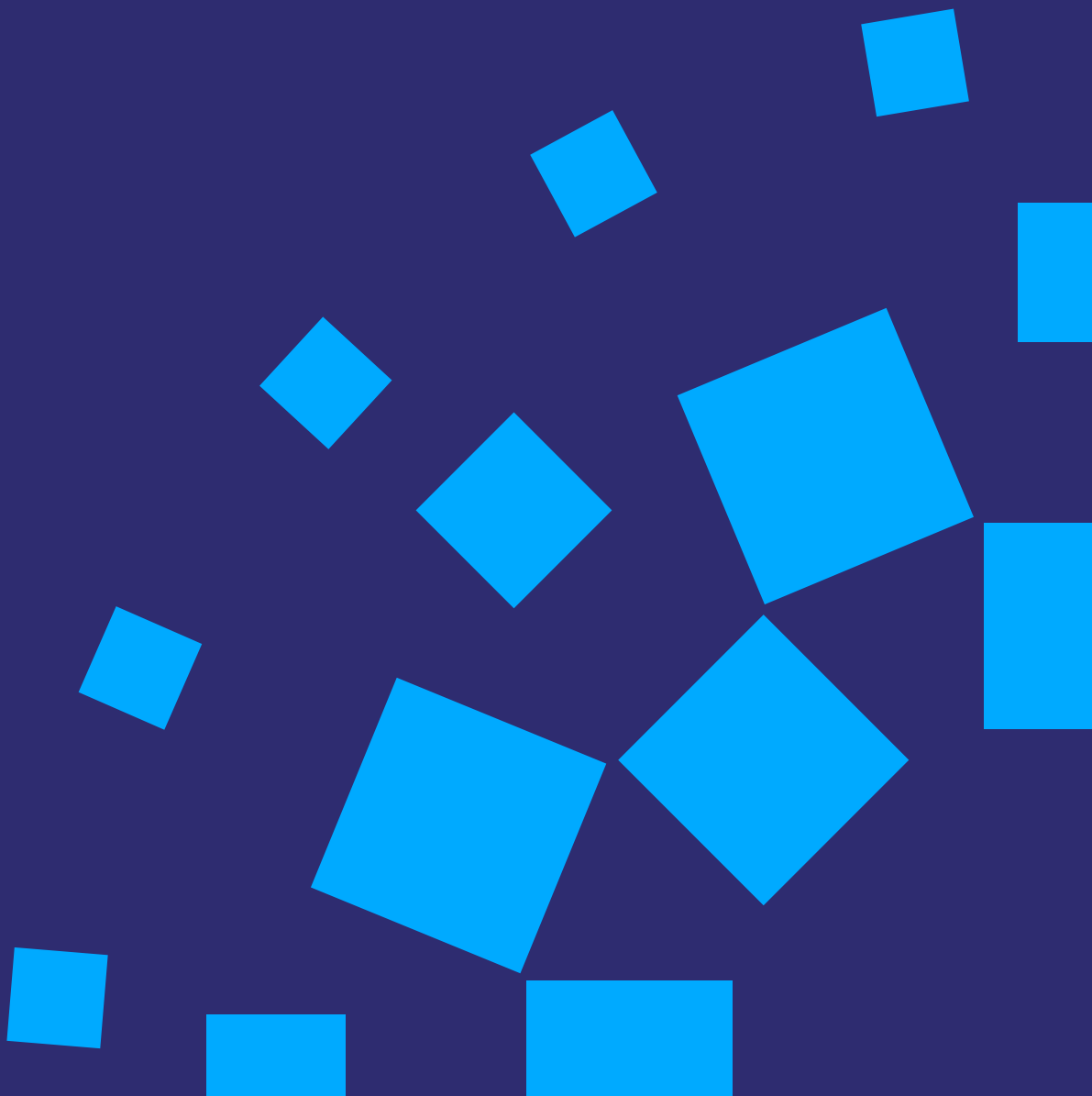
College of Policing

Working together to keep people safe

Authorised Professional Practice

Extraction of material from digital devices

May 2021



If you have any enquiries regarding this publication, please contact us on email **contactus@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 contact us on email **contactus@college.pnn.police.uk**

Contents

Introduction

Background

In recent years, mobile phones and other digital devices have played an increasing part in daily life. In addition to communication such as SMS messages, apps and social media, they are being used for a wide range of functions, from personal banking to recording health and fitness data and storing photographs. As a consequence of their prevalence, material from digital devices is increasingly used as evidence in criminal investigations and prosecutions.

Interest groups and privacy campaigners have raised concerns that the extraction of material from these devices is excessive. **Victims of rape and sexual violence** are disproportionately affected by the intrusion. For example, it has become almost routine for victims of rape to be asked to hand over digital devices and for most or all of the material to be downloaded. The excessive intrusion of this data extraction has been found **to affect victims' wellbeing**, their confidence in the police and criminal justice system (CJS) and is related to the tendency to withdraw their complaint.

Privacy groups, and others representing victims of sexual violence, 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 material 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 Data Protection Act 2018 (DPA 2018) in their extraction of material from these devices as part of investigations.

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

> The Government should strengthen the current legislative framework by producing a statutory code or other equivalent measure to ensure the law is sufficiently clear and foreseeable. The following information, which is not exhaustive, should be set out with sufficient detail to ensure that interference with the rights of individuals is not arbitrary and is in accordance with the law:
>
> - under what circumstances mobile phone extraction is permitted and why (including for which categories of offence under investigation)
> - the options available for lawfully obtaining devices and examining their contents, including the circumstances in which consent or coercive powers should be used
> - how lines of enquiry relate to requirements for mobile phone data
> - which categories of individual are liable to have their mobile devices examined (eg, suspects, witnesses, third parties)
> - the nature of the material to be examined
> - the time limits on the period of examination
> - the procedure to be followed for authorising, examining, using and storing the data obtained

The sources of law and guidance (see **lawful basis**) relevant to the extraction of material from digital devices such as mobile phones apply to the police, but also across all agencies of the CJS including defence and the courts. Any requests to policing that go beyond what is allowed by law should be raised with a supervisor or manager.

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 judgement and the recommendations of the ICO.

Aims of the Authorised Professional Practice (APP)

This APP sets out the obligations on the police under the **DPA 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

digital devices – most often mobile phones but also laptops and other computers – from victims, witnesses and suspects for the purpose of an investigation and how they then extract the digital material from those devices. It will also help the public understand the responsibilities of the police when gathering evidence, obtaining devices and accessing the material held on them.

This APP aims to ensure that the way in which police obtain material from mobile phones and other digital devices complies with the relevant legislation and balances the individual's right to privacy against the absolute right of all individuals to a fair trial. In the case of victims and witnesses, the guidance aims to ensure that material from mobile phones and other devices is obtained with their informed agreement. In a small number of cases, material may be obtained from a victim or witness without their agreement. 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 use an alternative legal power in these cases. See **Principle 4** for further information.

In the case of suspects, there is a range of powers available for acquiring the device. But the DPA 2018 applies to the extraction of the material from those devices just as it does to victims and witnesses.

The College has developed an **Equality Impact Assessment (EIA)**, which will help forces develop their own EIAs for implementation of this APP.

Lawful basis

While material from mobile phones and other digital devices can provide a useful source of evidence in the investigation of offences, the decision to obtain evidence in this form must take account of human rights and comply with both data protection legislation and the legislation relating to investigations.

The right to privacy must be balanced against the absolute right to a fair trial and the level of intrusion into individuals' privacy must be necessary and proportionate to the matter being investigated. Any interference with the right to privacy must satisfy the four-stage proportionality test set out by the Supreme Court in the case of **Bank Mellat v Her Majesty's Treasury (No. 2) [2013] UKSC 39**. This considered whether a less intrusive measure could have been implemented and whether the measure was proportionate and rationally connected to the aim sought.

This section sets out:

- the considerations required before making the decision to acquire a device for the purposes of extracting the material and once that decision has been made
- the options available for lawfully acquiring devices and examining their contents, including the circumstances in which consent/agreement or legal powers should be used

Considerations

The Code of Practice to the Criminal Procedure and Investigation Act 1996 (**CPIA 1996**) provides the duty for officers to pursue all **reasonable** lines of enquiry, whether they point towards or away from the suspect, and to gather and retain **relevant** material. However, if there is a belief that data, images or other information on a digital device could provide material to satisfy a reasonable line of enquiry, consideration should first be given to the potential for other less intrusive sources of evidence to satisfy that line of enquiry. Further, consideration should also be given to whether the extraction of material from the device and the intrusion and inconvenience this would cause the individual is proportionate to the offence being investigated.

Using evidence from digital devices

Once the decision has been made that the extraction of material on a digital device is necessary and proportionate to satisfy a reasonable line of enquiry, there are two parts to the process to obtain that evidence. These processes, while inextricably linked, should be considered separately in terms of the lawful bases. These are:

- the acquisition of the device
- the extraction of material from the device

These are separate processes but in many cases they must be considered together.

Acquiring the device

Victims and witnesses

- **Common law consent** – the acquisition of the device from a victim or witness would generally be under common law consent, for example you ask the victim/witness for their agreement to hand over the device.
- **Other options** – it is also possible that there are circumstances in which victims'/witnesses' devices could be acquired using police powers. For example, if the offence under investigation was felt to be sufficiently serious that police were going to continue the investigation without the victim, they may consider it necessary to obtain a warrant to obtain that evidence from a reluctant witness.

Suspects

There are many powers that could be used to acquire a device from a suspect depending on the circumstances.

- **Using a statutory power or court order** – for example, powers of seizure conferred by the Police and Criminal Evidence Act 1984, including where an officer is lawfully on premises, a person searched under the provisions of sections 32 and/or 54 PACE and powers under Part 5 of the Investigatory Powers Act 2016.
- **Common law consent** – where no other power has been used, an approach that involves engaging with the suspect to seek agreement to acquire their device can be applied.

Extraction of the material

Extraction of the material must be lawful and fair in accordance with the **first data protection principle (DPA 2018)**. **This applies to all individuals whatever their status, for example victims, witnesses and suspects**. Once a basis in law has been established, for example the obligation under the CPIA to pursue all reasonable lines of enquiry, one of the following conditions must be satisfied to ensure the extraction is lawful:

- informed consent has been given
- the extraction is necessary for a law enforcement purpose

In relation to law enforcement processing, there are additional protections where the data is considered to be 'sensitive'. Since police practitioners cannot be certain about the nature of the material before viewing it, the requirements for 'sensitive processing' should be applied. Sensitive processing for law enforcement purposes is only permitted in cases where either:

- there is informed consent
- the processing is strictly necessary for the law enforcement purpose and at least one of the conditions in Schedule 8 of the DPA 2018 is met

The ICO found it was more appropriate to rely on the condition that the extraction is strictly necessary for a law enforcement purpose. This was for a number of reasons, including that it is unlikely that all those who should provide informed consent would be able to do so as material on the device may relate to many individuals. Further, the perceived power imbalance between the individual and the police could mean that consent may not be freely given.

To meet the condition that it is 'strictly necessary' for the law enforcement purpose, investigators need to demonstrate they have considered other, less privacy-intrusive means and have found that they do not meet the objective of the processing. They must also demonstrate that the processing meets at least one of the conditions found in **Schedule 8 of the DPA 2018**:

- 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

The CPIA Code of Practice establishes the duty for officers to pursue all **reasonable lines of enquiry**, whether they point towards or away from the suspect, and to gather and retain **relevant** material. This duty could be considered to provide the basis for satisfying the 'strictly necessary' criterion in the situation of an investigation.

If the device is acquired under common law, in most investigative circumstances officers or staff will be intending to take the device for the purposes of extracting material[1]. This means that investigators should consider and explain the requirement for them to acquire the device and to acquire the material at the same time. Therefore officers and staff should apply both the common law consent to the physical device and DPA 2018 requirements for processing the data. Consequently officers and staff will:

- identify reasonable lines of enquiry for the investigation
- consider whether they have reasonable grounds to believe that a search of a personal device may reveal material relevant to the line of enquiry
- consider whether other less intrusive means could provide the material in a way that will support the investigation of the reasonable line of enquiry

If, as a result, they believe acquisition of the material to be '**strictly necessary**' to satisfy the reasonable line of enquiry, officers and staff will:

- inform the victim/witness/suspect of all the relevant information required by the DPA 2018 for sensitive processing by using, for example, the National Police Chiefs' Council (NPCC) Digital Processing Notices (DPN).
- Once informed, they will ask for agreement (common law consent) to acquire the device for the purposes of extracting material.

1 If you acquire the device as evidence as an object rather than for the purposes of acquiring the data on it, you should apply the rules that apply to physical evidence but you should also consider any safeguarding issue arising from the loss of the device.

Glossary of terms

Concept/phrase	Definition
Informed agreement	Throughout the document, the phrase 'informed agreement' is used to avoid further confusion with the term 'consent' as used formally within the DPA 2018. It was felt this better reflected the process of obtaining the device user's agreement or permission to acquire the device.
Consent	**Consent** is defined in **Article 4(11) of the general data protection regulation (GDPR)** as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. The conditions required for valid consent under the DPA 2018 are explained **here**. The ICO found it was more appropriate to rely on the condition that the extraction is 'strictly necessary' for law enforcement purposes rather than consent for a number of reasons. These include that it is unlikely that all those who should provide informed consent would be able to do so as material on the device may relate to many individuals. Also the perceived power imbalance between the individual and the police could mean consent may not be freely given.
Suspect	Throughout this document, in relation to the acquisition of the device, we are clear that we are referring to un-arrested suspects. If a suspect is arrested, there is a well-developed legal framework for acquiring evidence. Once evidence has been acquired from a digital device, broadly the same handling rules for the material will apply to victims, witnesses and suspects. Investigators may choose to use this guidance to assist them in the lawful and fair extraction of material from devices belonging to suspects.
Device	Any device on which information is capable of being stored electronically. This includes: mobile phones, laptops, in-car computers, sat navs, fitness trackers and other internet-enabled devices.

Concept/phrase	Definition
Device user	Throughout this document the phrase 'device user' is used to indicate the person who has regular access to and use of the device and from whom informed agreement should be sought to acquire the device for the purposes of extracting material. In some situations the officer/staff may need to get informed agreement from more than one person where, for example, the device is owned by one person but the material on it belongs to someone else. For example, a parent owner/child user, where an organisation owns a device but an employee uses it or where a device is shared.
Article 8 the European Convention on Human Rights	**Article 8 of the Convention – Right to respect for private and family life** states that: 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
Proportionate	In **Bank Mellat v HM Treasury (No 2) [2013] UKSC 39, [2014] AC 700** the Supreme Court applied a four-stage structured proportionality test. This can be applied by considering: 1. Is the objective sufficiently important to justify limiting a fundamental right? 2. Is the measure rationally connected to the objective? 3. Could a less intrusive measure be used without unacceptably compromising the objective? 4. Is the impact of the rights infringement disproportionate to the likely benefit of the impugned measure?

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 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 DPA 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 police cannot reasonably achieve it through less intrusive means. This is a requirement that will not be met if police 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.
Law enforcement purposes	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 prevention of threats to public security.

Concept/phrase	Definition
Sensitive processing	Sensitive processing is defined in **Section 35(8) of the DPA 2018** as the processing of: ■ personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership ■ genetic data or biometric data, for the purpose of uniquely identifying an individual ■ data concerning health ■ data concerning an individual's sex life or sexual orientation In all cases, where sensitive data may be involved, police forces must have an appropriate policy document in place, describing how sensitive data is handled and what safeguards are applied.
Appropriate policy document	The conditions for sensitive processing include the following. The data controller has an **appropriate policy document** in place in relation to the sensitive processing if the controller has produced a document that: (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; (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.
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.

Concept/phrase	Definition
Reasonable lines of enquiry	The CPIA Code of Practice 2020 states that, in conducting an investigation, the investigator should 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. It is a matter for the investigator, with the assistance of the prosecutor if required, to decide what constitutes a reasonable line of enquiry in each case. R v Bater James and Mohammed [2020] EWCA Crim 790 states it is not a 'reasonable' line of enquiry if the investigator pursues fanciful or inherently speculative research. 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. It goes on to provide examples taken from 'A guide to reasonable lines of enquiry' and Communications Evidence (Crown Prosecution Service (CPS), 2018): 'There will be cases where there is no requirement for the police to take the media devices of a complainant or others at all. Examples of this would include sexual offences committed opportunistically against strangers, or historic allegations where there is considered to be no prospect that the complainant's phone will retain any material relevant to the period in which the conduct is said to have occurred and/or the complainant through age or other circumstances did not have access to a phone at that time.' The **Attorney General's (AG) Guidelines on Disclosure 2020** Annex A, paragraph 39 states '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'.

Concept/phrase	Definition
	An example provided within the AG's Guidelines (paragraph 13) states: 'A case might, for example, involve a complainant contacting the police to make an allegation of an offence against a person they had met that same day. The suspect may accept that they met the complainant but deny the allegation. The complainant and suspect communicated on a single medium. The investigator may consider it is a reasonable line of enquiry to view the messages from the day on which the two persons met as, before and after, they are highly unlikely to be relevant. They may contain material about what was expected or not expected when complainant and suspect met, the nature of their relationship, and the response after they met, all of which may cast light on the complainant's account and the suspect's account. That is unlikely to require the investigator taking custody of the phone or obtaining a large volume of data. If, by way of example and contrast, the complainant alleged coercive and controlling behaviour over a period of years, including manipulative conduct over various platforms, a larger quantity of data may be relevant and require review and retention by the investigator by different means.'
Disclosure test	Material is 'disclosable' if it might reasonably be considered capable of undermining the case for the prosecution or assisting the case for the accused. If material, including data from digital devices, is disclosable, it will be disclosed to the defence. Redaction will take place when necessary.
Material	Throughout the Guidance we refer to 'material'. In this context, material means material of any kind held on a digital device, such as information, data images, video, voice recordings, messages, GPS information or content from apps.
Relevant material	The **CPIA Code of Practice** states that material may be relevant to an investigation if it appears to an investigator, 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.

Concept/phrase	Definition
Unused material	This is material that is relevant to the investigation but does not actually form part of the case for the prosecution against the accused. Even though the material may not be used as evidence, it is important that, for the purposes of disclosure, this material is recorded, retained and where necessary revealed to the defence in accordance with the CPIA Code of Practice. See **Guidance for experts on disclosure, unused material and case management (CPS 2019)**.
Non-relevant material	This is material that may be acquired from a device that has no bearing on any offence under investigation or any person being investigated, or on the surrounding circumstances of the case, and is not capable of having any impact on the case. It may be material 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, not all data held on devices can be searched using currently available technologies for triage and live previews. Some data, usually data that is deleted or hidden, requires a comprehensive extraction of the full raw data to enable more complicated searching techniques to be applied. The material that is not recovered in the search is irrelevant material and should be managed in accordance with the CPIA Code of Practice and with the principles in this APP. 'Irrelevant material' is not the same as 'unused material'. It is important to note that technology is developing, both that used for data extraction and that used within the device. It is not always possible to separate the unused non-relevant material from that of the unused relevant material. The way in which material may be extracted is likely, therefore, to change as technology changes, sometimes allowing more targeted extraction but also sometimes meaning that targeting of material is more difficult.
Excluded material	Excluded material is defined in **section 11 of PACE 1984**. Special procedure material is defined in section 14 of PACE 1984, and includes journalistic material that isn't excluded material.

Concept/phrase	Definition
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 of 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 21 and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more
Investigator	An investigator is defined in the CPIA Code of Practice as any police officer or member of police staff involved in the conduct of a criminal investigation. All investigators have a responsibility for carrying out the duties imposed on them under this code, including in particular recording information, and retaining records of information and other material. Anyone, including first responders, involved in an investigation could play the role of an investigator and, if considering whether to obtain a digital device to download material, will need to apply this guidance.

Summary: Principles for the extraction of material from digital devices for the purposes of an investigation

These principles have been developed based on the **DPA 2018**, the **2020 ICO report on mobile phone data extraction,** the Court of Appeal judgment in the case of **Bater-James and Mohammed [2020] EWCA Crim 790** and with consideration of other relevant legislation and guidelines, including the **CPIA 1996 Section (23(1)) Code of Practice** and the **Attorney General's Guidelines on Disclosure**. In the application of the legislation, the principles also take account of extensive feedback from police practitioners and external stakeholders to ensure they balance the rights of victims and witnesses to privacy with the right of suspects to a fair trial and are practical to implement. The sources of law and guidance listed above apply across all agencies of the CJS including defence and the courts. See here for details of the consultation response.

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

Principle 1: **Strictly necessary and avoiding unnecessary intrusion**. Material will only be extracted from a personal digital device if it is proportionate and strictly necessary for an investigation. Intrusion into the personal or family life of device users will be avoided wherever possible. Only the minimum material that is strictly necessary will be extracted.

Principle 2: **Provision of information**. Where material is extracted from a personal digital device, investigators will provide full and clear details about the extraction of material to the device user and/or those supporting the device user (for example those supporting people who lack capacity).

Principle 3: **Requesting agreement**. Investigators will ask the device user for informed agreement to hand over their personal digital device to the police for the purpose of extracting material. (It should be noted that devices can be acquired using statutory powers, for example powers of seizure conferred by PACE 1984).

Principle 4: **The right to refuse**. Where the device is being acquired through informed agreement, the device user has the right to refuse to hand over their personal digital device for the purpose of extracting material. If the device is being acquired using powers, such as those conferred under PACE 1984, the right to refuse may not apply.

Principle 5: **Adequate, relevant and not excessive for the purpose for which it was processed**. Investigators will extract and examine the minimum material required to satisfy the reasonable lines of enquiry. Any information or material irrelevant to the investigation will be deleted where possible.

Principle 6: **Safeguarding**. Investigators will consider risk of harm and any issues that could have adverse impact on the device user when deciding how to extract material from a digital device.

Principle 7: **Updating, reviewing and managing material obtained during an investigation**. Investigators will review the retention of digital devices and the extracted material at regular intervals. The storage, retention and disposal of material extracted from a digital device will be managed in line with data protection legislation and will be retained for no longer than necessary. Where a device has been acquired by agreement, the investigating officer will inform the device user of any proposal to change how the extracted material is used and request further agreement.

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 material was extracted, or where there is a strictly necessary policing objective, such as protecting a vulnerable person from harm.

Principle 9: **Recording actions**. A record should be made of all actions in relation to the extraction of digital material and management of that extracted material.

Principle 10: **Implementation**. Chief officers are responsible for the 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 (DPIA) and EIA 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. The roles included are: chief officer, first responder, investigator, supervisor, inspector and digital forensic specialist.

Chief officer

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 EIA is carried out on all local investigative and material extraction policies.
- Ensure a DPIA is carried out on all relevant local investigative policies governing processing material extracted from personal digital devices. This should be carried out in consultation with the force data protection team. The Information Commissioner has published guidance on DPIAs and detailed additional guidance for police data protection professionals is included in the NPCC Data Protection Manual of Guidance.
- Ensure the force implements technology that supports staff to follow this APP, taking into account the changing nature of extraction technology and the changes in devices, software and cost.
- Ensure procurement and/or rollout of new hardware or software for data extraction from personal digital devices is undertaken with 'privacy by design' principles in mind.
- Ensure 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 an appropriate policy document for sensitive processing of data is developed and implemented.

First responder

In some cases, for example volume and priority crime investigations, the first responder may also be the investigator. In this case, they will carry out the responsibilities for both roles.

	Victims, witnesses and suspects
Reasonable lines of enquiry	First responders should identify lines of enquiry for the investigation. First responders should consider whether there are reasonable grounds to believe a search of a personal digital device may reveal material relevant to the investigation and whether it is likely to satisfy a reasonable line of enquiry.

Less intrusive means	**Victims, witnesses and suspects**
	First responders should consider what material is likely to be on the device and whether there are other sources of material that will achieve the same objective, such as CCTV or material from the arrested suspect's device. If it is still strictly necessary to obtain material from a device, first responders should consider 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 by taking screenshots or making a record of what is on the device. It is important to consider whether a proposed measure fulfils evidential requirements and retains the required evidential integrity. If in doubt, a digital forensic specialist should be consulted. Manual examination, including screenshots or other images or record of what is on screen, should only be considered when: ■ There is minimal material that would be of significant evidential value. ■ Material on devices may be lost if not captured immediately. ■ Volatile material is present, such as data that might be lost if the device is turned off. ■ If, after seeking to reassure the device user, persuade them of the strict necessity of acquiring their device, and explaining the potential consequences of refusing to provide it, the device user does not agree to hand over the device, but will agree to screenshots as an option to secure a record of the material. **See also Annex A of the AG's Guidelines on Disclosure**.
Proportionate	**Victims, witnesses and suspects**
	First responders will consider whether extraction of material from a digital device is proportionate to the offence. For example, does the public interest in obtaining this material outweigh the privacy concerns of such intrusion?

<table>
<tr><td rowspan="2">Lawful basis</td><td colspan="2">If it is both strictly necessary and proportionate to acquire the device for the purpose of extracting material, first responders should consider the lawful basis for acquiring the device.</td></tr>
<tr><td>Victims and witnesses</td><td>Suspects</td></tr>
<tr><td></td><td>In the case of victims and witnesses, this will often be through their informed agreement, otherwise called ‘common law consent’.</td><td>In the case of suspects, where the suspect has been arrested, other powers will usually have been used to acquire the device such as the powers of seizure conferred by PACE 1984.

If, however, the suspect has not been arrested, asking for informed agreement may be the way to proceed. Or you could, for example, seek a court order.</td></tr>
<tr><td rowspan="2">Capacity to provide informed agreement</td><td>Victims and witnesses</td><td>Suspects</td></tr>
<tr><td>Consider whether the device user has capacity to provide informed agreement for the police to take possession of the personal device. For example:

■ does the device user have an impairment that affects their understanding, for example a cognitive impairment or a neurodiversity issue?

■ is the device holder a child? does the device holder understand English?

■ does the device holder understand English?</td><td>In the case of suspects, where the suspect has been arrested, other powers will usually have been used to acquire the device such as the powers of seizure conferred by PACE 1984.

Where a device is being acquired from a suspect using informed agreement, their capacity to provide that informed agreement should also be considered. See victims and witnesses column.</td></tr>
</table>

Also consider whether the device user has a temporary reduced capacity to understand what they are agreeing to due to:

- injury
- trauma
- intoxication
- a mental health crisis

Where the device user lacks capacity or has temporarily reduced capacity to provide informed agreement, consider what steps can be taken to support them to fully understand the implications of the request. This could involve, for example:

- allowing them more time to make the decision
- seeking an alternative person to provide the informed agreement, such as a carer, parent/guardian or appropriate adult.
- the device holder seeking support from an independent legal representative

If there are reasonable grounds to believe material may be lost, you should consider the full range of powers available to acquire the device.

Click **here** for a brief guide to capacity and consent in under 18s and **here** for information on the impact of trauma.

<table>
<tr><td>Safeguarding issues</td><td colspan="2">Victims, witnesses and suspects
Consider any safeguarding requirements for the victim/ witness/suspect. In particular, consider whether taking their device might further compromise their safety and what safeguards need to be put in place.</td></tr>
<tr><td>Provide information</td><td>Victims and witnesses
Provide information to the device user before requesting their agreement to take possession of the device. This could be done by providing a copy of the NPCC-approved Digital Processing Notice (DPN) or your force version.

The information provided should include:
■ why the material on the device is required – what reasonable line of enquiry the material on the device is likely to satisfy
■ the lawful basis for taking possession of the device and for extracting the material
■ how the material will be extracted and used
■ when the device is likely to be returned to them
■ their rights to refuse and to make complaints to the ICO
■ who they should contact if they have any questions or concerns</td><td>Suspects
Where the device is being acquired from a suspect using informed agreement and no other lawful power is being used, they should be provided with information (listed under victims and witnesses) before requesting their agreement to take possession of their device.

Where the device is being acquired through another lawful power, such as the powers of seizure conferred by PACE 1984, the suspect should still be provided with information on how and why their material will be extracted and used, as listed under victims and witnesses. But this can be done after acquiring the device, using for example the NPCC DPN.

The information provided can be restricted if it is necessary and proportionate for at least one of the conditions detailed in section 44(4) of the DPA 2018. These include where providing information to the suspect would:</td></tr>
</table>

	The information provided can be restricted if it is necessary and proportionate for at least one of the conditions detailed in section 44(4) of the DPA 2018. These include where providing information would: ■ obstruct an official or legal enquiry, investigation or procedure ■ prejudice the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties	■ obstruct an official or legal enquiry, investigation or procedure ■ prejudice the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties
Ask for informed agreement to acquire the device	**Victims and witnesses**	**Suspects**
	Ask for the owner's informed agreement to take possession of a personal digital device for the purposes of extracting material. The device user has the right to refuse to hand over the device. See below for actions that should be taken if the device user does not agree to hand over the device.	In most cases, a suspect's device will have been acquired using a lawful power of seizure such as those conferred under PACE 1984. But it is also possible that their device could be acquired by asking for their informed agreement. Where informed agreement has been used, the suspect has the right to refuse.

Agree updating arrangements	**Victims and witnesses**	**Suspects**
	The first responders should discuss how frequently the device user would like to be updated on the investigation and through what medium. Ensure updating arrangements are carried out as agreed. Tell the device user of any changes to the police contacts if the case is passed on. Record this information in the crime report.	If the device was acquired using informed agreement, updated arrangements should be agreed as for victims and witnesses. If a statutory power is being used you may consider updating the suspect but there is no legal requirement to do so.
Record decision	**Victims and witnesses**	**Suspects**
	The first responder will make a record of the decisions taken and any agreement given, together with a rationale for the necessity to extract material from the device on the relevant forms, for example on the NPCC-approved DPN and body-worn video (BWV).	The first responder will make a record of the decisions taken and any agreement, together with a rationale for the necessity to extract material from the device given on the relevant forms, for example on the NPCC-approved DPN and BWV.
Seek inspector's authority	**Victims, witnesses and suspects**	
	The first responder will seek inspector's or police staff equivalent authority for the **extraction of material** from the device.	

Delete extracted irrelevant material	**Victims, witnesses and suspects** If the first responder is responsible for extracting the material, for example through use of a kiosk, they should only extract material that is relevant to the reasonable lines of enquiry. Where it is unavoidable to extract material that is not relevant, for example where it is inextricably linked to relevant material, that material should be deleted unless it is not reasonably practicable to separate it from the other linked material without prejudicing the use of that other material in any investigation or proceedings. See **CPIA Code of Practice** (CPIA 1996) for further information on unused material. See also **NPCC DPNa** officer information form.
Return the device	**Victims, witnesses and suspects** Where the first responder still has possession of the device, they should return the device to the device user without undue delay. They cannot retain a device in anticipation of a future line of enquiry. The first responder should inform the device user that it is possible further examination may be required if new lines of enquiry emerge, and advise the device user they should not delete or amend any material that could be relevant to the investigation. There are some circumstances in which it may not be possible to return the device, for example if there is illegal material on a device such as indecent images. In such cases, it is unlikely the device would be returned as it is difficult to remove that material from the device. When returning the device to the device user, inform them they should not delete or alter anything they think is relevant to the investigation. Also inform the investigator if any further material becomes relevant because of a development in the case.

If agreement is refused	**Victims and witnesses**	**Suspects**
	The first responder should: ■ Further explain why the material on the device is needed and try to understand and allay any concerns the device user has. These concerns should be considered and all efforts to obtain the evidence through less intrusive means should be made. ■ Where the victim/witness still feels unable to hand over their device, explain there is a risk that: - it may not be possible to pursue the investigation - a witness summons may be issued - any trial resulting from the investigation may be halted ■ Explain to the victim/witness they must not delete potentially relevant material from their device and if they do so this might prevent the police from carrying out a fair investigation, which could result in the investigation being closed. ■ Continue to investigate the case where possible, considering alternative sources of material that may support the line of enquiry.	The right to refuse to hand over the device also applies to suspects where the device is being acquired by informed agreement. For example, if they have not been arrested and no other powers have been used to seize the device. The police do have specific powers to seize devices from suspects when they believe them to contain evidence of an offence. The use of these powers will depend on the specific circumstances of the case.

	■ Make a record of all actions in relation to the extracted material.	
Record all actions	**Victims, witnesses and suspects**	
	A processing log should be kept, recording all actions in relation to the extraction of digital material and management of that extracted material. This includes each time the extracted material is examined, any changes to the use of the material and the deletion of the material.	

Investigators

Investigators should:

- Seek authorisation from an inspector or police staff equivalent for the extraction of strictly necessary material from the device before extracting the material or requesting the extraction.
- ensure search parameters are as well defined as possible and appropriately focused to extract only what is necessary and relevant to the line of enquiry. Provide these search parameters to any digital forensic practitioners undertaking the extraction of the material. 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.
- Record the search parameters as part of the investigation record.
- Review and develop lines of enquiry. If further searches are required, for example to pursue new lines of enquiry or there is a change in how the material is to be used, such as after a suspect is identified, the investigator will inform the device user and ask for agreement to extract the additional material if necessary. An incremental approach should be taken.

- Delete extracted material that cannot have a bearing on the investigation without undue delay. See the CPIA Code of Practice for detail on unused material. Liaise with specialist forensic staff to ensure this deletion happens where necessary. Investigators should consider the following before the deletion of non-relevant material:
  - If a suspect has been identified and it is anticipated that they can suggest different search parameters within a reasonable time, the material may be retained to allow this to happen. In making this decision, the investigating officer will need to decide what is necessary and proportionate to the investigation.
  - Where it is not possible to separate non-relevant material from relevant material, it may be necessary to retain a wider extract of material for the purposes of evidential credibility and continuity. In this case the investigator will ensure any working copy contains only the relevant material and appropriate safeguards are in place to ensure no further processing of the wider extraction occurs.
- Ensure all safeguarding risks are identified and mitigated for all parties involved, for example the impact of not having access to their personal digital device. Investigators will also consider how the extracted material could increase risk to the victim/witness, or may affect their private life or relationships.
- Only share material with CJS partners that is relevant to the investigation. If a request for material is received from another CJS organisation or the defence, and the requested material is not supported by a reasonable line of enquiry, the request must be considered and consideration given to whether there are other legal powers to do so. Liaise with the CPS or force solicitors if necessary. If there is no reasonable line of enquiry, the request must be refused. Any sharing must be conducted in accordance with the DPA 2018 (see **APP on sharing police information**). Follow force escalation policies if necessary.
- There are specific considerations that apply to **excluded material**, special procedure material or material that is subject to legal professional privilege. Should this type of material be sought, anticipated or inadvertently acquired, the appropriate legal provisions should be applied. See the **AG's Guidelines on Disclosure** for further guidance.

- Update the device user at regular intervals as agreed with them. The investigator will provide updates on the progress and any significant developments in the investigation. Ensure the device is returned without undue delay.
- Ensure a processing log is made, recording all actions undertaken in relation to the extracted material.
- Provide support and advice to first responders on how to apply this guidance.

Supervisors

Supervisors should ensure:

- All reasonable lines of enquiry have been identified and are being followed.
- Material from personal digital devices is only extracted when less intrusive methods have been considered and it is both proportionate and strictly necessary to do so.
- Failure to follow the APP is 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 should:

- Be responsible for authorising applications to lawfully obtain material from a personal digital device when a device has been acquired, either through informed agreement or through a lawful power. This level of authority reflects the significance of potential intrusion.
- Ensure authority is only given when the **strictly necessary** criterion is met, for example:
  - the inspector is satisfied there are reasonable grounds to believe a search of a personal digital device may reveal material relevant to the investigation and is likely to satisfy a reasonable line of enquiry

  - at least one of the conditions in Schedule 8 is met

- Ensure less intrusive methods have been explored and it is considered that the purpose cannot reasonably be achieved through less intrusive means.

- Inspectors should record all decisions and the strictly necessary rationale for the authorisation of the extraction of material from a personal digital device on the appropriate force form (for example, see the **NPCC DPNa**).

Inspectors may also be asked to authorise warrants to obtain devices where informed agreement to acquire the device has been refused and it is in the public interest to obtain that device to extract material. This would only be in circumstances where there is an identifiable basis for believing the device user or someone else is at risk of harm and where consideration has been given to the privacy rights of the victim or witness. Along with the responsibilities associated with authorising an application for a warrant, they will need to provide a rationale describing how strict necessity and minimal intrusion have been considered.

Staff in specialist digital forensics units

Digital forensic specialists will:

- Ensure material extracted is not excessive and only the minimum material required to satisfy the line of enquiry is extracted and analysed using the least intrusive methods, subject to the capability of the available technology. They will liaise closely with the investigator to ensure only the minimum material necessary is extracted.

- Consult with the investigator to ensure irrelevant material that cannot have a bearing on the investigation is deleted without undue delay once the required material has been identified and retained as evidence. See Annex A, paragraphs 21-25 of the **AG Guidelines on Disclosure 2020** for more detail. Digital forensic specialists should consider the following before the deletion of non-relevant material.

  - If a suspect has been identified and it is anticipated they can suggest different search parameters within a reasonable time, the material may be retained to allow this to happen. In making

this decision, the investigating officer will need to decide what is necessary and proportionate for the investigation.

Where it is not possible to separate non-relevant material from relevant, it may be necessary to retain a wider extract of material for the purposes of evidential credibility and continuity. In this case the digital forensic specialist will ensure any working copy contains only the relevant material and that appropriate safeguards are in place to ensure no further processing of the wider extraction occurs.

- Ensure the extraction is carried out in a timely way so the device is returned to the owner without undue delay. There are some circumstances in which it may not be possible to return the device. For example, if there is illegal material on a device, for example indecent images, it is unlikely that device would be returned to the device user as it is difficult to remove that material from the device.
- Record how the extraction was undertaken and the methods used, including details of any search parameter used.
- Ensure the extracted material is stored securely in accordance with the DPA 2018, the CPIA Code of Practice and Management of Police Information (MoPI) Code and APP (to be replaced by Information Management APP). The extracted material will not be shared with anyone other than the investigator or other authorised persons, in accordance with the DPA 2018 and this APP.

Principles for the extraction of material from digital devices for the purposes of an investigation

Principle	Detail
Principle 1: Strictly necessary and avoiding unnecessary intrusion Material will only be extracted from a personal digital device if it is proportionate and strictly necessary for an investigation. Intrusion into the personal or family life of device users will be avoided wherever possible. Only the minimum material that is strictly necessary will be extracted.	**Victims and witnesses** 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 it is proportionate and strictly necessary to acquire material 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 . Where material is required from a personal digital device, it must meet the' strictly necessary' test. The processing of the material should not be excessive. The strictly necessary condition can only be satisfied where all other less intrusive methods have been explored and it is considered that the purpose cannot reasonably be achieved through less intrusive means. For example, 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 material from the device. Alternatively, material may be available on the suspect's device. It is important to consider whether a proposed measure fulfils evidential requirements, retains the required evidential integrity and is proportionate to the offence being investigated. Manual examination, including screenshots, will be considered when: ■ There is minimal material that would be of significant evidential value.

Principle	Detail
	■ Material on devices may be lost if not captured immediately. ■ Volatile material is present, such as data that might be lost if the device is turned off. ■ If, after seeking to reassure the device user, persuade them of the strict necessity of acquiring their device, and explaining the potential consequences of refusing to provide it, the device user does not agree to hand over the device, but will agree to screenshots as an option to secure a record of the material. See also **Annex A of the AG's Guidelines on disclosure**. If in doubt, the investigator will consult a specialist in digital forensics. 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 focused searches of the device. 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 held on the device. The investigator will then need to apply the 'strictly necessary' test. ■ Use the least intrusive method available, including the techniques, software and equipment with privacy by design and default. ■ Disregard information irrelevant to the search parameters and line of enquiry (except where additional serious offences are identified – see **Principle 5**).

Principle	Detail
	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 it is **strictly necessary** to acquire material 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 should be pursued, whether they point towards or away from the suspect . Where material is required from a personal device, it must meet the strict necessity test. The processing of the material should not be excessive. The '**strictly necessary**' condition can only be satisfied where all other less intrusive methods have been explored and it is considered that the purpose cannot reasonably be achieved through less intrusive means. For example, 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). Where police have carried out a search of a device and a suspect has been identified, the police should 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 parameters. These must be precise so a reasonable and proportionate search can be undertaken. A search cannot be speculative.

Principle	Detail
Principle 2: Provision of information. Where material is to be extracted from a digital device, investigators will provide full and clear details about the extraction to the device user.	**Victims, witnesses and suspects** **Sensitive processing** It is likely some information on a digital device will be considered sensitive. Under **Section 35(8) of the DPA 2018**, sensitive processing is the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, data concerning health or information concerning an individual's sex life or sexual orientation. It is also possible the material may relate to individuals other than the owner of the device. Police practitioners are unable to assess the nature of the material before viewing it, so they should assume it is sensitive and comply with Section 42, Part 3 of the DPA 2018. Chief officers must ensure an **appropriate policy about sensitive processing** is implemented, explaining the procedures for ensuring compliance with the law enforcement data protection principles; and policies on the retention and erasure of this material. Sensitive processing applies to data obtained from victims, witnesses and suspects. The device user has the right to be informed of information relating to the sensitive processing of their data.
	Victims, witnesses and suspects When acquiring a digital device to extract material using informed agreement, the device user must be provided with information before asking for their agreement to hand over the device. Where a lawful power is used to acquire the device, the information must still be provided but can be provided after the acquisition of the device.

Principle	Detail
	An NPCC-approved Digital Processing Authorisation Form (DPNa for victims/witnesses and DPNc for suspects) or similar will be provided to the device user before a device is processed and material extracted. The notice will explain the following. ■ **Legislation** – the lawful basis for acquiring the device and extracting material. The lawful basis for acquiring the device may differ depending on the status of the device user, for example victim/witness, unarrested suspect or arrested suspect (see **lawful basis**). However, the lawful basis for the extraction and use of the material will, in most cases, be that it is strictly necessary for law enforcement purposes for all except arrested suspects where different laws and procedures apply. ■ **Reason** – why it is strictly necessary for the police 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 that will be used to pursue the line of enquiry and what that means when searching for and extracting material. For example, material will be limited to the time of the offence and to communications between victim and suspect identified by the victim. Searches cannot be speculative.

Principle	Detail
	■ **Technical limitations** – explain in simple terms as far as possible how the technology will be used and what its limitations are. Explain the police will use the most appropriate and best available technology and techniques to limit their examination of a device to only that material strictly necessary for the line of enquiry. Technology is developing, both that used for extraction and that used in 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, so the material must be downloaded so a search tool can then be applied. ■ **Length of time** – how long the device and material 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 offering an alternative device where possible. Devices will be returned without any unnecessary delay. ■ **Contact details** – how to contact the investigator responsible for the device and extracting the material. This will also include how to withdraw consent for having possession of the device and/or extracting material. ■ **The individual's rights** – right to complain to the ICO with details on how to do so and in particular their right to refuse to hand over their device (See **Principle 4**). The inspector's (or police staff equivalent) authority will be required to authorise the extraction of the material. This inspector's authorisation should also be noted on the DPN, together with a record of their rationale, including the considerations of the 'strictly necessary' and proportionate criteria.

Principle	Detail
	Victims, witnesses and suspects **Limiting the information given to device users** When managing an individual's personal information, the police will be as transparent as possible. However, there may be circumstances where it is not possible to provide the device users with the full details of the use of their material. For example, where doing so may alert a suspect to an investigation or may adversely affect safeguarding measures. In these situations, **section 44 (4) of the DPA 2018** gives data controllers the right to restrict the sharing of this information if it is a necessary and proportionate measure to: ■ avoid obstructing an official or legal enquiry, investigation or procedure ■ avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties ■ protect public security ■ protect national security ■ protect the rights and freedoms of others This power may be considered to prevent the device user tampering with or remotely accessing the device.
Principle 3: Request agreement. Investigators will ask the device user for informed agreement to take possession of the personal digital device for the purpose of extracting material.	**Victims and witnesses** The investigator will ask the victim or witness for their informed agreement when acquiring the digital device. The investigator will consider who can give informed agreement in cases where, for example, the device is shared, owned or used by different people. The investigator will also consider whether the device user has the capacity to give permission (see below). In all cases, where the device and/or material is owned by a victim or witness, an inspector's authority (or equivalent police staff grade) will be required to extract material from it because of the potential intrusion into a person's private life.

Principle	Detail
	Capacity to give informed agreement The investigator or police responder will consider whether the victim or witness has capacity to give informed agreement for their digital device to be taken by the police and data to be extracted. They will also consider whether their ability to understand is affected by their age or any learning impairment, injury, intoxication or trauma for example. They will specifically consider their capacity to provide informed agreement to hand over the device where the device user is a child; an adult with cognitive impairment; a person for whom English is not their first language or the victim/witness has experienced trauma. There may be obvious and non-obvious indicators. Consider whether the individual needs independent legal support and/or time to consider their decision. Where it is believed the device user may lack capacity or is incapacitated, the investigator will ensure steps are taken to ensure informed agreement is obtained in a way that reflects the rights of that person. For example, more time could be allowed to make the decision or investigators could ensure suitable support is available. Where appropriate, contact details may be provided so support can be obtained before informed agreement is sought, for example by an appropriate adult, guardian, advocate, interpreter or legal representative. If the device user is not present (for example in missing persons investigations or where the device user is deceased), the investigator should consider whether it is 'strictly necessary' that material is extracted to support a law enforcement purpose. If it is strictly necessary and: ■ **urgent** – seek the authority of a person most likely to be able to provide informed agreement on behalf of the absent individual (consideration should be given to the possibility that the person could be considered a suspect)

Principle	Detail
	■ **there is an immediate risk to an individual** – if there is no other way of obtaining informed agreement and there is no apparent power to obtain material, the policing requirement to safeguard people would suggest that strictly necessary material can be extracted from the phone in these circumstances ■ **not urgent** – seek legal advice For further information on capacity in under 18s, see **here** and for the impact of trauma, see **here**. For information on the impact of the provision of independent legal support for victims of sexual violence, see the evaluation of the pilot **here**.
	Suspects In cases where a digital device is being acquired through informed agreement, for example the suspect has not been arrested and no other legal power has been used, the same requirement to obtain informed agreement and to ensure the individual has the capacity to provide that informed agreement apply. Where the device has been acquired through other lawful means (for example arrest or the use of a warrant) there is the same requirement to inform the suspect of what material will be extracted, for what reason, under what lawful basis and how it will be used (subject to the exceptions in section 45(4) of the DPA 2018 noted above). See **Principle 2**.

Principle	Detail
Principle 4: The right to refuse permission. Where the device is being acquired through informed agreement, the device user has the right to refuse to hand over their personal digital device for the purpose of extracting material. There are some exceptions to this principle.	**Victims and witnesses** The police will always seek the informed agreement of victims and witnesses to acquire their personal digital devices for the purposes of extracting material. Where informed agreement is being used to acquire the device, investigators will advise that victims and witnesses have the right to refuse to hand over their device to the police for the purposes of extracting material. Investigators may provide contact details for agencies and organisations who can advise the device user on their decision to hand over their device (see **Principle 3** – section on capacity for further details). Some device users may wish to seek legal advice.
	If permission is refused Investigators will explain further the reasons for needing to obtain material from the device and what will happen to it if it is made available to the investigator. Investigators should seek to understand the concerns of the individuals to allay them as far as possible and, where necessary, mitigate any safeguarding risks raised. Many factors may influence an individual's willingness to share their material. For example, they may: ■ be concerned about intrusion into material not relevant to the case and that information about for example, their sexuality, health or immigration status may be used to discredit them ■ feel at risk without their device ■ feel unable to make an informed decision at that time because of trauma or injury These concerns should be considered and all efforts to obtain the evidence while addressing these issues made, such as through less intrusive means (see, for example, **Principle 1** in relation to screenshots). Where the victim/witness still feels unable to hand over their device, investigators should explain there is a risk that:

Principle	Detail
	■ it may not be possible to pursue the investigation ■ a witness summons may be issued ■ any trial resulting from the investigation may be halted Explain to the victim or witness they must not delete potentially relevant material from their device and, if they do so, this might prevent the police from carrying out a fair investigation, which could result in the investigation being closed. Investigators will continue to investigate the case, considering alternative sources of material that may support the line of enquiry. The defence may seek to have charges dismissed where relevant evidence is not available. Investigators will make a record of all actions and conversations about the refusal and the rationale for the decisions made. There are some circumstances where it may be necessary and proportionate to acquire a device without the agreement of the victim or witness. For example, when there is an identifiable basis for believing the device user or someone else is at risk of harm. Where this is the case, the investigator can apply for a warrant to seize the device and relevant material (see, for example, College of Policing **APP on search warrants**). An inspector should authorise any such applications.
	Withdrawing agreement If the victim or witness changes their mind and wishes to withdraw their agreement for the use of their material, the investigator should try to understand why, allay any concerns and explain the reasons why the material is necessary. The investigator will explain the potential impact of withdrawing agreement: ■ it may not be possible to pursue the investigation ■ any trial resulting from the investigation may be halted ■ the material already extracted as part of the investigation so far will be retained The investigator may decide to proceed without agreement. This could be because:

Principle	Detail
	■ there is a risk of harm to the device user or others that cannot be mitigated through less intrusive means ■ they need to fulfil police obligations under the CPIA to obtain and retain materials and to pursue all reasonable lines of enquiry The investigator will explain the reasons to the device user, unless doing so would put them or others at an increased risk. If a person withdraws their agreement, material that has already been acquired and is relevant material will be retained as part of the investigation records.
	Suspects The right to refuse to agree to hand over the device as described above for victims and witnesses also applies to suspects where the device is being acquired by informed agreement. For example, they have not been arrested and no other powers have been used to seize the device. The police do have specific powers to seize material from suspects that they believe to contain evidence of an offence. These powers vary from case to case and agreement is not required in these circumstances. Where these powers are used, they will be explained to the suspect.

Principle	Detail
Principle 5: Ensure extracted material is adequate, relevant and not excessive for the purpose for which it was processed. 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 where possible.	**Victims, witnesses and suspects** Investigators will only extract the minimum amount of data required to satisfy the line of enquiry. Where material has been extracted, but it is not relevant to the investigation, it will not be examined and will be deleted where possible. When material has been acquired as part of a search and some of that material has been identified as irrelevant before it has been examined, for example material predating an offence that could not have a bearing on the investigation, this material should be deleted and not retained in anticipation of it possibly being relevant later. If technology doesn't allow the targeting of only the relevant material, it may be necessary to acquire more material than needed. If this happens, the investigator will set clear parameters to satisfy the reasonable line of enquiry and review material only within those parameters. Where possible, the working copy for the investigator should contain only the necessary material. If further searches of the device or the extracted material are required, an incremental approach should be applied. The victim/witness/suspect should be informed of the details of the new lines of enquiry, the lawful basis and their right to refuse. Their agreement should be sought and authorisation by an inspector obtained for the additional searches. Once the material has been extracted, the device will be returned to the owner without undue delay. Deletion of non-relevant material should take place as soon as reasonably possible. If a suspect has been identified and it is anticipated they can suggest different search parameters within a reasonable time, the material may be retained to allow this to happen. In making this decision, the investigating officer will need to decide what is necessary and proportionate for the investigation.

Principle	Detail
	When material is extracted from a digital device, a copy of the material is created. The copied material will be deleted and the original material will be retained on the device. In some cases, it may not be possible to delete non-relevant material from the extracted material without deleting relevant material, If this is the case the following is required. ■ It should be retained securely. ■ It should not be subject to further processing. ■ Processes should be in place to ensure it cannot be inappropriately accessed, reviewed or disseminated. ■ There should be clear retention and deletion policies in place. See paragraph 21-25 of **Annex A of the AG's Guidelines on Disclosure (2020)** and also the **NPCC DPNa** officer information form. Specific considerations apply to **excluded material**, special procedure material or material that is subject to legal professional privilege. Should this type of material be sought, anticipated or inadvertently acquired, the appropriate legal provisions should be applied. See the **AG's Guidelines on Disclosure** for further guidance. Extracted material will fall into four categories: **Used material** ■ Evidence – 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**. **Unused material** ■ Unused relevant material, although it is relevant to the case, 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**.

Principle	Detail
	■ 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 (where possible) and as soon as reasonably possible. ■ Unused, non-relevant material that cannot be separated from the evidence or unused relevant material. This material will be retained and stored in the same way as the evidence or unused material.
	Victims and witnesses **Identification of additional criminality** Where the extraction of strictly necessary material identifies material relating to offences not under investigation, the investigating officer will need to decide what action to take. The investigator will need to bear in mind the seriousness of the initial offence being investigated and what is in the best interest of criminal justice. The National Crime Recording Standard (NCRS) will have to be applied and the rationale for all decisions should be recorded for the purposes of accountability and transparency. Before initiating an investigation into such activity, consider the following: ■ 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 on the current investigation, for example the risk to public safety if an offender is not brought to justice. ■ Whether the information about the offence is capable of having a bearing on the initial offence being investigated. If not, it does not need to be revealed to the CPS. But if so, it will need to be added to the disclosure schedule covering sensitive material.

Principle	Detail
	For example, in domestic abuse cases involving people of insecure or uncertain immigration status, or where evidence of drug use is also identified, there will be a need to consider the potential of pursing these issues. For example, could a decision to share information with Immigration Enforcement or prosecute for drug use affect an investigation into a domestic abuse incident or crime? If so, is it more desirable not to share information because more effective provisions for safety would be achieved through investigation of the domestic abuse, through safeguarding measures for the victim and/or taking action against the alleged perpetrator that might protect the victim and others? Where the investigation relates to a sexual assault, a detective chief inspector must authorise investigation of the unrelated criminal activity. This level of authority is considered appropriate because of the sensitive judgement to be made. Where material is recovered during a strictly necessary and proportionate examination of material 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 material may be retained and investigated by the police as part of a new investigation, in accordance with this guidance.
	Suspects If police identify an unrelated risk to any individual or identify evidence of unrelated offences, they may share that material in line with the DPA 2018. They will tell the suspect when this has been done unless doing so would put anyone at risk, or prejudice an ongoing investigation.

Principle	Detail
Principle 6: Safeguarding. Investigators will consider risk of harm and any issues that could have adverse impact on the device user when deciding how to extract material.	**Victims, witnesses and suspects** Consideration will be given to any situational or personal factors that may be affected if the device user permits the police to take possession of their device, in particular an increased risk of harm or impact to 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, material on the device may highlight confidential personal information, for example their sexuality. Or information that may create risk of harm through, for example, honour-based abuse, threats of violence and intimidation. There may also be also a risk to the privacy of others whose information is included in the material on the device. Efforts will be made to mitigate those risks, for example: exploring all other methods to obtain the evidence; not taking 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 material will be stored securely and only accessed by those with a legitimate reason to do so, in line with the DPA 2018 (see storage **Principle 8**). ■ Only material that meets the test for disclosure under the CPIA Code of Practice will be shared with the defence. Under the DPA 2018, disclosed material will be appropriately redacted so personal details or other irrelevant information are not disclosed (eg, photographs, addresses or full telephone numbers). Material can be shared for the purposes of safeguarding in accordance with the DPA 2018.

Principle	Detail
Principle 7: Updating, reviewing and managing material obtained during an investigation. Investigators will review the retention of digital devices and the extracted material at regular intervals. The storage, retention and disposal of material 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 device user of any proposal to change how the extracted material is used and request further agreement.	**Victims and witnesses** The investigator will be responsible for updating, reviewing and managing any material obtained during the investigation. During an investigation there may be a change to how the material is used or a new line of enquiry may develop. This may require further material to be examined, either by further searches of a securely held full download or by returning to the device user to request agreement for further material to be extracted. These changes may occur when, for example: ■ the investigation has uncovered new material identifying new lines of enquiry, for example 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 material extracted from the device has been or will be shown to the suspect and they identify further reasonable lines of enquiry ■ if there is a decision-point in the case where the device is relevant, for example a suspect is to be charged The investigating officer will inform the victim or witness of any proposed changes and seek renewed agreement to extract or use the material. The victim/witness has the right to refuse further requests or withdraw their agreement as they do for the initial request. See **Principle 4**. Investigations can take a long time and a device may be required for a significant period until all relevant material has been extracted. However, the device will be returned to the device user without undue delay.

Principle	Detail
	The victim or witness will be kept informed of the progress of the investigation at a frequency 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, such as the arrest of a suspect ■ the use of the material on the device ■ the likely timescales for return of the device and for the retention of any downloaded material A specific update timetable will be agreed. See **Victims' Code**. **Storage** – All material extracted from personal digital devices will be stored with effective safeguards in place to prevent unauthorised access or disclosure (the **ICO report** sets an expectation that all extracted material should be stored in encrypted form).
	Suspects Suspects will be told when a new or revised search of their device is needed, for example in respect of a new line of enquiry and how the material recovered will be used. When managing personal information, including a suspect's, the police will be as transparent as possible. **Section 44(4) of the DPA 2018**, however, gives data controllers the right to restrict information given to suspects if it is necessary and proportionate (see **Principle 2**).

Principle	Detail
Principle 8: Sharing information. Investigators will not reveal personal information unless it is strictly necessary to do so as part of the investigation or for other law enforcement purposes.	**Victims and witnesses** Investigators will not reveal personal information to the defence unless it is part of the prosecution case or it meets the **test for disclosure**. When sharing the material, it will be served in a suitably redacted form to ensure personal details or other irrelevant information are not unnecessarily revealed (for example photographs, addresses or full telephone numbers). Any further processing, such as sharing data, is possible but must be in accordance with the DPA 2018 (see **APP on sharing police information**). See Principle 5 relating to criminality uncovered during a search of a digital device. When managing an individual's personal information, the police will be as transparent as possible. However, there may be circumstances when informing people of how their material is being shared is not advisable. In these circumstances, **Section 44(4) of the DPA 2018** gives data controllers the right to restrict the sharing of this information if it is necessary and proportionate (see **Principle 2**).
	Suspects/defendants Material from a suspect's device will not be shown to the victim or witness unless it is necessary as part of the investigation. Only material 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	Detail
Principle 9: Recording actions. All actions in relation to the extraction of digital material and management of that extracted material should be recorded.	**Victims, witnesses and suspects** A record should be made of all actions in relation to the extraction of digital material, including collection, alteration, consultation, disclosure (including transfers), combination and deletion. For example, a record should be kept of: ■ All conversations with the device user; all decisions made and any approvals given, including the rationale for the extraction of material. This record could be in writing on a pro forma (for example, the NPCC-approved DPN) or as a verbal record recorded by BWV. ■ Each time an investigator or analyst examines the material extracted, this will also be logged. ■ Where a change to the use of the extracted material or further searches of a securely held full download are required, because for example of a development in the investigation or a new line of enquiry, these will also be recorded. ■ If a device user refuses to allow their device to be seized, or the material extracted, this decision will be logged, outlining their reasons and including any associated conversation and decisions. ■ Where extracted material is deleted, this will be recorded. ■ The details of the searches and any search parameters will also be recorded within the investigation record. **Section 61 of the DPA 2018** outlines the responsibilities for recording processing activities. **Section 62 of the DPA 2018** relates to logging and states that logs must be kept of at least the following processing operations in automated processing systems: collection, alteration, consultation, disclosure (including transfers), combination and erasure. See also **College of Policing APP on data protection**.

Principle	Detail
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 guidance and that a DPIA and EIA of all relevant investigative processes are undertaken.	Chief officers will ensure this guidance is implemented. This includes ensuring: ■ an appropriate sensitive processing policy is in place ■ records are made of all data processing actions in relation to extracted digital material ■ A DPIA is carried out on all relevant investigative processes and data processing operations. A DPIA will be completed: - before the procurement or rollout of new hardware or software for mobile phone data extraction and processing, including any analytical capabilities - for any software used for the extraction of material from mobile phone and other devices, ensuring privacy by design is maintained and privacy safeguards are built into any new procurement or upgrade - 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 EIA is completed for all investigative processes and data extraction procedures ■ officers and staff have the required skills and knowledge to implement this guidance ■ supervision and other supporting processes are in place to embed the guidance

References

Attorney General's Office. (2020). '**Attorney General's Guidelines on Disclosure**' [internet]. Available from: **assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946082/Attorney_General_s_Guidelines_2020_FINAL_Effective_31Dec2020.pdf**

British and Irish Legal Information Institute. (2020). '**Bater-James & Anor v R. [2020] EWCA Crim 790**' [internet]. Available from: bailii.org/ew/cases/EWCA/Crim/2020/790.html

British and Irish Legal Information Institute. (2013). '**Bank Mellat v Her Majesty's Treasury (No. 2) [2013] UKSC 39**' [internet]. Available from: bailii.org/uk/cases/UKSC/2013/39.html

Care Quality Commission. (2019). '**Brief guide: capacity and competence to consent in under 18s**' [internet]. Available from: **cqc.org.uk/sites/default/files/Brief_guide_Capacity_and_consent_in_under_18s%20v3.pdf**

Crown Prosecution Service. (2018). '**A guide to "reasonable lines of enquiry" and Communications Evidence**' [internet]. Available from: **cps.gov.uk/sites/default/files/documents/legal_guidance/Disclosure-reasonable-lines-of-enquiry-and-communications-evidence.pdf**

Crown Prosecution Service. (2019). '**Psychological Evidence Toolkit – A guide for Crown Prosecutors**' [internet]. Available from: **cps.gov.uk/legal-guidance/psychological-evidence-toolkit-guide-crown-prosecutors** [Accessed 16 March 2020]

Crown Prosecution Service. (2019). '**CPS Guidance for Experts on Disclosure, Unused Material and Case Management**' [internet] Available from: **cps.gov.uk/legal-guidance/cps-guidance-experts-disclosure-unused-material-and-case-management**

Forensic Science Regulator. (2020). '**Annual Report (17 November 2019 – 16 November 2020**' [internet] Available from: **assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950087/FSR_Annual_Report_2019-2020_Issue_1.pdf**

Home Office. (2019). '**Crime Recording General Rules**' [internet]. Available from: **assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/977232/count-general-apr-2021.pdf**

Information Commissioner's Office. (2020). '**Investigation report: Mobile phone data extraction by police forces in England and Wales**' [internet] Available from: **ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/**

Information Commissioner's Office. (2018). '**Guide to Data Protection**' [internet]. Available from: **ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/**

Ministry of Justice. (2020). '**Criminal Procedure and Investigations Act 1996 (section 23(1)) Code of Practice**' [internet]. Available from: **assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/931173/Criminal-procedure-and-investigations-act-1996.pdf**

Privacy International. (2018). '**Digital stop and search: how the UK police can secretly download everything from your mobile phone**' [internet]. Available from: **privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf**

Smith O and Daley E. (2020). '**FINAL REPORT: Evaluation of the Sexual Violence Complainants' Advocate Scheme**' [internet]. Available from: **needisclear.files.wordpress.com/2020/11/svca-evaluation-final-report-1.pdf**

United Kingdom. Parliament. (1997). '**Police Act 1997**' [internet]. Available from: **legislation.gov.uk/ukpga/1997/50/contents**

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

Follow us
@CollegeofPolice

C74I0521