



Home Office

Extraction of Information from electronic devices: code of practice

October 2022

Extraction of Information from electronic devices: code of practice

Presented to Parliament pursuant to Section 42(5) of the Police, Crime,
Sentencing and Courts Act 2022

October 2022



© Crown copyright 2022

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at <http://www.gov.uk/government/consultations>

ISBN 978-1-5286-3700-8

E02802691 10/22

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of His Majesty's Stationery Office

Contents

Part 1: Introduction	5
Preamble	5
Introduction	5
Effect of the code	8
What this code does not cover	9
Part 2: Human Rights and Data Protection	11
The Human Rights Act 1998	11
The Equality Act 2010	12
The Data Protection Act 2018 and the UK General Data Protection Regulation	12
Data processing for law enforcement purposes	13
Data processing for non-law enforcement purposes	16
Part 3: Exercise of these powers	18
Section 37: the power and the purposes for which it may be exercised	18
Section 38: Voluntary provisions and agreement where a device user is a child or adult without capacity	20
Section 40: Extracting information under Section 37 without voluntary provision or agreement: special cases	20
Section 41: Extracting information: investigations of death	21
Section 41: the power and the purposes for which it may be exercised	21
Reasonable belief that the information on the device is relevant	22
Relevant to a reasonable line of enquiry	22
Relevant to a purpose in the Act – Missing persons etc	23
Necessity and proportionality	24
Risk of obtaining other information	25
Confidential information	26
Assessing whether there is a risk of obtaining confidential information	27
How to proceed after assessing whether there is a risk of obtaining confidential information	28
What to do if confidential information is unintentionally obtained	29
Sanctioning use of the powers	29

Recording the use of these powers	30
Extracting Information	31
Applicable devices	32
CCTV	33
Type of extraction	33
Retention and deletion of extracted information	34
Part 4: Voluntary provision of device and agreement to extract information	35
Requirements for voluntary provision and agreement	35
Voluntary provision, agreement and undue pressure	35
Written notice	36
Confirmation of voluntary provision and agreement	38
Withdrawal of agreement	39
Part 5: Use of the Section 37 power with vulnerable people	40
Vulnerable people / victims of crime	40
What does 'vulnerable' mean?	41
Voluntary provision and agreement and vulnerable people	43
Privacy impact and vulnerable people/victims	44
Safeguarding and vulnerable victims	45
Part 6: Section 38: Children and adults without capacity	47
Children	47
Who can, and cannot, make decisions for a child?	47
Adults without capacity	50
Who can, and cannot, make decisions for an adult without capacity?	51
Obtaining the views of the adult without capacity	54
Definitions	56
Annexes	59
Annex A – Schedule 3 Authorised Persons	59
Annex B - Overview of the principles of Bate-James	62
Annex C – DPA and GDPR	63
Annex D – Example Digital Processing Notice to obtain written agreement	68

Part 1: Introduction

Preamble

1. This code of practice relates to the exercise of powers in Chapter 3 of Part 2 of the Police, Crime, Sentencing and Courts Act 2022 (“the Act”). It should be read alongside the explanatory notes for Chapter 3 of Part 2. This code is issued pursuant to Section 42 of the Act, which provides that the Secretary of State must prepare a code of practice containing guidance about the exercise of the powers in Sections 37(1) and 41(1). These powers allow authorised persons to extract information stored on electronic devices in certain circumstances.
2. This code applies to all authorised persons named in Schedule 3 to the Act. It is a publicly available document and should be readily accessible by any authorised persons who may wish to review it¹.

Introduction

3. This code of practice provides practical guidance to authorised persons on the use of the powers, including how they should determine the correct legal power to use in the circumstances and how they should confirm that extraction of information is necessary and proportionate. This is needed to ensure that authorities exercise their functions in accordance with the law and protect the privacy of those whose information is extracted. This code will ensure a greater understanding of the use of the powers and their application will support the overall aims of maintaining and improving the trust and confidence of the public.
4. This code does not supersede guidance/codes that accompany other pieces of legislation, and only applies as regards the powers in Chapter 3 of Part 2 of the Act. If another power is being used as the basis for extracting information from an electronic device, the guidance/code for that power will apply.
5. The power in Section 37 of the Act allows authorised persons to extract information stored on an electronic device if a user of the device has voluntarily provided the device and agreed to the extraction of information from it². The power may be exercised for the purposes of preventing, detecting, investigating or prosecuting

¹ See Annex A for the list of authorised persons in Schedule 3 to the Act and a definition of an ‘authorised person’.

² Section 37(10) defines ‘electronic device’, ‘information’ and ‘user’. Section 37(11) is clear that references to the extraction of information include its reproduction in any form.

crime³; helping to locate a missing person, or protecting a child or an at-risk adult⁴ from neglect or physical, mental or emotional harm.

6. Section 38 deals with the application of Section 37 in cases where a user of a device is a child, or adult without capacity.
7. Section 40 deals with the application of Section 37 in three special cases, including:
 - i. where the device user has died, and they were a user of the device immediately before they died, or
 - ii. where the device user is a child or an adult without capacity and the authorised person reasonably believes that their life is at risk, or there is risk of serious harm to them, or
 - iii. where the device user is missing, and they were a user of the device immediately before they went missing and the authorised person reasonably believes that their life is at risk or there is a risk of serious harm to them.
8. The power in Section 41 of the Act allows authorised persons to extract information stored on an electronic device if a person who was a user of the device has died and, immediately before they died, they were a user of the device. This power may be exercised for the purposes of certain investigations or inquests into the person's death⁵.
9. An electronic device is defined in the Act as 'any device on which information is capable of being stored electronically and includes any component of such a device.' This can include devices such as mobile phones, tablets, laptops and computers, and components such as removable storage USB or other storage devices, and may include 'smart' devices such as smart watches or voice activated speakers. This list is not exhaustive. The definition is necessarily broad to ensure it is not rendered redundant by changing technology. The device must be capable of storing information and not merely a means of accessing it.
10. Extraction of information also includes reproduction in any form and so activities such as physical copying and all forms of electronic or digital reproduction, for example screenshots (depending on the technology used), are within scope of this code and

³ Section 37(3) explains that the reference to 'crime' is a reference to (i) conduct which constitutes one or more criminal offences in any part of the UK, or (ii) conduct which, if it took place in any part of the UK, would constitute one or more criminal offences.

⁴ Section 37(10) defines 'adult' and 'child', and Section 37(4) sets out when an adult is an 'at-risk adult'.

⁵ Section 41(2) lists the relevant investigations and inquests, and Section 41(3) makes clear that the power may be exercised for the purposes of determining whether such an investigation or inquest should be held.

the powers in the Act. Further information on the types of devices and extraction technology can be found in [Part 3](#) of this code.

11. Section 44 of, and Schedule 3 to, the Act set out who is an authorised person:
 - Part 1 of Schedule 3 names those authorised persons who may exercise either power for any specified purpose
 - Part 2 of Schedule 3 names those authorised persons who may exercise the Section 37 power for any specified purpose (these authorised persons may not exercise the Section 41 power)
 - Part 3 of Schedule 3 names those authorised persons who may only exercise the power in Section 37 for the purposes of the prevention, detection, investigation or prosecution of crime (these authorised persons may not exercise the Section 37 power for other purposes or the Section 41 power)
12. An 'authorised person' can refer to the person interacting with the device user and the person providing agreement (where different), the person authorising the scope of the extraction of information, and the person completing the extraction of information from the electronic device.
13. The agreement to extract information has only to be given once for each request in order for the extraction to be carried out. For example, the first authorised person is a police officer responsible for investigating an allegation of crime. They are responsible for establishing the reasonable line of enquiry, for satisfying all other requirements of the Act, (necessity and proportionality etc) and for seeking authorisation to use the powers. This authorised person will interact with the device user and, if different, the person providing agreement (where this is required by the Act, such as when the device user is a child, or an adult without capacity) and they will ensure that the device is volunteered, and agreement given. They may be suitably trained and have access to technology that allows them to carry out the extraction themselves, or they may give the device to a second authorised person to extract the information, for example to a Digital Forensic Unit or to an external digital forensic service provider. This second authorised person will then carry out the extraction in accordance with the details on the written agreement. They do not need to seek further agreement to carry out the extraction.
14. An authorised person must only exercise the Section 37 power for the purposes of preventing, detecting, investigating or prosecuting crime if they reasonably believe that information stored on the device is relevant to a reasonable line of enquiry⁶ which is being, or is to be, pursued by an authorised person.⁷

⁶ [CPS guidance for England and Wales - Disclosure - A guide to "reasonable lines of enquiry" and communications evidence | The Crown Prosecution Service \(cps.gov.uk\)](#)

⁷ Section 37(2)(a) and Section 37(5)(a) and 37(5)(c) of the Act.

15. In a case where the authorised person proposes to exercise the Section 37 power to help locate a missing person, or for the purposes of protecting a child or an at-risk adult from neglect or physical, mental or emotional harm, the authorised person must reasonably believe that the information stored on the device is relevant to that purpose.⁸
16. In any case, the authorised person must be satisfied that the exercise of the Section 37 or 41 power is necessary and proportionate to achieve the purpose for which they propose to exercise the power. Where an authorised person thinks that there is a risk of obtaining excess information, the exercise of the power will only be proportionate if they are satisfied that:
 - (i) there are no other means of obtaining the information sought which avoid that risk, or
 - (ii) there are such other means, but it is not reasonably practicable to use them.
17. In all cases, the authorised person must use the least intrusive means of processing the information as possible in the circumstances. This may be by selectively extracting the relevant information, or where this is not technically possible, by restricting the review of the excess information obtained.
18. Section 39 sets out the requirements that must be met for an individual to be treated as having voluntarily provided a device and agreed to the extraction of information from it (for the purposes of Section 37 or 38). These requirements ensure that individuals are not placed under undue pressure and are given written notice of their right to refuse, and of the reason for, and details of, the request.

Effect of the code

19. When using or deciding whether to use the Section 37 power or the Section 41 power, an authorised person must have regard to this code⁹.
20. Failure to comply with the code could result in the incorrect processing of personal information and to a breach of the Data Protection Act 2018 and therefore be subject to further enforcement regulations, such as fines issued by the Information Commissioner¹⁰. A failure on the part of an authorised person to act in accordance with the code does not of itself render the person liable to any criminal or civil proceedings. However, a decision to exercise (or not exercise) the power under Sections 37 and 41 of Chapter 3 of Part 2 of the Police, Crime, Sentencing and Courts Act 2022 (“the Act”) may be open to legal challenge.

⁸ Section 37(2)(b) and (c) and Section 37(5)(b) and 37(5)(c) of the Act.

⁹ Sections 37(11) and 41(10) of the Act.

¹⁰ Section 67 of Part 3 of the DPA 2018 introduces a duty on all organisations to report certain types of personal data breach to the Information Commissioner. [Report a breach - ICO](#)

21. The code is admissible in evidence in criminal or civil proceedings, and a court may take into account a failure to act in accordance with the code in determining any question in the proceedings (e.g., on the admissibility of evidence extracted from an electronic device)¹¹. Any misuse of these powers or failure to follow this code is likely to have serious negative consequences for complainants whether by resulting in unnecessary requests to share personal information, or by sharing of information that is later deemed inadmissible. Failure to comply with the code could also be considered in professional disciplinary hearings. Authorised persons should act in accordance with any guidance such as codes of conduct or ethics issued by their organisation. Where the authorised person is a police officer or member of police staff the following may apply:

- In **England and Wales** – Failure to follow the code and use the powers lawfully could result in a breach of the College of Policing Code of Ethics, for example the second standard to use powers and authority lawfully and proportionately and will respect the rights of all individuals.¹²
- In **Scotland** – Failure to follow the code and use the powers lawfully could result in a breach of the Code of Ethics for Policing in Scotland, for example the commitment that ‘In carrying out my duties I shall respect everyone’s fundamental rights. I will only interfere with privacy or family life when I am legally authorised to do so.’¹³
- In **Northern Ireland** – Failure to follow the code and use the powers lawfully could result in a breach of the Code of Ethics for the Police Service Northern Ireland, for example article 3.1 on Privacy and confidentiality which states that ‘Police officers shall gather, retain, use and disclose information or data in accordance with the right to respect for private and family life contained in Article 8 of the European Convention on Human Rights and shall comply with all relevant legislation and Police Service policy and procedure governing the gathering, retention, use and disclosure of information or data.’¹⁴

What this code does not cover

22. This code does not contain guidance about the following:

- other sections of the Act (i.e., sections other than those contained in Chapter 3 of Part 2)

¹¹ Section 42(9) and (10) of the Act.

¹² [Code_of_ethics.pdf \(college.police.uk\)](#)

¹³ [Code of Ethics for policing in Scotland - Police Scotland](#)

¹⁴ [nipb08ethics-2.pdf \(ulster.ac.uk\)](#)

- extraction of information from a device using coercive or compulsory powers, such as a search warrant, production order or statutory notice
- covert extraction of information from a device – for example, where it is necessary as part of the investigation to obtain evidence from a device without a user's knowledge
- extraction of information that is not stored on the device but held elsewhere, such as 'cloud' storage¹⁵

¹⁵ The 'cloud' is sometimes referred to as the system of remote data storage or the sharing of data through a computer or telecommunications network.

Part 2: Human Rights and Data Protection

23. Both the Section 37 power and the Section 41 power must be exercised in accordance with other legal obligations and duties, including the following:
- **The Human Rights Act 1998, ensuring compliance with the European Convention on Human Rights ('the ECHR')**
 - **The Equality Act 2010¹⁶**
 - **Data Protection Act 2018 ('the DPA')**
 - **UK General Data Protection Regulation ('the UK GDPR')**

The Human Rights Act 1998

24. The Human Rights Act 1998 gives effect in UK law to the rights set out in the ECHR. Section 6 of the Human Rights Act makes it unlawful for any public authority to act in a way which is incompatible with a Convention right.
25. Article 8 of the ECHR sets out the right to respect for their private and family life, home, and correspondence. It provides that 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. This includes, among other things, where interference is necessary for the prevention of disorder or crime and for the protection of the rights and freedoms of others¹⁷.
26. The authorised person must carefully consider (i) whether the extraction of information in pursuance of the powers will amount to an interference with the exercise of a person's rights under Article 8, and (ii) if so, whether that interference is justifiable (bearing in mind the test set out in Article 8 and summarised above).
27. Electronic devices such as mobile phones are almost certain to contain sensitive information about the individual device user and their family and friends. The authorised person should consider the impact of intrusion into the private life of the individual and their contacts at all points in the decision-making process – when determining what information is needed to support a reasonable line of enquiry (where applicable), and in determining if the use of these powers is necessary, proportionate and that there are no other, less intrusive means of accessing the

¹⁶ [Equality Act 2010 \(legislation.gov.uk\)](https://legislation.gov.uk)

¹⁷ [Link to the Guide on Article 8 of the European Convention on Human Rights](#)

required information. Further detail on obligations to protect the privacy of device users that must be considered before using the powers can be found in [Part 3](#) of this code.

28. When considering Article 8, authorised persons must also consider compliance with other Convention rights, including Article 6 of the ECHR. Article 6 of the ECHR sets out the right to a fair trial, so it is necessary for authorised persons to consider how the information sought may impact on that right. The Attorney General’s Office has produced guidance on the balance between Article 8 and Article 6 rights¹⁸.

The Equality Act 2010

29. Authorised persons must ensure they act in accordance with the Equality Act 2010 and the Public Sector Equality Duty¹⁹ to eliminate discrimination, advance equality of opportunity and foster good relations between people when carrying out their duties.
30. An Equality Impact Assessment (EIA) has been produced for the PCSC Act that demonstrates compliance with the Public Sector Equality Duty²⁰ (PSED)

The Data Protection Act 2018 and the UK General Data Protection Regulation

31. Careful considerations as to which data protection regime is applicable to the processing of personal data when using the powers, ensuring that the relevant regime is complied with. When deciding which regime applies, consideration should be given to the primary purpose for the processing. If the primary purpose for processing is law enforcement,²¹ then Part 3 of the DPA will apply, otherwise Part 2 of the DPA read with the UK GDPR will apply.
32. Article 4 of the UK GDPR and Section 3 of the DPA defines ‘processing’ as meaning “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”.

¹⁸ [AG Guidelines 2022 Revision Publication Copy.pdf \(publishing.service.gov.uk\)](#)

¹⁹ [Public sector equality duty - GOV.UK](#)

²⁰ [Home Office measures in the Police, Crime, Sentencing and Courts Bill: Equalities Impact Assessment - GOV.UK \(www.gov.uk\)](#)

²¹ S.31 DPA defines ‘law enforcement purposes’ as “the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

33. Any processing information handled in accordance with the Data Protection Act 2018/UK GDPR must ensure that any information extracted is minimised, and that only the data that is needed for the purpose it is being extracted for is collected and retained.²²
34. Authorities named on Schedule 3 should consider if they need to complete or update an existing Data Protection Impact Assessment their organisations use of these powers.
35. Information about a deceased person does not constitute personal data and therefore is not subject to the UK GDPR or DPA, which only applies to personal data relating to living individuals. However, processing data from a device obtained from a deceased person that contains data relating to other identifiable living persons, may constitute the processing of personal data under the DPA or UK GDPR. This means that in all cases where the power in Section 37 and Section 41 is used where the device user has died, the authorised person must consider if the device being extracted is likely to contain information about identifiable living persons. It is almost certain in the case of devices such as mobile phones, tablets, and laptops that they will and so the following guidance on the application of data protection applies.
36. In order for the use of the power under Section 37(2)(a) to be lawful the authorised person must meet all requirements of the Act to ensure that the device is volunteered, agreement given etc and the processing of the information must be strictly necessary for a law enforcement purpose.
37. In order for use of the power under Section 37(2)(b), 37(2)(c) and Section 41 to be lawful the authorised person must meet all requirements of the Act and the processing of the information must be necessary for one of the purposes in UK GDPR, Article 6, 2-6.

Data processing for law enforcement purposes

General overview of DPA responsibilities

38. Part 3 of the DPA is applicable to data processing by competent authorities for law enforcement purposes. Part 3 outlines six data protection principles which must be complied with when processing data for law enforcement purposes, including when exercising these powers, summarised below.
 - (1) The processing of personal data for any of the law enforcement purposes must be lawful and fair.

²² For more information: [Data Protection Act 2018 \(legislation.gov.uk\)](https://legislation.gov.uk)

- (2) The law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.
 - (3) Personal data processed for any of the law enforcement purposes must be adequate, relevant, and not excessive in relation to the purpose for which it is processed.
 - (4) Personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.
 - (5) Personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.
 - (6) Personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, “appropriate security” includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).
39. Authorised persons should refer to their own guidance on responsibilities under the DPA.
40. When the power in Section 37 of the Act is used for the extraction of information for law enforcement purposes, for example preventing, detecting, investigating, or prosecuting crime, the authorised person must comply with Part 3 of the DPA²³.
41. The DPA states that the processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law, and either;
- (a) the data subject has given consent to the processing for that purpose, or
 - (b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority.²⁴
42. Section 35 of the DPA also applies when processing for law enforcement purposes is ‘sensitive processing’²⁵. In these circumstances, the processing is permitted only in the two cases set out in subsections (4) and (5).

²³ See Part 3 of the DPA Act 2018 when processing personal data for law enforcement purposes.

²⁴ See s.30 DPA 2018 for the meaning of “competent authority”.

²⁵ See s.35(8) for a definition of ‘sensitive processing’ and Annex C for an explanation of ‘sensitive processing’ under the DPA Act 2018.

(4) The first case is where—

(a) the data subject has given consent to the processing for the law enforcement purpose, and

(b) at the time when the processing is carried out, the controller has an appropriate policy document in place²⁶.

(5) The second case is where—

(a) the processing is strictly necessary for the law enforcement purpose,

(b) the processing meets at least one of the conditions in Schedule 8, and

(c) at the time when the processing is carried out, the controller has an appropriate policy document in place²⁷

43. The Information Commissioner's Office report on 'Mobile phone data extraction by police forces',²⁸ concludes that **'consent' under the DPA is highly unlikely to be an appropriate condition for processing personal data**, referred to as 'sensitive processing'²⁹ for law enforcement purposes due to the standards that need to be met, and that it would be more appropriate to rely on the condition that the extraction is **strictly necessary** for a law enforcement purpose. Voluntary provision in the PCSC Act does not equal 'consent' as defined under the Data Protection Act 2018³⁰. It is unlikely, because of the imbalance of power between the police and an individual, that the high threshold of fully informed and freely given consent can be achieved. It is also a requirement of 'consent' that it can be withdrawn at any time. This would not always be possible where data has been extracted because of the lawful requirement upon the investigator to reveal the material to a Crown Prosecutor where the material is capable of undermining, or materially weakens the prosecution case, or where it strengthens or assists the defence case. Further, it is unlikely that all of those who must provide consent under UK data protection legislation would be able to do so, as material on the device may relate to many individuals. In these circumstances, the data subjects may not be easily identifiable, or it would be impracticable to do so due to the volume of the material.

44. For 'sensitive processing' for law enforcement purposes, as defined in the DPA, you must be able to demonstrate that the processing is 'strictly necessary' and that you can satisfy one of the conditions in Schedule 8³¹ (statutory purposes, administration

²⁶ For example, the NPCC Digital Processing Notice (DPN).

²⁷ For more information: [Data Protection Act 2018 \(legislation.gov.uk\)](https://legislation.gov.uk)

²⁸ [ICO investigation into mobile phone data extraction by police in the UK | ICO](#)

²⁹ See s.35(8) for a definition of 'sensitive processing' and Annex C for an explanation of 'sensitive processing' under the DPA Act 2018.

³⁰ See Part 4, Chapter 1, Paragraph 84 of the [Data Protection Act 2018 \(legislation.gov.uk\)](https://legislation.gov.uk) for definition of 'consent'.

³¹ [Schedule 8 of the Data Protection Act 2018](#)

of justice, protecting individual's vital interests, safeguarding of children and individuals at risk, personal data already in public domain, legal claims, judicial acts, preventing fraud, archiving etc). This is a requirement that will not be met if you can achieve the purpose by some other reasonable means.

Relevant existing guidance

45. When exercising the Section 37 power for the purposes of preventing, detecting, investigating, or prosecuting crime, authorised persons should consider the responsibilities for disclosure that may arise and should be familiar with the documentation listed below.

In England and Wales

- Attorney General's Guidelines on Disclosure July 2022 (Annex A, Digital Material) and guidance on balancing Article 6 and Article 8 ECHR³².
- Criminal Procedure and Investigations Act Code of Practice February 2015 - GOV.UK

In Scotland

- The Crown Office and Procurator Fiscal Service Disclosure Manual
- Code of Practice of Disclosure of Evidence in Criminal Proceedings

In Northern Ireland

- The Criminal Procedure and Investigations Act 1996 Code of Practice for Northern Ireland (Revised) 2005
- The Code for Prosecutors | Public Prosecution Service Northern Ireland (ppsni.gov.uk)

Data processing for non-law enforcement purposes

46. When the power in Section 37 or in Section 41 of the Act is used for non-law enforcement purposes – for example, to help locate a missing person or to protect a child or an at-risk adult from neglect or physical, mental or emotional harm (where no criminal element exists), or for the purposes of certain non-criminal investigations or inquests into the person's death³³, – the authorised person must comply with the UK

³² [AG Guidelines 2022 Revision Publication Copy.pdf \(publishing.service.gov.uk\)](#)

³³ The DPA only applies to the processing of data for living persons, however, where the processing of data from a deceased's device involves the processing of another person's data, you must comply with UK GDPR and Part 2 of the DPA. For criminal investigations in this scenario, you must comply with Part 3 of the DPA.

GDPR³⁴ (read with Part 2 of the DPA). When extracting information for non-law enforcement purposes, the seven principles under Article 5³⁵ of the UK GDPR need to be met and Article 6³⁶ of the UK GDPR defines the lawful basis on which you can process the data. Article 9 of the UK GDPR also applies when processing 'special category data'³⁷.

47. In every case when assessing if it is necessary and proportionate to use the powers and process information for a non-law enforcement purpose, authorised persons should balance the assessment of risk to the device user with the likely intrusion into their privacy and the privacy of others whose information is stored on their device. Full details of obligations and conditions for processing for non-law enforcement purposes can be found in [Annex C](#) of this code.

³⁴ See the UK General Data Protection Regulation (UK GDPR) when processing personal data for non-law enforcement purposes.

³⁵ See annex C for the seven UK GDPR principles in Article 5.

³⁶ See annex C for the conditions that must be met under Article 6.

³⁷ See annex C for an explanation of 'special category data' under UK GDPR.

Part 3: Exercise of these powers

Section 37: the power and the purposes for which it may be exercised

48. The powers in Section 37 may be used for the purpose of
- 37(2)(a) preventing, detecting, investigating or prosecuting crime,
 - 37(2)(b) helping to locate a missing person, or
 - 37(2)(c) protecting a child or an at-risk adult from neglect or physical, mental or emotional harm.
49. The power in Section 37(2)(a) requires that a user of the device has voluntarily provided their device to an authorised person and has agreed to the extraction of information from it³⁸. Detailed guidance on how to obtain agreement and ensure the device has been freely volunteered can be found in [Part 4](#) of this code.
50. Where the power is being exercised for the purposes of preventing, detecting, investigating, or prosecuting crime, this will commonly (but not exclusively) be a victim or a witness to a crime. Where the authorised person's organisational guidance and policies allow for it, the Act does not prohibit making a request to a suspect to volunteer a device and agree to the extraction of information from it. In most cases where the device user is a suspect it is likely that any device will be seized using other lawful powers, such as those under PACE, to prevent the loss or destruction of evidence and to ensure compliance with CPIA and disclosure principles. In all cases, it is for the authorised person to determine the appropriate power depending on the circumstances – not just when the person is a suspect.
51. If a device has multiple users, for example a shared laptop or tablet device, it is the responsibility of the authorised person to ensure that the person volunteering the device and agreeing to the extraction of information from it is a person who ordinarily uses the device.
52. 'Ordinarily uses' does not necessarily mean that this person was the original purchaser of the device or that they must own it outright. For example, a person may have a mobile phone or laptop that they regularly use which has been provided by their employer or other organisation. Where it is believed that the device contains relevant information for the purpose for which it is sought, the authorised person must take into account the fact that multiple people use the device when making their

³⁸ The only exceptions to this are where a user is a child, or an adult without capacity (in which case Section 38 applies) or where one of the conditions in Section 40 applies.

assessment of necessity, proportionality and the risk of obtaining other information, including confidential information.

53. If another user of that device objects to the extraction of information from it, it will be for the authorised person to consider the most appropriate course of action. In these circumstances, the authorised person must balance the rights and needs of both individuals against the necessity and proportionality of continuing with the information extraction.
54. The power in Section 37 may also be used for the purposes of helping to locate a missing person or to protect a child, or an at-risk adult from neglect or physical, mental, or emotional harm. An adult is at-risk if the authorised person reasonably believes that the adult is experiencing, or at risk of, neglect or physical, mental or emotional harm, and is unable to protect themselves against that neglect or harm (or risk of it)³⁹. Harm may also include financial abuse or coercive control. An authorised person does not need to obtain agreement in these cases but must satisfy relevant conditions in Section 40. This states the powers can be exercised when a person is missing and where that person was a user of the device immediately before they went missing. An authorised person will need to reasonably believe that the person's life is at risk or there is a risk of serious harm to the person in order to exercise these powers.
55. 'Immediately before they went missing' means that they were an active user of the device up until they were reported missing. For example, if during the search of a missing person's home two devices are found and one matches the description of the device the person reporting the missing person believes the individual uses, then it would be reasonable for the authorised person to believe this was the device being used "immediately before they went missing" and most likely to contain information relevant to helping to locate them.
56. Where a person is missing and it is believed that they are at risk of harm but there are no witnesses to help ascertain what device(s) they use, in the event that their home, vehicle or other significant location is searched, the authorised person should make an assessment of any devices found. The person sanctioning use of the powers should note the justification for the reasonable belief that any device was in use by the missing person at the time they went missing along with considerations required by the Act, such as the necessity, proportionality, and risk of obtaining other information etc.
57. Before exercising the Section 37 power to help locate a missing person, an authorised person should consult their own organisational guidance for missing person investigations and if necessary, seek guidance from a person who can sanction use of the powers to help determine what device information can be

³⁹ See part 5 Use of the Section 37 power with vulnerable people.

extracted from and to determine if the conditions for extracting information have been met.

Section 38: Voluntary provisions and agreement where a device user is a child or adult without capacity

58. A child⁴⁰ or adult without capacity is not able to voluntarily provide a device or agree to the extraction of information from it for the purposes of Section 37 of the Act.
59. An alternative individual will be responsible for making these decisions on behalf of the child or adult without capacity. In England, Wales, and Northern Ireland this means ensuring their best interests are considered in their decision or, for authorised persons operating in Scotland that they receive benefit from the intervention.
60. Detailed guidance on the use of these powers with children and adults without capacity, including who can act as an alternative individual to make decisions on behalf of a child or adult without capacity, is set out in [Part 6](#) of this code.

Section 40: Extracting information under Section 37 without voluntary provision or agreement: special cases

61. The following guidance only applies in cases where:
 - the device user has died, and they were a user of the device immediately before they died
 - the device user is a child or an adult without capacity and the authorised person reasonably believes that their life is at risk, or there is risk of serious harm to them
 - the device user is missing, they were a user of the device immediately before they went missing and the authorised person reasonably believes that their life is at risk or there is a risk of serious harm to them
62. In these cases, the authorised person may extract information from the device even though it has not been voluntarily provided and agreement to extract information from it has not been given. However, the other provisions of Section 37 still apply (e.g., the authorised person must still reasonably believe that information stored on the device is relevant to a purpose for which they may exercise the power).
63. For example, a police force may be attempting to locate a missing person who they believe to be at risk of serious harm. If, while attempting to locate the person, the police find or are given the missing person's device, they can exercise the Section 37 power to extract information from the device, without seeking agreement from the

⁴⁰ Section 37(13), Chapter 3 of Part 2 defines what is a child for the purposes of the Act.

device user or someone acting on their behalf. This applies even when the missing person is a child or an adult without capacity, where in other circumstances an alternative individual would be required to provide agreement to the extraction of information.

Section 41: Extracting information: investigations of death

64. In the case of Section 41 (extraction for the purposes of an investigation or inquest into a death), the authorised person may extract information from the device even though it has not been voluntarily provided and agreement to extract information from it has not been given. However, the other provisions of Section 41 still apply (e.g., the authorised person must still reasonably believe that information stored on the device is relevant to the investigation or inquest).

Section 41: the power and the purposes for which it may be exercised

65. The power in Section 41 may be used where a person who was a user of the device has died and, immediately before they died, they were a user of the device. The power may be exercised for the purposes of:
- 41(2)(a) an investigation into the person's death under the Coroners and Justice Act 2009 (England and Wales),
 - 41(2)(b) an inquest into the person's death under the Coroners Act (Northern Ireland) 1959 or,
 - 41(2)(c) an investigation into the person's death by the Lord Advocate (Scotland).
66. This includes determining whether such an investigation or inquest should take place.
67. This power is separate to any other power for the seizure of devices, such as those contained in the Coroners and Justice Act 2009. Authorised persons do not need to obtain agreement to exercise the power for this purpose, but must ensure that the requirements of necessity, proportionality, and assessment of risk of obtaining other information or confidential information have been met.
68. This is separate to the power in Section 37 which may also be used where a person has died if the purpose for obtaining information is for the detection, investigation or prosecution of a criminal offence related to their death.
69. 'Immediately before they died' means that they were the user of the device around the time of their death, but not necessarily that they were actively using it at the moment of their death. Although information about deceased people does not constitute personal data under data protection legislation, authorised persons must still consider

third party information contained in the electronic device when assessing necessity, proportionality and the risk of obtaining other information and confidential information.

Reasonable belief that the information on the device is relevant

70. The test as to what is ‘reasonable belief’ is an objective one. Any decision to extract information from a device should be made having considered all pertinent information available at the time, taking into account the provenance and the accuracy of the information available and based on more than mere suspicion or speculation on the part of the authorised person.

Relevant to a reasonable line of enquiry

71. An authorised person must only exercise the Section 37 power for the purposes of preventing, detecting, investigating, or prosecuting crime if they reasonably believe that information on the device is relevant to a reasonable line of enquiry and authorised persons are bound by the following, relevant guidance:

- **In England and Wales**, the code of practice made under Section 23 of the Criminal Procedure and Investigations Act 1996 (‘the CPIA’). This places a duty on investigators in England and Wales to pursue all reasonable lines of enquiry whether they point towards or away from the suspect.

72. As noted in the Attorney General’s Disclosure Guidelines 2022, “Investigators should ensure that all reasonable lines of inquiry are investigated, whether they point towards or away from the suspect. What is ‘reasonable’ will depend on the context of the case. A fair investigation does not mean an endless investigation. Investigators and disclosure officers must give thought to defining and articulating the limits of the scope of their investigations. When assessing what is reasonable, thought should be given to what is likely to be obtained as a result of the line of enquiry and how it can be obtained. An investigator may seek the advice of the prosecutor when considering which lines of inquiry should be pursued where appropriate”.⁴¹

- **In Scotland**, the Criminal Justice and Licensing (Scotland) Act 2010 applies. A statutory code of practice has been published under Section 164 of that Act.

The code of practice states, “An essential element of the duty of disclosure is the obligation on the police or other investigating agency to pursue all reasonable lines of enquiry, including any line of enquiry that might point away from the accused as the perpetrator of the offence. What constitutes a reasonable line of enquiry will be dependent upon the circumstances of each individual investigation”.

⁴¹ [AG Guidelines 2022 Revision Publication Copy.pdf \(publishing.service.gov.uk\)](#)

- **In Northern Ireland**, The Criminal Procedure and Investigations Act 1996 Code of Practice for Northern Ireland (Revised) 2005 applies.

Relevant to a purpose in the Act – Missing persons etc

73. In the case where the authorised person proposes to exercise the Section 37 power to help locate a missing person, or for the purposes of protecting a child, or an at-risk adult from neglect or physical, mental or emotional harm, the authorised person must reasonably believe that information stored on the device is relevant to that purpose.⁴²
74. Reasonable belief that information is relevant will be informed by the circumstances of the missing person investigation or why it is believed they are at risk of harm. This may include details such as their age, or concerns regarding their mental or physical health. Due to the vast amount of information contained on a device, such as a mobile phone, it is reasonable to assume that the device may contain information that is relevant. This may include:
- any indication that the person may commit suicide or self-harm,
 - any indication that the person has been groomed or is at risk of exploitation,
 - any unknown contacts who may know the current location of the missing person, or
 - any indication of where the missing person may have gone.
75. In all cases where the power is used to locate a missing person or protect a child, or an at-risk adult from harm, the authorised person must still consider if use of the power is necessary and proportionate and whether there are other means of obtaining the relevant information that are less intrusive than extracting it from their device.
76. In the case where the authorised person proposes to exercise the Section 41 power for the purposes of an investigation into the person's death under the Coroners and Justice Act 2009 (England and Wales), an inquest into the person's death under the Coroners Act (Northern Ireland) 1959, or an investigation into the person's death by the Lord Advocate (Scotland), or to determine whether such an investigation or inquest should take place, the authorised person must reasonably believe that information stored on the device is relevant to a purpose with Section 41(2) (a)-(c) of the Act.

⁴² Sections 37(5)(a-c) of the Act set out the conditions for the use of the Section 37 powers.

Necessity and proportionality

77. **Regardless of the purpose for which the powers are being considered, there must be no presumption that information will be extracted from a device.**
78. If less intrusive means of obtaining information are available, they must be considered, and used where reasonably practicable to ensure the extraction meets the test of strict necessity and proportionality.
79. Key considerations when deciding if the use of the powers is necessary and proportionate are the impact on the right to privacy of the device user and collateral intrusion on the right to privacy of third parties whose information may also be extracted. Before using these powers, authorised persons must consider whether there are other less intrusive ways of obtaining the required information that would avoid intruding on the right to privacy of the device user or that of any third party whose information may be visible.
80. Whilst each case must be carefully considered, it is highly unlikely that a full extraction from a device, such as a mobile phone, tablet, laptop or other computer and a review of all the content will meet the necessity and proportionality test in most cases. This is due to the volume of information that may be stored on such devices and the unlikely event that all such information will be relevant to a line of enquiry.
81. Sections 37(5)(c) and 41(4)(b) require that even when the authorised person reasonably believes that information stored on the device is relevant to a reasonable line of enquiry or purpose as above, they must also be satisfied that the use of the Section 37 or Section 41 power is necessary and proportionate to achieve the purpose.
82. In order for the exercise of either power to be necessary and proportionate, the authorised person will have to be satisfied that the information sought is required to achieve the relevant purpose, e.g., preventing crime, and that the purpose cannot be achieved by other less intrusive means. For the exercise of the power to be proportionate, they must consider if the purpose justifies the intrusion into the persons privacy, and that the amount of information obtained has been minimised. For example, it may be proportionate to extract specific information for serious crimes, such as murder or kidnap, but not for lower-level crime, such as anti-social behaviour or minor damage. Each case must be carefully considered on its own merit and there must be no presumption that information will be extracted from a device unless all of the conditions set out in Section 37 and Section 41 and the relevant data processing regimes are met.
83. In all cases the authorised person must carefully balance the need for the information against the interference with an individual's (or individuals') right to privacy and a defendant's absolute right to a fair trial.

84. Where it is determined that extraction is necessary and proportionate the authorised person must record their rationale for making the request in the written notice, which is to be provided to the device user. Further information on what else must be contained in this written notice and how it is to be shared with the device user can be viewed in the [Written notice](#) section of this code.
85. Whilst nothing in this code prevents the lawful application of alternative powers to obtain a device or extract information from it, it is not recommended that coercive powers are used to obtain devices containing personal or sensitive information from victims and witnesses, for example the powers of seizure under PACE⁴³. Obtaining information from a victim or witness device that contains sensitive or personal information other than by agreement should be rare.

Risk of obtaining other information

86. Section 37(6) and (7) and Section 41(5) and (6) require that an authorised person, exercising either power, must consider whether there is a risk of obtaining information other than that necessary for a purpose for which they may exercise the power. If this risk exists, for the use of either power to be proportionate, an authorised person must be satisfied that there are no other means of obtaining the information that avoid that risk, or if there are such means, it is not reasonably practicable to use them.
87. To be satisfied that there are no other means of obtaining the information, authorised persons should consider the type of information required and whether there are other methods available to obtain it. For example, communications providers may hold information about account holders to identify users of online accounts, email addresses or phone numbers. Extraction from a suspect's device should always be considered first. Where the requirement is to obtain a limited number of messages between a victim and a suspect, consider capturing images of the messages by taking screenshots.
88. The judgment in the Bater-James case specifically refers to the circumstances when it would be appropriate to use alternative methods to a 'digital download' and suggests that taking screenshots or making some other suitable record, may meet the needs of the case⁴⁴. Where alternative means of obtaining the information are identified, if these reduce the risk of obtaining other information, these should be used unless it is not reasonably practical to do so. The test of what is reasonably practical is objective. The authorised person must assess whether it would be reasonably practicable to use the other means in the circumstances. The exception of what is not reasonably practicable is intended to ensure that in certain cases, for example where there is a

⁴³ The Police and Criminal Evidence Act 1984 or The Police and Criminal Evidence (Northern Ireland) Order 1989.

⁴⁴ See the judgement R V Bater-James and Mohammed [2020] EWCA Crim 970 and annex B of this Code

time critical need for the information to protect life or prevent harm, that authorised persons are able to seek agreement rather than apply for a court order or other delay. Where alternative methods are used to obtain the information, the relevant evidential requirements of that jurisdiction will still need to be met. Delay alone would not provide sufficient justification not to pursue an alternative method unless there was a real and immediate risk of harm. In all cases, extracting information from a device (other than a suspect's device) should be the last resort and only considered when other less intrusive methods to obtain the sought information have been exhausted or not deemed reasonably practicable to pursue.

89. Other information might include:

- personal information on the device that is about the user but not necessary for the purpose, such as photos, content of messages or details of their contacts
- information on the device that is about a third party and not necessary for the purpose – for example, photos sent to the device user taken by someone else, content of messages, or contact information such as email addresses and phone numbers

90. If, after considering necessity and proportionality (including the risk of obtaining other information), the authorised person is satisfied that use of one of these powers is justified, they can proceed, but should minimise the risk of obtaining other information as far as is practically possible. This should include use of appropriate technologies to support selective extraction and use of targeted key words, date ranges or other specifics to identify necessary information. Technological capabilities are improving at pace and authorised persons should be aware of, and keep up to date with, the technology options available in their organisations and ensure they use those that offer the most selective extraction of information.

Confidential information

91. The following paragraphs give guidance on the exercise of the powers in Section 37 and Section 41 of the Act in relation to confidential information. This includes what confidential information is, how authorised persons should consider the risk of obtaining confidential information, and how they should proceed if they think there is a risk of obtaining confidential information.

92. Confidential information is defined in Section 43 of the Act. Confidential information refers to the following:

- 'Confidential journalistic material' - as defined in the Investigatory Powers Act 2016⁴⁵. That is material created or acquired for the purposes of journalism which is

⁴⁵ Part 2, Chapter 1, paragraph 28 [Investigatory Powers Act 2016 \(legislation.gov.uk\)](https://www.legislation.gov.uk)

held in confidence (or which, in the case of material in a communication, the sender holds in confidence or intends the recipient to hold in confidence).

- 'Protected material' - as defined in defined in Section 43(2) of the Act, which includes:
 - i. Certain communications between a professional legal adviser and their client (or between such a person and others).
 - ii. Personal records and other material acquired or created during the course of a trade, business, profession or occupation (or for the purposes of any office) which are held in confidence.
93. These powers **must not** be used where the intention is to extract confidential information. If the authorised person is seeking confidential information on the device that is relevant to the investigation, a different power such as, in England and Wales, the Criminal Justice and Police Act 2001, must be used to obtain it. Authorised persons should consult local policy on the appropriate lawful power where confidential or protected information is sought.
94. If the authorised person believes there may be confidential information on the device but is not seeking it, then the following sections apply.
95. If a person indicates that there is confidential information on their device the authorised person should determine if it is likely to be relevant to the line of enquiry.
96. In no circumstances should an authorised person ask a device user to waive their right to confidentiality for the purposes of obtaining confidential information. If a device user expresses their wish to do so, the authorised person should advise that this decision is only taken after the device user has received legal advice.
97. Authorised persons should familiarise themselves with organisational and national guidance and policies regarding digital material, confidential information and protected material, in addition to this code of practice⁴⁶.

Assessing whether there is a risk of obtaining confidential information

98. In every case where an authorised person is considering using the Section 37 or Section 41 power, they must assess whether there is a risk of obtaining confidential information. Due to the vast amount of material held on some devices, such as smartphones, it is reasonable to assume that many people are likely to have some information on the device that could be considered "confidential information" for the purposes of the Act. In some cases, the confidential information may not be relevant to the case, for example, where a victim of a sexual assault has correspondence on their device with a solicitor relating to the sale of a property. However, in other cases,

⁴⁶ For example, [Attorney General's Guidelines on Disclosure - GOV.UK \(www.gov.uk\)](http://www.gov.uk)

it is possible that a device will contain confidential information which is of potential relevance to the investigation by the authorised person, for example, correspondence between the device user and a legal professional regarding a criminal allegation made by the victim which the police are investigating.

99. Authorised persons should use their professional judgement to assess whether there is a risk of obtaining confidential information. In some cases, the device user may not know whether they have confidential information on their device but an authorised person should consider asking every person providing agreement whether there is likely to be confidential information on their device.
100. Where the device user is a lawyer or journalist and the device to be examined is used for their work, it may be reasonable to assume that their device will contain a high volume of the confidential information. In this scenario, it is strongly advised that the authorised person should ask them whether confidential information is stored on their device.
101. Authorised persons should use the facts of the case, and information from the device user to make an informed judgement about whether there is a risk of obtaining confidential information.
102. The authorised person should record their risk assessment and their decision on how they will proceed.

How to proceed after assessing whether there is a risk of obtaining confidential information

103. If the authorised person does not think there is a risk of obtaining confidential information, they may proceed with use of these powers (subject to the other requirements of the Act and this code being satisfied).
104. In the event the authorised person thinks there is a risk of obtaining confidential information, they must consider all of the following:
 - (a) the type of confidential information likely to be stored on the device
 - (b) the amount of confidential information likely to be stored on the device
 - (c) the potential relevance of that information to the purpose(s) for which they may extract information
 - (d) whether there are other means of obtaining the information sought which do not risk obtaining confidential information and be satisfied that (i) there are not, or (ii) if there are, it is not reasonably practicable to use them

105. The exercise of the Section 37 or Section 41 power will only be proportionate if the authorised person has considered the matters at (a), (b) and (c) above and satisfied themselves as per (d) above.
106. Authorised persons must consider the type of confidential information that is likely to be stored on the device and whether there are additional restrictions or considerations on handling that type of information.
107. If the amount of confidential information being extracted is likely to be minimal, and the information is likely to be irrelevant to the case, the authorised person can proceed with the extraction. In all cases where selective extraction technology is available it must be used to minimise the risk of obtaining any irrelevant information including confidential information.
108. If there is likely to be such a high volume of confidential information on the device that it will almost certainly be obtained during an extraction, the authorised person should consider using a different power if the circumstances of the purpose allow. If there is likely to be confidential information on the device and it is likely to be relevant to the case, then the authorised person must use another power to obtain it.

What to do if confidential information is unintentionally obtained

109. There may be occasions when confidential information is unintentionally obtained and reviewed during an extraction. Depending on what the information is, the authorised person should proceed as follows:
- if the confidential information accidentally obtained is irrelevant to the case, it must be deleted or redacted as soon as is practically possible.
 - If the confidential information is relevant to the case, the authorised person should initially consult other available guidance regarding what to do in this scenario. For example, for some types of confidential information, it may be necessary to send all the extracted material for review by a lawyer independent from the public authority.
110. In all cases where it is known that confidential information has been obtained from the device without the device user's knowledge, the authorised person should inform them at the earliest opportunity of what has been extracted and the actions that have been taken to protect their information, unless there is a lawful basis not to do so.

Sanctioning use of the powers

111. All authorities who use these powers should have a procedure that clearly states who should sanction the use of the powers and the process they should follow.

112. This procedure should include information about:

- the grade or rank of the individual who should sanction any use of the powers ('the Sanctioning Officer')
- the documentation that the Sanctioning Officer should complete in order to allow extraction, including the record of how the request meets the requirements for use of the power set out in Section 37 and 41
- the procedure that the Sanctioning Officer should follow in the case of an urgent oral authorisation to use the powers

113. The Sanctioning Officer should be at least one grade or rank higher than that of the individual requesting the extraction, but some agencies may dictate a specific grade or rank. All authorised persons should refer to their own organisational guidance on the rank of the Sanctioning Officer.

114. The Sanctioning Officer should refer to the Equality Impact Assessment for the Act when deciding the appropriate course of action.⁴⁷

115. An urgent oral authorisation may be given by a person at least one grade or rank above the person seeking the authorisation where there is a real and immediate risk of serious harm to a person and the requirements for use of the power in Section 37 are met. The person sanctioning the power should make a written record of their authority and the reason for it at the earliest opportunity.

116. Urgent authority refers only to the internal process of authorising use of the powers. Regardless of the urgency of a case, if voluntary provision and agreement is needed i.e., for the prevention etc of crime, then all obligations of Section 37 and Section 39 must be met.

117. The authorisation should be limited to the extraction of the specific information required for the purposes of which it is sought or to address the reasonable line of enquiry.

Recording the use of these powers

118. Authorised persons should record in writing their rationale for their decisions to use these powers, to include the points noted above – the relevant information sought, why the use of these powers is necessary and proportionate, what alternative options for obtaining the information have been considered and, if any were identified, why it was not reasonably practicable to use them.

⁴⁷ [Home Office measures in the Police, Crime, Sentencing and Courts Bill: Equalities Impact Assessment - GOV.UK](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/674212/Home_Office_measures_in_the_Police_Crime_Sentencing_and_Courts_Bill_Equalities_Impact_Assessment_-_GOV.UK)

119. Part 4 of the code provides more detail on the requirements for the recording of information.

Extracting Information

120. Extraction may only be carried out by persons who are appropriately trained in any extraction technique they are applying. In England and Wales extraction should be carried out in accordance with the quality standards set out in the Forensic Science Regulator's Code of Practice and any additional guidance issued by the Regulator. In Scotland and Northern Ireland extraction can be carried out in accordance with the quality standards set out in the Forensic Science Regulator's Code of Practice and additional guidance issued by the relevant authority in those countries. This includes the achievement of accreditation where this is required by the Code or guidance document. The relevant authorities are:

- In **England and Wales** –Forensic Science Regulator's Code of Practice.⁴⁸
- In **Scotland** - Scottish Police Authority Forensic Services.⁴⁹
- In **Northern Ireland** –Forensic Science Northern Ireland.⁵⁰

121. It may, in certain circumstances, be possible for the authorised person to carry out the extraction in the presence of the device user for them to view the extraction process. If the device user has requested this, it is recommended that this is facilitated unless it is impracticable or inappropriate to do so.

122. Authorised persons must ensure that the extraction is properly authorised before they commence, and where the powers in Section 37 have been used for the purpose of prevention, detection etc of crime, that they have the appropriate written agreement detailing the information sought.

123. In every case, the authorised person must consider the power used to obtain the device and the power used to extract the information. Where personal information is extracted and processed, the authorised person must also meet the requirements of data protection legislation.⁵¹ Information extracted should not exceed what is relevant and the speed of extraction should not be prioritised over the ability to carry out selective extraction.

⁴⁸ [Forensic Science Regulator - GOV.UK \(www.gov.uk\)](http://www.gov.uk)

⁴⁹ [Forensic Services for Policing - Scottish Police Authority \(spa.police.uk\)](http://spa.police.uk)

⁵⁰ [About Forensic Science Northern Ireland | Department of Justice \(justice-ni.gov.uk\)](http://justice-ni.gov.uk)

⁵¹ [Data Protection Act 2018](#)

124. These powers do not allow for obtaining information that is held off the device, sometimes referred to as information held in the ‘cloud’⁵².
125. The Section 37 and 41 powers allow an authorised person to extract information stored on an electronic device when the conditions are met. As detailed in [Part 3](#) of this code (proportionality and the risk of obtaining other information), an authorised person must consider the risk of obtaining other information and should choose the most selective extraction method available to minimise the risk of obtaining other or excessive information.
126. For the purposes of these powers, the term ‘extraction’ includes the reproduction of digital information or data from a device in any form⁵³. This includes taking screenshots by any method but does not restrict the ability of authorised persons to receive copies of digital information, such as a screenshot taken by the device user and shared with the authorised person in another way such as being attached to an email.
127. In all cases it will be for the authorised person to decide on the lawful basis to extract the information required. In the case of obtaining screenshot or screen capture information, the authorised person must carefully consider whether the use of these, or another power, is required to obtain the screenshot. Where the image it contains ‘personal data’ as defined in the Data Protection Act 2018⁵⁴, they will also need to meet the requirements of the Act to process the information. Authorised persons should refer to their own organisational guidance on capturing screenshot information, which may include a requirement for the copies to be certified⁵⁵.
128. Information includes moving or still images and sounds⁵⁶, text messages or documents which are stored on the device, as well as other data such as file directories and location information.

Applicable devices

129. For the purposes of these powers, ‘electronic device’ means any device on which information is capable of being stored electronically and includes any component of such a device⁵⁷. Whilst the primary purpose of the powers is to enable the authorised person to obtain relevant information from personal electronic devices, which will most frequently be mobile phones, tablets and laptops, the definition is deliberately

⁵² The ‘cloud’ is sometimes referred to as the system of remote data storage or sharing of data through a computer or telecommunications network.

⁵³ Section 37(14)

⁵⁴ [Data Protection Act 2018 \(legislation.gov.uk\)](#)

⁵⁵ For example, this includes Criminal Justice Act 2003 and Criminal Procedure (Scotland) Act 1995

⁵⁶ Section 37(13).

⁵⁷ Section 37(13).

broad so that the powers may be used to lawfully obtain information from any device or item that stores information electronically where the Section 37 or Section 41 conditions are met.

CCTV

130. The Section 37 and 41 powers may be used to obtain any form of digital or electronic information, including CCTV material where the information is stored locally on a device.
131. It may be more appropriate to use alternative powers to obtain and process CCTV material. The often-speculative nature of CCTV enquiries may make it difficult to meet the requirements of the Section 37 or 41 powers. This is because without reviewing it, the authorised person may be unable to demonstrate that they reasonably believe that information stored on the CCTV system is relevant to a reasonable line of enquiry or relevant to the purpose for which it is sought. Authorised persons should refer to their own organisational and national guidance for obtaining and managing CCTV material⁵⁸.

Type of extraction

132. Technical capabilities may vary between authorised persons. It is for the authorised person and forensic practitioner (if used) to determine the most appropriate method of extraction to obtain the required information that limits the extraction of other information, bearing in mind the technical capabilities available. Some technology will facilitate targeted extraction, others may require the recovery of a larger data set to obtain the information required.
133. In all cases, authorised persons must ensure information extraction is not excessive, minimising intrusion into the device user's privacy and the privacy of others.
134. In some cases, it may be necessary to extract a larger subset of information to understand the context of it. For example, viewing the conversation immediately before and after a relevant comment.
135. Authorised persons should make every effort to limit the time that a device user is left without their device. The loss of the device may be distressing, this is particularly true of vulnerable victims who will rely on it to communicate with their support network. The loss of the device for any significant length of time will adversely affect all device users who rely upon it as their main means of communication or to organise their day-to-day living.

⁵⁸ Examples of national guidance: Information Commissioner's Office (ICO), Update to Surveillance Camera Code of Practice - GOV.UK (www.gov.uk)

136. Where the Section 37 power is used, the device user, or person providing agreement if different, should be offered an opportunity to be present when the extraction takes place. The exceptions to this are where the authorised persons consider it impractical or inappropriate to do so, or where there are technical limitations that do not allow it.
137. Authorised persons in England and Wales can find advice and information about examination of digital media device in CPS Guidance which has been endorsed by the court of appeal.⁵⁹ Authorised persons in Scotland can find guidance in the Crown Office and Procurator Fiscal Service Disclosure Manual. Authorised persons in Northern Ireland should refer to the Public Protection Service Code for Prosecutors.

Retention and deletion of extracted information

138. Information which is extracted and deemed not relevant must be deleted unless there is a lawful basis to retain it. Any decisions regarding the retention or deletion of information should be considered in line with relevant disclosure guidelines⁶⁰.
139. Where excessive or other information has been obtained because it has not been possible to restrict the extraction to the relevant material due to technological reasons, or following review, information obtained is no longer deemed relevant, unless there is a lawful basis to retain it, it must be deleted.
140. When considering whether to retain or delete extracted information, authorised persons must comply with relevant disclosure requirements, other legislative requirements, for example the Data protection Act 2018, and their own organisational information management guidance.⁶¹

⁵⁹ CPS Guidance on 'Reasonable lines of Enquiry and Communications Evidence and 'Disclosure – Guidance on Communications Evidence', endorsed in the case of R v E [2018] EWCA 2426 (Crim)

⁶⁰ For England and Wales: [Attorney General's Guidelines on Disclosure - GOV.UK](#), for Northern Ireland: the Public Prosecution Service Code for Prosecutors' and for Scotland: the COPFS Disclosure Manual - Page 3 (copfs.gov.uk)

⁶¹ For example, the NPCC Management of Physical and Digital Retention Guidance 2021, The College of Policing APP [Management of Police Information](#), [CPIA Code of Practice](#), [Data Protection Act 2018](#), Criminal Justice and Licensing (Scotland) Act 2010, For England and Wales: [Attorney General's Guidelines on Disclosure - GOV.UK](#), for Northern Ireland: the Public Prosecution Service Code for Prosecutors' and for Scotland: the COPFS Disclosure Manual - Page 3 (copfs.gov.uk)

Part 4: Voluntary provision of device and agreement to extract information

Requirements for voluntary provision and agreement

141. Section 39 of the Act sets out the requirements which must be met in order for a person to be treated as having voluntarily provided a device and agreed to the extraction of information from it in (for the purposes of Section 37 or 38).

142. This part of the code includes guidance on:

- the criteria that must be met for a person to be treated as having voluntarily provided an electronic device, and agreed to the extraction of information from it
- the difference between voluntarily providing the device and providing agreement to extract information from it
- what agreement means
- how to obtain agreement
- how to ensure agreement is freely given without the application of undue pressure
- details of the written notice including what it should contain and how it should be explained to the device user
- recording confirmation of the voluntary provision and agreement to the extraction of information
- the right of an individual to refuse to provide a device or agree to the extraction of information from it what to do when a new reasonable line of enquiry is identified after the initial extraction process takes place
- what to do in circumstances where the device user is not capable of voluntarily providing the device or agreeing to the extraction of information from it (if they are a child or an adult without capacity)
- what to do when the device user is unable to provide confirmation of voluntary provision and agreement in writing because of a physical impairment or lack of literacy skills

Voluntary provision, agreement and undue pressure

143. Where the use of the Section 37 power requires a device user, or their representative (in the case of child or adult without capacity), to volunteer the device and agree to

the information extraction, this agreement must be provided in the form of a written notice before the extraction is commenced. If agreement cannot be provided in writing because of the person's physical impairment or lack of literacy skills, then agreement may be given orally. In this instance the device user should be asked whether they wish to have another person present, such as a family member or friend, to ensure the oral discussion accurately reflects what is in the written notice. The authorised person must record the agreement in writing.

144. The individual must have made a fully informed and conscious decision to volunteer the device and have freely given their agreement to the extraction of information from it.
145. The individual must not have had any undue pressure placed on them or been coerced by anyone (including an authorised person) to provide the device or agree to the extraction of information from it.
146. 'Undue pressure' means making the person feel as though they do not have a choice about volunteering the device and agreeing to extraction. For example, if they are made to feel that an investigation will be discontinued prematurely, or other reasonable lines of enquiry not followed if they do not agree to extraction. There may be cases where the information on the device is the only remaining reasonable line of enquiry, this should be clearly explained to the individual. It is recognised that in some circumstances the very act of making a request for a device and the extraction of information from it, may make the victim or witness feel a degree of pressure. The authorised person should take this into account when communicating the reason for the request.

Written notice

147. In order to ensure that a device has been volunteered and agreement obtained, the authorised person must provide the device user, or if different, the person providing agreement, with a written notice (in hard copy or electronic form), specifying:
 - a. the information that is sought
 - b. the reason why the information is sought, for example how it may answer a reasonable line of enquiry, and how this meets the necessity and proportionately requirements
 - c. how the information will be dealt with once it has been extracted, for example who it will be shared with and how long it may be retained for
 - d. that the person may refuse to provide the device or agree to the extraction of information from it

e. and that the enquiry will not be brought to end merely because of this refusal.⁶²

148. In addition, authorised persons should include the following additional information in the written notice that will aid the person providing agreement and provide reassurance about the process and their rights:

- that the person may withdraw their agreement any point before the extraction takes place, but where the extraction has already taken place, the requirements of disclosure may mean that some of the information obtained with their agreement may be disclosed to the CPS or the defence where it is relevant
- how long the device user is expected to be without their device
- if an additional extraction is required, what action will be taken to obtain further agreement
- the other, less intrusive methods, the authorised person has considered to obtain this information and if any were identified, why they have not been followed
- of how any collateral information obtained will be managed
- how to challenge a request, both at the point it is made, and at a later date.

149. The information contained in the written notice to seek agreement should be carefully explained to the individual to ensure they have understood it. Where there is any doubt as to their understanding, additional support should be provided to the device user to assist their decision making.⁶³

150. Police forces in England and Wales are expected to use the approved NPCC Digital Processing Notices (DPN) for the written notice and agreement⁶⁴. A copy of this can be found in [Annex D](#) of this code. Other authorities are encouraged to use the DPN but may decide to use a form of their own devising so long as it meets the requirements of the Act. In all cases there must be a clear and obvious link between the information that is required to be provided to a device user in writing and the signed agreement. It must be explicitly clear as to what information they have agreed can be extracted and for what purpose. Authorised persons should consider periodically reviewing their written notice to ensure it remains fit for purpose.

⁶² Section 39(3)(a-e) of the Act

⁶³ See Part 5: Use of the Section 37 power with vulnerable people for more information on providing support

⁶⁴ For the NPCC DPN forms: [NPCC internet page containing the latest DPN documents](#)

Confirmation of voluntary provision and agreement

151. Before extraction can take place, the authorised person must obtain confirmation in writing through the written notice⁶⁵ that the device has been volunteered and there is agreement as to what information can be extracted from it. The authorised person must then give the person a copy of the agreement.
152. If it is not possible to obtain written agreement because of physical impairment or a lack of literacy skills of the device user or the person providing agreement, then oral confirmation may be obtained. Any request to obtain oral agreement should be agreed by the Sanctioning Officer and the reasons for it recorded. There should be no automatic assumption that a person is incapable of providing written agreement. The authorised person must record the verbal confirmation and provide the person with a written notice containing all the required information for future reference.
153. In all cases, the authorised person must consider the individuals needs and vulnerabilities⁶⁶ and take the action necessary to provide them the support needed to understand what it is they are being asked to agree to and why. The device user may be supported by a number of different professionals during this process, for example, a language interpreter, an intermediary, an Independent Domestic Violence Advisor (IDVA), or an Independent Sexual Violence Advisor.
154. Under no circumstances must agreement be sought without providing the device user or the person providing agreement (where different) with the required information in writing.
155. A record of confirmation must be kept, even if confirmation was provided verbally,⁶⁷ as it may be requested at a later stage to show that the device was provided voluntarily with agreement.
156. If an additional line or lines of enquiry are identified that are beyond the scope of what has been agreed with the device user, or the person providing agreement on their behalf, the authorised person will need to consider the obligations of the Act again. Provided that these obligations are met, the authorised person should provide the device user with a new written notice and seek voluntary provision and agreement again.
157. Further guidance about obtaining the views of those other than the person providing agreement, such as where the device user is a child, or adult without capacity, are explained in [Part 5](#) of this code.

⁶⁵ For example, the NPCC DPN

⁶⁶ See Section 5 Use of the Section 37 with vulnerable people for more information

⁶⁷ Section 39(5) of the Act

Withdrawal of agreement

158. The device user, or the person who has voluntarily provided the device and agreed to the extraction of information from it in accordance with Section 38, has the right to withdraw their agreement for information to be extracted from the device. It is that individual's decision to give the authorised person the device and to agree to the extraction of information from it, and they can change their mind. In the case of a device that is used by multiple users, only the person who voluntarily provided the device and agreed to the extraction of information from it can withdraw that agreement.
159. It should be made clear that withdrawal of agreement will mean that the device is returned, if the extraction has not already taken place, then the information will not be taken from the device. However, if agreement is withdrawn after the extraction of information has taken place, it may not be possible to delete or return it. This is because of the duties on investigating agencies and prosecution services to disclose information to the defence. In all cases, however, the extracted information and the device must only be retained where there is a lawful basis to do so and as long as necessary in line with each authority's data retention policies and other relevant guidance.
160. This is important to help the individual make an informed decision on what to do, especially as they may be allowing the authorised person to access a significant amount of personal information. Information about rights to withdraw agreement should be included in your organisation's version of a Data Processing Notice (DPN) as appropriate.

Part 5: Use of the Section 37 power with vulnerable people

Vulnerable people / victims of crime

161. The purpose of this part is to offer guidance on what authorised persons should carefully consider when using the Section 37 power in cases where the device user is vulnerable.

162. In this part, we will focus on vulnerable victims of crime, who may have experienced trauma and who may need more support to make an informed decision as to whether to voluntarily provide their device and agree to the extraction of information from it. However, in all cases where an authorised person is considering exercising the Section 37 power, they should consider if a person is vulnerable and whether they may need more support to decide whether to voluntarily provide their device and agree to the extraction of information from it.

163. By way of example, the Victims Code⁶⁸ for England and Wales⁶⁹ defines a victim as:

- a person who has suffered harm, including physical, mental or emotional harm or economic loss, which was directly caused by a criminal offence
- a close relative (or a nominated family spokesperson) of a person whose death was directly caused by a criminal offence

164. Children and adults without capacity, although vulnerable, cannot voluntarily provide their device or agree to the extraction of information from it for the purposes of Section 37. Where the user is a child or adult without capacity, authorised persons should follow the guidance set out in Part 6: Section 38: Children and adults without capacity.

165. All authorised persons should be aware of their existing responsibilities to protect the rights of victims. You can find guidance on these responsibilities in -

- [The code of practice for victims of crime in England and Wales](#)
- [The Victims' Code for Scotland](#)
- [The Victim Charter, A charter for victims of crime - Northern Ireland](#)

⁶⁸ [Code of Practice for Victims of Crime in England and Wales \(Victim's Code\) - GOV.UK](#)

⁶⁹ See also the Victims' Code for Scotland and in relation to Northern Ireland, the Victims' Charter is relevant.

What does ‘vulnerable’ mean?

166. There is no single legal definition of ‘vulnerable’. For the purposes of the Section 37 power, an individual can be considered vulnerable if they require some level of additional support to make an informed decision to provide their device and agree to the extraction of information from it.
167. Authorised persons should be aware that someone may try to hide their vulnerability. There are many reasons for this such as fear, shame, past experiences of engaging with the police or other agencies⁷⁰ or because they do not view themselves as vulnerable. Authorised persons should consider if a person may be vulnerable in every case when determining if appropriate to use the Section 37 power.
168. The College of Policing have said that “a person is vulnerable if as a result of their situation or circumstances, they are unable to take care of or protect themselves, or others, from harm or exploitation”.⁷¹
169. In addition, authorised people should consider if a person is vulnerable due a protected characteristic such as race or disability where minority status may result in someone feeling less able to engage with the police or other law enforcement authority.
170. Many victims and witnesses experience stress and fear during the investigation of a crime. Stress can affect the quantity and the quality of the communication with, and by, the individual concerned. The authorised person should be mindful of hidden vulnerabilities caused through disability, shock or trauma.
171. Where an individual is deemed vulnerable, authorised persons should make them aware that they can have additional support to help make an informed decision as to whether they will voluntarily provide their device and agree to the extraction of information from it. The authorised person should take all reasonable steps to ensure that this support is accessible. The support may come from a range of persons or specialist support services – for example, from a family member, a friend or, in a case of a sexual offence, an Independent Sexual Violence Advisor⁷² or other rape advocacy worker, where the service is available. In Scotland, victims and witnesses may also receive support from an Appropriate Adult⁷³ whose role is to facilitate communication for vulnerable adults during criminal investigations. In Northern Ireland, children may also receive support from an Independent Guardian.

⁷⁰ [Vulnerability-related risks | College of Policing](#)

⁷¹ From the College of Policing (for England, Wales) training ‘Vulnerability-Look Beyond the Obvious’.

⁷² [The role of the Independent Sexual Violence Adviser \(ISVA\) - GOV.UK \(www.gov.uk\)](#)

⁷³ [Appropriate Adults: guidance for local authorities - gov.scot \(www.gov.scot\)](#)

172. Where a victim is from a minority community, they should be offered to be referred to a specialist organisation run by or for that minority community, where the service or support is available.
173. Where the person does not speak English, the services of an interpreter must be provided. Where a person is deaf, it may be necessary to obtain the services of a British sign languages (BSL) interpreter if there is no other support available at the time. If there is any doubt as to whether the support available can facilitate communication to the required standard, a BSL interpreter must be provided.
174. The following list can be used as guidance for determining if a person may be vulnerable and whether they require additional, independent support to make a fully informed decision as to whether to voluntarily provide their device and agree to the extraction of information from it. This is not an exhaustive list. The needs of the individual must be carefully considered on a case-by-case basis, taking into account both the nature of the investigation and their involvement in it. If you are unsure whether a person is vulnerable, it may be appropriate to assume that a level of vulnerability exists, particularly for victims of sexual offences or in a case where someone has been physically or mentally harmed.
175. Authorised persons should recognise that an individual may have several different vulnerabilities and in their approach to engagement consider how the vulnerabilities overlap and interact to provide the correct support. For example, the approach to someone who is vulnerable to trauma who fears repercussions, will be different to someone who is vulnerable due to trauma who has learning difficulties.
176. Examples of people who may be vulnerable:
- someone who has been the victim of a traumatic crime, such as rape or sexual assault or another type of violent crime
 - someone who has been the victim of domestic abuse
 - someone who has been the victim of stalking
 - someone who has been the victim of people trafficking
 - someone who is an asylum seeker or undocumented person
 - someone who fears repercussions from working with an authorised person to further an investigation – for example, a whistle-blower
 - someone who is suffering from fear or distress
 - someone who is suffering from a mental disorder
 - someone who has difficulty with social functioning
 - someone with a physical disability
 - someone on the autistic spectrum
 - someone with learning difficulties
 - someone who has difficulty in understanding what is being communicated to them (including language barriers)
 - someone who has difficulty reading or writing

177. Authorised persons must follow any existing legislation and local guidance regarding vulnerable people as appropriate to the specific case, in addition to this code of practice.

Voluntary provision and agreement and vulnerable people

178. Victims of crimes such as rape and other sexual offences may be particularly concerned about agreeing to share information. The possibility that they may be asked to hand over personal and sensitive information has been found to be a principal reason why victims of rape may withdraw from the criminal investigation process or may choose not to report the crime at all.

179. Detailed guidance on what information to give to individuals to ensure that they are able to voluntarily provide their device and provide free and unambiguous agreement to the extraction of information from it can be found in Part 4: Voluntary provision of device and agreement to extract.

180. An authorised person may need to go further to support and appropriately account for the needs of a vulnerable person/victim when exercising this power. For example, where an individual is in shock, such that they are unable to comprehend what is being asked of them in terms of providing their device and agreeing to the extraction of information from it, the authorised person may need to wait until such a time that the shock or effects of it have receded sufficiently for the person to decide. The powers and processes for an adult without capacity are intended primarily for use where an adult has a long-term lack of capacity due to disability and not for cases of fluctuating capacity where someone who would ordinarily be able to make decision for themselves is temporarily unable to do so.

181. Trauma can impact decision making, so it is important that authorised persons familiarise themselves with their organisational guidance on how to recognise and support and engage with witnesses and victims who are suffering from trauma.

182. The authorised person should consider whether to seek the support of an independent advisor for the vulnerable person, for example, an Independent Guardian, an Independent Sexual Violence Advisor (ISVA), an Independent Domestic Violence Advisor (IDVA), a learning disability advocate or an Independent Mental Health Advisor (IMHA) where available to support to the individual. In all cases the authorised person should ensure that it is a person and role that the person trusts. A family friend will not be able to offer the same level of support as a professional independent advisor and these should be sought first.

183. **In Scotland**, the authorised person should request Appropriate Adult support for victims and witnesses who are unable to understand proceedings or communicate effectively because of a mental disorder.

184. Although an individual may seek support on the decision to volunteer their device and agree to the extraction of information from it, the decision must be theirs. Only in cases where the device user is a child or an adult without capacity can (indeed, must) another person make those decisions.
185. Wherever it is possible to do so, the authorised person should ensure the individual has sufficient time to make these decisions.
186. If, because of their vulnerability, the individual cannot understand the DPN, the authorised person must offer the device user the option of having the person providing independent support (a person referred to in paragraph 183 above) read the DPN out loud to the individual if they are unable to read or comprehend the material on their own and explain it to them in simple terms. If the person providing support is unavailable to do so, then the authorised person may need to explain the contents of the form and read it out loud to the device user.
187. If language is an additional barrier to understanding what is being asked of the individual, an interpreter should be made available. If the device user has someone providing independent support, they may be able to assist with this.
188. In all cases when dealing with a vulnerable victim, the utmost sensitivity and support should be exercised to ensure that the vulnerable victim understands what is being asked of them and to ensure that their trauma is not further exacerbated because of engaging in an investigative process.
189. If you are unsure about the level of support a person requires you should consult a supervisor or review appropriate guidance in your organisation.

Privacy impact and vulnerable people/victims

190. It is highly likely that a person's electronic device will contain sensitive personal information about them or other persons, and authorised persons must consider the individual's Article 8 right to respect for private life before any sensitive information is extracted (see [Part 2](#) of this code). Authorised persons should act in the knowledge that agreeing to the extraction of this kind of information will be an incredibly difficult experience for all device users and particularly where the person is vulnerable. Victims of rape and sexual offences may be less willing to proceed with the criminal investigation process if they are concerned about having to share sensitive information.
191. In all cases, before exercising the Section 37 power an authorised person must consider other methods for obtaining the required information that do not have the same level of intrusion. This is particularly important when there might be an acute privacy impact on a vulnerable victim.

Safeguarding and vulnerable victims

192. When exercising the power in Section 37 in relation to a vulnerable victim, there are certain measures that should be taken to ensure they are adequately safeguarded. The following paragraphs give examples.
193. There may be cases when a vulnerable victim is involved in an activity where they are a victim, but do not see themselves as such – for example, if they have been sexually abused, groomed or are the victim of domestic abuse, but believe they are in a consenting relationship with their abuser. In cases such as these, the authorised person will need to work carefully with the vulnerable victim and any support representative (such as an independent guardian, an Independent Sexual Violence Advisor (ISVA) or an Independent Domestic Violence Advisor (IDVA) to decide on the right course of action. In cases where the only option is to examine a device belonging to someone who does not believe they are a victim; it may be necessary to use a different power to obtain the device that does not rely on the individual's agreement. Any use of an alternative power in these circumstances should be carefully considered and must only be used in the case of a victim as a last resort.
194. Engaging in an investigation can be an especially traumatic experience for vulnerable victims. To account for this, authorised persons should make appropriate adjustments and consider the needs of the victim and where they will be most comfortable and able to make the best decisions for themselves. Being in a police station may be intimidating, but equally it may be the case that they don't want the police to attend their home address for many different reasons. In every case the individual's needs must be carefully considered.
195. In all cases, where a person has provided agreement to extract information authorised persons should aim to return a device as quickly as possible. In the case of a rape victim, the device should ideally be returned within 24 hours of the being taken. This 24-hour period starts at the point the device is physically transferred to the authority for the extraction⁷⁴.
196. For vulnerable victims, it is especially important that their device receives priority examination so that it can be returned to them as soon as possible. If it is possible to prioritise the examination of a vulnerable victim's device or allow the individual to make an appointment to have their device examined, thus ensuring they retain possession of it until it is ready to be processed, an authorised person should do so.
197. In the case where a rape victim's electronic device is taken for examination and it is not possible to return it within 24 hours, they should be provided with a replacement device or support in obtaining one.

⁷⁴ Authorised persons should also refer to their own process guidance, for example, the College of Policing APP for the extraction of material from digital devices

198. For vulnerable people who are not rape victims and where it may take longer than 24 hours to examine their device and return it to them, authorised persons should consult local safeguarding guidelines and provide a replacement device as appropriate according to their organisation's best practice.
199. All individuals may be eligible for assistance from their mobile phone provider, per Ofcom's vulnerable customer guidelines.⁷⁵
200. A vulnerable victim and, if appropriate, their support representative (independent advisor, independent guardian family friend etc) should be referred to the relevant services (social services, counselling, independent guardian service etc) if ongoing professional support is necessary.

⁷⁵ [Treating vulnerable customers fairly: A guide for phone, broadband and pay-tv providers \(ofcom.org.uk\)](https://www.ofcom.gov.uk/consult/condocs/vulnerablecustomers/vulnerablecustomers.pdf)

Part 6: Section 38: Children and adults without capacity

201. This part of the code gives guidance on cases where a user of a device is a child or an adult without capacity. Children and adults without capacity are not able to make the decisions in Section 37 for themselves. This part sets out who can make those decisions on their behalf ('the alternative individual') and what must be considered by the authorised person and by the alternative individual.

202. It is important to recognise that many children and adults without capacity who can use an electronic device will have some capacity to understand and provide their opinion on whether they wish their device to be examined⁷⁶.

Children

203. For the purposes of Chapter 3 of Part 2 of the Act, a child is a person under the age of 18⁷⁷.

204. Even if a child is deemed as having capacity, an alternative individual will still need to make decisions on whether to provide the device and agree to the extraction of information on behalf of the child.

Who can, and cannot, make decisions for a child?

205. The people referred to in the sections below, may act as an alternative individual where the device user is a child and they are unable to provide agreement for information to be extracted from their device themselves. In doing so, the alternative individual must act in the best interests (for those in England, Wales and Northern Ireland) or for (those in Scotland) the benefit of that child.

A parent or guardian of the child

206. "Parent" includes a biological parent, an adoptive parent, a step-parent who has been granted legal parental responsibility and a parent by virtue of the Human Fertilisation and Embryology Act 2008 (for example, a second female parent).

207. "Guardian" means another person who has been granted legal parental responsibility, a person who has been appointed as a guardian by court order or by a will (where the parents are deceased), or a person who, in practice, carries out the day-to-day care

⁷⁶ See the sections on Views of the child and Views of the adult without capacity for more information

⁷⁷ Section 37(13).

of a child, such as a local authority approved kinship or foster carer. Authorised persons should be clear about and record the status of the parent or guardian who is making the decisions. For further definitions of who can be considered as parent or guardian refer to the sections below.

208. In Northern Ireland, this may also include parent or guardian or other persons or bodies with parental responsibility for the child. The term 'Guardian' should be interpreted according to the Children (Northern Ireland) Order 1995. Article 2 states that "guardian of a child" means a guardian (other than a guardian of the fortune or estate of a child) appointed in accordance with the provisions of Article 159 (Appointment by Court) or Article 160 (Appointment by parent or guardian). In Northern Ireland this will also include Independent Guardians appointed to any child under the provisions of s.21 of the Human Trafficking and Exploitation (Criminal Justice and Support for Victims) Act (Northern Ireland) 2015. Independent Guardians may continue to support and represent the child they are appointed to (with their consent) after that person attains the age of 18 years but is under the age of 21.
209. In England, Wales, and Scotland the term 'Guardian' includes adults who have been appointed to the role of guardian by a court.

A person representing a relevant authority or voluntary organisation

210. If the child is in care and it is not appropriate for agreement to be sought from a parent or guardian, then a person representing the relevant authority or voluntary organisation providing care to that child can provide agreement instead. This should, unless not possible in the circumstances, be a person known to the child.
211. In all cases, the authorised person must satisfy themselves that there is no conflict of interest for the person who is required to represent the best interests of, or act for the benefit of, the child. In the case of where the suspect is someone within the same organisation that supports the child, for example their social worker, it is recommended that the support is obtained from a person unconnected to that organisation. Careful consideration must always be given as to the status of the person providing agreement on behalf of the child and their role in the investigation.
212. A responsible person, who must be 18 or over, must only be used as a last resort if a parent or guardian, or a person representing a relevant authority or voluntary organisation is unavailable to make the decisions on behalf of the child. Unless inappropriate to do so, authorised persons must contact a parent, guardian or person representing the relevant authority or voluntary organisation responsible for the child before turning to another responsible person. Best practice is to wait for such a person to be available to make the decisions.
213. If there is any doubt on the suitability of a responsible person, the authorised person must delay the extraction of information until a parent, a guardian, a representative of

the relevant authority or another, suitable responsible person can be found to provide agreement instead.

214. Where the decisions have been made on behalf of the child by a responsible person, the authorised person must, unless they consider it is inappropriate to do so, notify a parent or guardian that the power has been used and for what purpose. This notification should be made as soon as possible. Where it is not appropriate to notify a parent or guardian because they are a suspect in the investigation, or where the authorised person believes that revealing that information has been extracted will put the child at risk, the authorised person should consider notifying another parent or guardian.
215. An authorised person who may exercise the Section 37 power for the purpose for which information is being sought cannot act as a responsible person.
216. The responsible person should not be a suspect in relation to the enquiry for which the power is being used and should ideally have an existing caregiving relationship with the child.
217. A person who is an authorised person, but who may not exercise the Section 37 power for the purpose for which information is being sought, may act as a responsible other. So, for example, a member of the Serious Fraud Office would be able to act as a responsible person in a case where information is required to help locate a missing person. That is because members of the Serious Fraud Office cannot exercise the Section 37 power for that purpose – they may only do so for the purposes of preventing, detecting, investigating or prosecuting crime.

Obtaining the views of the child

218. Before exercising the Section 37 power, the authorised person must, so far as it is reasonably practicable to do so, ascertain the views of the child and have regard to any views so ascertained, taking account of the child's age and maturity⁷⁸.
219. Very young children and those with significant learning or mental health needs may be incapable of expressing an informed view on the extraction of information from their device. It may not always be clear whether the child is capable of expressing their views or understanding what is being asked of them and therefore, authorised persons must presume that in all instances a child victim or witness is able to provide a view. This means where the child is reasonably locatable, their views must be sought. The age and maturity of the child should be taken into account in having regard to the views ascertained.
220. Authorised persons should ensure that an explanation has been provided to the child as to what will happen to their information and device and that, whilst their views will

⁷⁸ Section 38(4).

be taken into account, it is only an adult who can make decisions on their behalf. The authorised person should confirm that the person making the decisions on behalf of the child is aware of the child's views. The adult may still decide to provide (or not to provide) the device and agree (or not agree) to the extraction of information from it having had regard to the child's views.

221. Authorised persons should consider if any additional support is required for the child or the person providing agreement such as from a family member, social worker, Independent Guardian, Independent Sexual Violence Advisor (ISVA), Independent Domestic Violence Advisor (IDVA), a learning disability advocate or an Independent Mental Health Advisor (IMHA).

222. The person making the decision on whether to provide agreement on behalf of the child must take into account the views the child has on this matter. If the child has a different view to the one held by the person making the decision on whether to provide agreement, the person providing agreement must ensure they seek clarity on why the child holds this view. They must ensure they have considered the child's view but ultimately, the decision on whether to provide the device and agree to extraction is for the person representing the child.

223. In cases where the user is a child, authorised persons should record all relevant information, including:

- if the child was asked for their views, what those views were
- if the child's views differed from the views of the person providing the device and agreeing to the extraction of information from it
- if the child was not asked their views, why not
- the decision the authorised person came to on use of the power and why

Adults without capacity

224. In relation to **England and Wales**, a person is an adult without capacity if, within the meaning of the Mental Capacity Act 2005, they lack capacity to voluntarily provide their device and agree to the extraction of information from it. In this regard, authorised persons must have in mind the principles set out in Section 1 of the Mental Capacity Act 2005.

225. In relation to **Scotland**, a person is an adult without capacity if they are incapable, within the meaning of the Adults with Incapacity (Scotland) Act 2000, in relation to the voluntary provision of their device and agreement to the extraction of information from it. In this regard, authorised persons must have in mind the principles set out in

Section 1 of the Adults with Incapacity (Scotland) Act 2000 and the codes of practice issued further to it.⁷⁹

226. In relation to **Northern Ireland**, a person is an adult without capacity if, within the meaning of the Mental Capacity Act (Northern Ireland) 2016, they lack capacity to voluntarily provide their device and agree to the extraction of information from it. When a determination falls to be made of whether a device user is an adult who lacks capacity, authorised persons must make that determination in accordance with the principles in Section 1 of Mental Capacity Act (Northern Ireland) 2016.

Who can, and cannot, make decisions for an adult without capacity?

227. The people referred to in the sections below, may act as an alternative individual where the device user is an adult without capacity and they are unable to provide agreement for information to be extracted from their device themselves. In so doing, they must act in the best interests of that adult (for those in England, Wales and Northern Ireland) and for their benefit (for those in Scotland).

A parent or guardian of the adult without capacity

228. "Parent" includes a biological parent, an adoptive parent, a stepparent who has been granted legal parental responsibility and a parent by virtue of the Human Fertilisation and Embryology Act 2008⁸⁰ (for example, a second female parent).

229. "Guardian" means another person who has been granted legal parental responsibility, a person who has been appointed as a guardian by court order or by a will (where the parents are deceased), or a person who, in practice, carries out the day-to-day care of the adult without capacity. Authorised persons should be clear about and record the status of the parent or guardian who is making the decisions. For further definitions of who can be considered as parent or guardian refer to the sections below.

230. In relation to **England and Wales**, the term 'Guardian' includes adults who have been appointed to the role of guardian by a court.

231. In relation to **Scotland**, the term 'Guardian' should be interpreted according to:

- Section 64 of the Adults with Incapacity (Scotland) Act 2000, which defines both welfare and financial guardians
- Section 58(1A) of the Criminal Procedure (Scotland) Act 1995, which points to guardians with powers relating to the personal welfare of an adult

⁷⁹ Six main Codes of Practice can be found at [Adults with incapacity: forms and guidance - gov.scot \(www.gov.scot\)](https://www.gov.scot/adults-with-incapacity-forms-and-guidance)

⁸⁰ Link to [The Human Fertilisation and Embryology Act 2008](#)

232. In relation to **Northern Ireland**, the term ‘Guardian’ should be interpreted according to [the Mental Health \(Northern Ireland\) Order 1986](#).

233. The term guardian also includes persons who are appointed as Independent Guardians under s.21 of the Human Trafficking and Exploitation (Criminal Justice and Support for Victims) Act (Northern Ireland) 2015.

A person representing a relevant authority or voluntary organisation

234. If the adult without capacity is in the care of a relevant authority or voluntary organisation and it is not appropriate for agreement to be sought from a parent or guardian, then a person representing the relevant authority or voluntary organisation providing that care can provide agreement instead.

235. This should, unless not possible in the circumstances, be a person known to the adult without capacity.

236. In all cases, the authorised person must satisfy themselves that there is no conflict of interest for the person who is required to represent the best interests or act for the benefit of the device user where they are an adult without capacity. In the case of where the suspect is someone within the organisation that supports the child, for example a care worker, it is recommended that the support is obtained from a person unconnected to that organisation. In all cases, careful consideration must also be given to the status of the person representing the child and their involvement in the investigation.

A registered social worker

237. In relation to **England**, “registered social worker” means a person registered as a social worker in a register maintained by Social Work England.

238. In relation to **Wales**, “registered social worker” means a person registered as a social worker in a register maintained by Social Care Wales (previously known as Care Council for Wales).

239. In relation to **Scotland**, “registered social worker” means a person registered as a social worker in a register maintained by the Scottish Social Services Council. The term ‘social worker’ should be interpreted in accordance with Section 77 of the [Regulation of Care \(Scotland\) Act 2001](#). Authorised persons should follow guidance on the role of the registered social worker in statutory interventions.

240. In relation to **Northern Ireland**, “registered social worker” means a person registered as a social worker in a register maintained by the Northern Ireland Social Care Council. The term ‘social worker’ should be interpreted in accordance with the Health and Personal Social Services Act (Northern Ireland) 2001.

A person who under a power of attorney may make the relevant decisions

241. In relation to **England and Wales**, this means a person with a lasting power of attorney which gives them the powers to make decisions on behalf of an individual who lacks capacity. Authorised persons should follow the relevant guidance [here](#).
242. In relation to **Scotland**, this means welfare attorneys and continuing attorneys who have combined powers to make decisions regarding the welfare and financial matters of an individual who lacks capacity. Authorised persons should follow the [Continuing and welfare attorneys: code of practice](#).
243. In relation to **Northern Ireland**, this means persons appointed under an enduring power of attorney, within the meaning of the Enduring Powers of Attorney (Northern Ireland) Order 1987; and following the commencement of Part 5 of the Mental Capacity Act (Northern Ireland) 2016, persons appointed under a lasting power of attorney, within the meaning of that Part.

A deputy who may make the relevant decisions (not Scotland)

244. In **England and Wales**, a deputy may be appointed under Section 16 of the Mental Capacity Act 2005. Further guidance on the role of a deputy in England and Wales can be found in the [Mental Capacity Act Code of Practice - GOV.UK \(www.gov.uk\)](#).
245. In **Northern Ireland**, a deputy may be appointed under Section 113 of the [Mental Capacity Act \(Northern Ireland\) 2016](#)⁸¹.

A person who under an intervention order may make the relevant decisions (Scotland only)

246. Section 53 of the Adults with Incapacity (Scotland) Act 2000 deals with intervention orders.

A responsible person

247. A responsible person, who must be 18 or over, must only be used as a last resort if no other person (as listed above) is unavailable to make the decisions on their behalf. Unless inappropriate to do so, authorised persons must contact a parent or guardian, or another suitable person, before turning to a responsible person to notify them of the need to exercise the power and for what purpose. Best practice is to wait for such a person to be available to make the decisions. Where it is not appropriate to notify a parent or guardian because they are a suspect in the investigation, or where the authorised person believes that revealing that information has been extracted will put

⁸¹ At the time of preparation of this code, Section 113 had not yet been commenced.

the adult without capacity at risk, the authorised person should consider notifying another parent or guardian.

248. If there is any doubt on the suitability of a responsible person, the authorised person must delay the extraction of information until a suitable responsible person can be found to provide agreement instead.
249. An authorised person who may exercise the Section 37 power for the purpose for which information is being sought may not act as a responsible person.
250. The responsible person should not be a suspect in relation to the enquiry for which the power is being used and should ideally have an existing caregiving relationship with the adult without capacity.
251. A person who is an authorised person, but who may not exercise the Section 37 power for the purpose for which information is being sought, may act as a responsible other.

Obtaining the views of the adult without capacity

252. Where an authorised person assesses that a device user is an adult without capacity, the decisions as to whether to voluntarily provide the device and agree to the extraction of information from it must fall to another person (as specified above).
253. Before exercising the Section 37 power, the authorised person should, so far as it is reasonably practicable to do so, ascertain the views of the adult without capacity and have regard to any views so ascertained, taking into account the conditions that affect their capacity. Those operating in England, Wales and Northern Ireland must have the individual's best interests in mind and for those in Scotland, be acting for their benefit.
254. Authorised persons should consider if any additional support is required for the adult without capacity or the person providing agreement, such as from a family member, social worker, Independent Guardian, Independent Sexual Violence Advisor (ISVA), Independent Domestic Violence Advisor (IDVA), a learning disability advocate or an Independent Mental Health Advisor (IMHA).
255. Authorised persons should ensure that an explanation has been provided to the adult without capacity as to what will happen to their information and device and that, whilst their views will be taken into account, it is only their parent, guardian or responsible other who can make decisions on their behalf. The authorised person should confirm that the person making the decisions on behalf of the individual is aware of their views. Ultimately, the person representing the individual may still decide to provide (or not to provide) the device and agree (or not agree) to the extraction of information from it having had regard to the individual's views.

256. Some people's ability to make decisions fluctuates because of a condition that they have. In such cases, if possible, the decisions as to whether to voluntarily provide the device and agree to the extraction of information from it should be made by the device user at a time when the person has the capacity to decide for themselves. It may also be helpful to discuss and record what the person would want if they lost capacity to make similar decisions in future, for example where it is anticipated that they will reach a stage due to a condition or illness that will prevent them from expressing an opinion should there be a need to extract additional information from their device in the future. This means that, if further decisions need to be taken in their best interests and for their benefit, the authorised person can take the person's wishes into consideration.

257. In cases where the user is an adult without capacity, authorised persons should record all relevant information, including:

- the basis of the assessment that the adult is without capacity
- if the adult without capacity was asked for their views, what those views were
- if the adult without capacity views differed from the views of the person providing the device and agreeing to the extraction of information from it
- if the adult without capacity was not asked their views, why not
- the decision the authorised person came to on use of the power and why

Definitions

Adult - a person aged 18 or over

Adult without capacity – an individual is without capacity if they are aged 18 or over and;

(a) in relation to England and Wales, the person is an adult who, within the meaning of the Mental Capacity Act 2005, lacks capacity to do the things mentioned in Section 1(1)(a) and (b);

(b) in relation to Scotland, the person is an adult who is incapable within the meaning of the Adults with Incapacity (Scotland) Act 2000 in relation to the matters mentioned in Section 1(1)(a) and (b);

(c) in relation to Northern Ireland, the person is an adult who, within the meaning of the Mental Capacity Act (Northern Ireland) 2016, lacks capacity to do the things mentioned in Section 1(1)(a) and (b).

Appropriate Adult (Scotland) – means:

A person appointed to provide support for an adult who is aged 16 and over and owing to a mental disorder (as defined in Section 328 of the Mental Health (Care and Treatment Act) (Scotland) Act 2003) appears unable to understand sufficiently what is happening or communicate effectively during a criminal investigation. The Criminal Justice (Scotland) Act 2016 (Support for Vulnerable Persons) Regulations 2019 places a duty on local authorities to deliver Appropriate Adult services.

At-risk adult – an individual who the authorised person reasonably believes:

(a) is experiencing, or at risk of, neglect or physical, mental, or emotional harm, and

(b) is unable to protect themselves against the neglect or harm or the risk of it.

Authorised Person - An authorised person can refer to the person interacting with the device user or person providing agreement (where different) the person authorising the scope of the extraction of information, and the person completing the extraction of data from the electronic device.

Child - a person aged under 18 years

Confidential information - information which constitutes or may constitute;

(a) confidential journalistic material within the meaning of the Investigatory Powers Act 2016 (see Section 264(6) and (7) of that Act), or

(b) protected material. (3) In subsection (2)(b)

Deputy – an individual appointed under Section 16 of the Mental Capacity Act 2005 or Section 113 of the Mental Capacity Act (Northern Ireland) 2016 who may make decisions for the purposes of subsection (7)(a) and (b) of the power on behalf of the adult without capacity by virtue of that appointment

Device user - a person who ordinarily uses the electronic device

Electronic device - any device on which information is capable of being stored electronically and includes any component of such a device

Enactment – includes;

(a) an enactment contained in subordinate legislation within the meaning of the Interpretation Act 1978,

(b) an enactment contained in, or in an instrument made under, an Act of the Scottish Parliament,

(c) an enactment contained in, or in an instrument made under, an Act or Measure of Senedd Cymru, and (d) an enactment contained in, or in an instrument made under, Northern Ireland legislation.

Information - includes moving or still images and sounds

Local authority – means;

a) in relation to England, a county council, a district council for an area for which there is no county council, a London borough council or the Common Council of the City of London;

(b) in relation to Wales, a county council or a county borough council;

(c) in relation to Scotland, a council constituted under Section 2 of the Local Government etc (Scotland) Act 1994;

Registered social worker - a person registered as a social worker in a register maintained by;

(a) Social Work England,

(b) Social Care Wales (previously known as Care Council Wales),

(c) the Scottish Social Services Council, or

(d) the Northern Ireland Social Care Council; “relevant authorised person”, in relation to the extraction of information from an electronic device for a particular purpose, means an authorised person who may extract the information from the device for that purpose.

Relevant authority – means;

- (a) in relation to England and Wales and Scotland, a local authority;
- (b) in relation to Northern Ireland, an authority within the meaning of the Children (Northern Ireland) Order 1995 (S.I. 1995/755 (N.I. 2)).

Protected material – means;

(a) in relation to England and Wales means

- (i) items subject to legal privilege, within the meaning of the Police and Criminal Evidence Act 1984 (see Section 10 of that Act),
- (ii) material falling within Section 11(1)(a) of that Act (certain personal records held in confidence), or
- (iii) material to which Section 14(2) of that Act applies (other material acquired in course of a trade etc that is held in confidence);

(b) in relation to Scotland means;

- (i) items in respect of which a claim to confidentiality of communications could be maintained in legal proceedings, or
- (ii) other material of a kind mentioned in paragraph (a)(ii) or

(c) in relation to Northern Ireland, means;

- (i) items subject to legal privilege, within the meaning of the Police and Criminal Evidence (Northern Ireland) Order 1989 (S.I. 1989/1341 (N.I. 12)) (see Article 12 of that Order),
- (ii) material falling with Article 13(1)(a) of that Order (certain personal records held in confidence), or
- (iii) material to which Article 16(2) of that Order applies (other material acquired in the course of a trade etc that is held in confidence).

Voluntary organisation – means:

- (a) in relation to England and Wales, has the same meaning as in the Children Act 1989;
- (b) in relation to Scotland, has the same meaning as in Part 2 of the Children (Scotland) Act 1995;
- (c) in relation to Northern Ireland, has the same meaning as in the Children (Northern Ireland) Order 1995.

Annexes

Annex A – Schedule 3 Authorised Persons

An authorised person can refer to the person interacting with the victim or witness, the person authorising the scope of the extraction of information, and the person completing the extraction of information from the electronic device.

The authorised persons able to use the powers in Sections 37 and 41 of the Act are listed in Schedule 3 to the Act. This schedule can be updated by secondary legislation, for the most up to date list of authorised persons please look up the most up to date version of the Act⁸².

Schedule 3 is split into three parts.

Authorities listed in **Part 1** of the Schedule may exercise either power for any specified purpose, that is to say:

- In the case of the Section 37 power:
 - preventing, detecting, investigating, or prosecuting crime,
 - helping to locate a missing person, or
 - protecting a child or an at-risk adult from neglect or physical, mental, or emotional harm,
- in the case of the Section 41 power, an investigation or inquest into a death.

Authorities listed in **Part 2** of the Schedule may exercise the Section 37 power for any specified purpose (these authorised persons may not exercise the Section 41 power):

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

Authorities listed in **Part 3** of the Schedule may exercise the Section 37 power for the following specified purpose, (these authorised persons may not exercise the Section 37 power for other purposes or the Section 41 power):

- preventing, detecting, investigating, or prosecuting crime.

Authorised persons should also refer to their own specific internal guidance to ensure they are meeting any organisation-specific responsibilities.

Schedule 3 Part 1

AUTHORISED PERSONS IN RELATION TO ALL PURPOSES WITHIN SECTION 37 OR 41
A constable of a police force in England and Wales.

⁸² [Police, Crime, Sentencing and Courts Act 2022 \(legislation.gov.uk\)](https://www.legislation.gov.uk)

A member of staff appointed by the chief officer of police of a police force in England and Wales
An employee of the Common Council of the City of London who is under the direction and control of a chief officer of police.
A constable within the meaning of Part 1 of the Police and Fire Reform (Scotland) Act 2012 (asp 8) (see Section 99 of that Act).
A member of staff appointed by the Scottish Police Authority under Section 26(1) of the Police and Fire Reform (Scotland) Act 2012.
A police officer within the meaning of the Police (Northern Ireland) Act 2000 (see Section 77(1) of that Act).
A constable of the British Transport Police Force
An employee of the British Transport Police Authority appointed under Section 27 of the Railways and Transport Safety Act 2003.
A constable of the Ministry of Defence police.
A National Crime Agency officer
A person who has been engaged to provide services consisting of or including the extraction of information from electronic devices for the purposes of the exercise of functions by a person listed in this part of this Schedule

Schedule 3 Part 2

AUTHORISED PERSONS IN RELATION TO ALL PURPOSES WITHIN SECTION 37 ONLY
A member of the Royal Navy Police, the Royal Military Police or the Royal Air Force Police.
A person appointed as an immigration officer under paragraph 1 of Schedule 2 to the Immigration Act 1971.
A person who is an enforcement officer by virtue of Section 15 of the Gangmasters (Licensing) Act 2004.
A person who has been engaged to provide services consisting of or including the extraction of information from electronic devices for the purposes of the exercise of functions by a person listed in this part of this Schedule.

Schedule 3 Part 3

AUTHORISED PERSONS IN RELATION TO SECTION 37 THE PREVENTION OF CRIME ETC ONLY
An officer of Revenue and Customs.
A person designated as a general customs official or a customs revenue official under the Borders, Citizenship and Immigration Act 2009 (see Sections 3 and 11 of that Act)
An officer of the department of the Secretary of State for Business, Energy and Industrial Strategy
A member of the Serious Fraud Office.
A person appointed by the Financial Conduct Authority under the Financial Services and Markets Act 2000 to conduct an investigation
An officer of the Competition and Markets Authority.
A person who is authorised by the Food Standards Agency to act in matters arising under or by virtue of the Food Safety Act 1990.
A person who is authorised for the purposes of Part 6 of the Social Security Administration Act 1992.
An inspector appointed under Section 15 of the Child Support Act 1991.

A person designated by the Director General of the Independent Office for Police Conduct under paragraph 19(2) of Schedule 3 to the Police Reform Act 2002.
The Police Investigations and Review Commissioner
A person designated by the Police Investigations and Review Commissioner under paragraph 7B(1) of Schedule 4 to the Police, Public Order and Criminal Justice (Scotland) Act 2006 (asp 10).
An officer appointed by the Police Ombudsman for Northern Ireland under Section 56(1) or (1A) of the Police (Northern Ireland) Act 1998.
A person who is an enforcement officer by virtue of Section 303 of the Gambling Act 2005.
A person who has been engaged to provide services consisting of or including the extraction of information from electronic devices for the purposes of the exercise of functions by a person listed in this part of this Schedule.

Annex B - Overview of the principles of Bater-James

The principles in R V Bater-James and Mohammed [2020] EWCA Crim 970

For authorised persons in England and Wales, the [Bater-James judgment](#) contains four principles in relation to the extraction and use of digital material, which are summarised below. While this was a criminal case that focused on the review of witnesses' electronic communications, the principles are relevant in any case, enquiry or investigation where it is necessary and proportionate to examine a device.

The first issue of principle concerns identifying the circumstances when it becomes necessary for investigators to seek details of digital communications, and notes that it should not be assumed that it is necessary to inspect digital material in every case and should only be conducted as part of a reasonable line of enquiry.

The second issue of principle concerns guidelines around how an investigation of a device should be carried out proportionately and with regard to the privacy impact on the victim.

The third issue of principle concerns the information that should be provided to the person whose device is being examined, ensuring they are sufficiently informed as to the ambit of the review.

The fourth issue of principle concerns the consequences for the case if the person refuses access to a potentially relevant device.

Annex C – DPA and GDPR

There are specific functions and responsibilities under the Data Protection Act 2018 and UK GDPR for persons acting in their capacity as a ‘controller’ or a ‘processor’⁸³.

‘Controllers’ exercise overall control over the purposes and means of the processing of personal data i.e., they will decide what data to process and why.

A ‘processor’ acts on behalf of the ‘controller’ to process the data. You are likely to be acting as a ‘processor’ if you extract and review the data on direct instruction from the controller, even if you make some technical decisions about how you process the data.

‘Sensitive processing’ under Part 3 of the DPA

Section 35 of the DPA outlines the requirements when processing sensitive data. This is referred to as ‘sensitive processing’. This is only permitted in the following circumstances:

- when the data subject has given consent to the processing for the law enforcement purpose and at the time when the processing is carried out, the controller has an appropriate policy document⁸⁴ in place.
- when the processing is **strictly necessary** for the law enforcement purpose, that the processing meets at least one of the conditions in Schedule 8, and at the time when the processing is carried out, the controller has an appropriate policy document⁸⁵ in place.

Part 3 of the DPA defines ‘sensitive processing’ as:

- a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership.
- (b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual.
- (c) the processing of data concerning health.
- (d) the processing of data concerning an individual’s sex life or sexual orientation

The conditions for ‘sensitive processing’ in Schedule 8 of the Act are:

1. necessary for judicial and statutory purposes – for reasons of substantial public interest;

⁸³ For further guidance on the application of the DPA and UK GDPR see [Information Commissioner's Office \(ICO\)](#)

⁸⁴ ICO – Conditions for sensitive processing: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-le-processing/conditions-for-sensitive-processing/#whatis>

⁸⁵ For example, the NPCC Digital Processing Notice (DPN)

2. necessary for the administration of justice;
3. necessary to protect the vital interests of the data subject or another individual;
4. necessary for the safeguarding of children and of individuals at risk;
5. personal data already in the public domain (manifestly made public);
6. necessary for legal claims;
7. necessary for when a court acts in its judicial capacity;
8. necessary for the purpose of preventing fraud; and
9. necessary for archiving, research or statistical purposes.

You must be able to demonstrate that the processing is strictly necessary and satisfies one of the conditions in Schedule 8. Strictly necessary in this context means that the processing must relate to a pressing social need, and you cannot reasonably achieve it through less intrusive means.

Individuals providing agreement will have a reasonable expectation that any personal information is managed to a high standard where it may relate to protected characteristics or otherwise be special category data within the meaning of the DPA.

General overview of the UK GDPR responsibilities

Article 5 of the UK GDPR sets out seven key principles which must be complied with when processing personal data for non-law enforcement purposes, including when exercising these powers

The seven principles as summarised below are:

1. Lawfulness, fairness, and transparency
 2. Purpose limitation
 3. Data minimisation
 4. Accuracy
 5. Storage limitation
 6. Integrity and confidentiality (security)
 7. Accountability
- 1) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
 - 2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
 - 3) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
 - 4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to

the purposes for which they are processed, are erased or rectified without delay ('accuracy');

- 5) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
- 6) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."
- 7) Article 5(2) adds that "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')." You must have appropriate measures and records in place as proof of your compliance with the data processing principles. Supervisory authorities can ask for this evidence at any time. Documentation is key here. It creates an audit trail you and the authorities can follow if you do need to prove responsibility.

Article 9 of the UK GDPR defines the lawful basis on which you can process 'special category data' whilst Article 9 defines the conditions for processing⁸⁶.

'special category data' - conditions for processing under UK GDPR

The UK GDPR defines 'special category data' as:

- 1) personal data revealing racial or ethnic origin;
- 2) personal data revealing political opinions;
- 3) personal data revealing religious or philosophical beliefs;
- 4) personal data revealing trade union membership;
- 5) genetic data;
- 6) biometric data (where used for identification purposes);
- 7) data concerning health;
- 8) data concerning a person's sex life; and
- 9) data concerning a person's sexual orientation.

Article 6 states that processing shall be lawful only if and to the extent that at least one of the following applies:

⁸⁶ See annex D for the UK GDPR definition of 'special category data' and the conditions for processing.

1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
3. processing is necessary for compliance with a legal obligation to which the controller is subject;
4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Article 9 defines the conditions for processing:

- Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
- Paragraph 1 shall not apply if one of the following applies:
 - the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
 - processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
 - processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
 - processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
 - processing relates to personal data which are manifestly made public by the data subject;

- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Information about a deceased person does not constitute personal data and therefore is not subject to the UK GDPR. However, processing data from a device obtained from a deceased person that contains data relating to other identifiable living persons, may constitute the processing of personal data under the UK GDPR regime.

Annex D – Example Digital Processing Notice to obtain written agreement

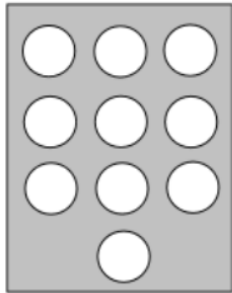
The below are samples of the NPCC Digital Processing Notices. For the most up to date forms please use this link: [NPCC internet page containing the latest DPN documents](#)

[Insert force logo]

Digital Processing Notice (DPNa) (Device taken from witness)

***** To be completed by the officer taking possession of the device. A separate form must be completed for each device. Provide a copy of pages 1 - 3 to the device owner once complete. *****

Throughout this form the term 'witness' is used to refer to victims and witnesses

Crime Report No:				
OIC Details				
Station / Department / Team				
Name & Shoulder No				
Device Details				
Exhibit Ref			Device Pattern Lock 	
Telephone No(s)				
Make of Device	Model			
Data Card Present	Yes <input type="checkbox"/> No <input type="checkbox"/>	No of Cards		
IMEI No.				
SIM PIN Code	Device Pass Code			
Alternative Lock Methods	If alternative lock methods are present (e.g. fingerprint or iris) please ask witness to disable			
Description of device condition (e.g. damage or faults, last used)				Indicate beginning and end

I have reasonable grounds to believe that an examination of the device may find material relevant to the investigation or the likely issues at trial (it is a reasonable line of enquiry) because:

Provide the identifiable basis for how this belief has been formed.

DPNa

I consider that it is strictly necessary to extract only the following material from the device in order to progress this reasonable line of enquiry:

What material are you looking for and why is it strictly necessary to extract that material from the device? Be specific. For example: Whatsapp messages between person A and person B between set dates in which the offence is discussed. Ensure you explain why the material is strictly necessary in light of the reasonable lines of enquiry you have identified above.

The material I am seeking to extract pursuant to the reasonable line of enquiry is (provide relevant dates, or start and end dates, where possible):

The material is strictly necessary because:

Detail what alternatives to extraction have been considered and rejected. *Explain your reasons:*

Give an indication of where the relevant material is likely to be stored on the device: *e.g. images, text messages, WhatsApp messages. This will enable the operator completing the forensic examination to be more precise in their search.*

Ask the witness where the relevant material is likely to be stored:

DPNa

--

Collateral Intrusion:

To what extent is there a risk of collateral intrusion and what steps, if any, have been taken or can be taken to mitigate this?

Collateral intrusion relates to the personal data of third parties on the device.

I have provided the witness with a copy of this form and form DPNb:

Signature :	
Time/date:	

Witness Declaration	
Name:	
DOB:	
Address:	
Role:	Victim / Witness / Other (delete/circle as appropriate)
Declaration	I agree to provide my device to the Police for the purposes of extracting data as set out in this form. I have been provided with a copy of DPNa and DPNb
Signature:	
Time/Date:	

AUTHORISATION FOR FORENSIC ANALYSIS
THIS MUST BE AUTHORISED PRIOR TO ACQUISITION

To be completed by the authorising Inspector

Authority Required From	INSPECTOR
Is the device lawfully in police possession?	YES / NO If no, detail below what action you have taken
Has the device been interfered with or interrogated in any way? (By police)	YES/NO Explain:
<p>I have considered this request for mobile device extraction and the specific information requested as set out above.</p> <p>I am satisfied that the request is a reasonable line of enquiry and strictly necessary based on the circumstances of the case. Yes/No</p> <p>I am satisfied that the officer requesting the extraction has considered less intrusive means of pursuing the reasonable line of enquiry. Yes/No</p> <p>I authorise/reject the request.</p>	
Name	Signature
Time & Date Authorised	

Guidance for officer completing the form – FAQs

When should I extract material from the device of a witness?

The request to inspect digital material, in every case, must have a proper basis, namely that there are reasonable grounds to *believe* that it may reveal material relevant to the investigation or the likely issues at trial – it has to be a reasonable line of enquiry (Bater-James and Mohammed v R [2020] EWCA Crim 790).

We are also required to comply with Part 3 of the Data Protection Act 2018 (DPA).

Devices should not routinely be obtained from victims and witnesses. You must have a properly identifiable basis for forming your belief that specific material is required from the device. Devices should not be sought on the basis of mere conjecture or speculation. The same requirements apply to requests for searches by the defence. Their requests must be sufficiently precise to enable targeted searching of devices for relevant material. You should challenge requests for searches for material from the defence when they are not sufficiently precise to enable targeted searching. If in doubt, seek the advice of the CPS.

Further guidance on communications evidence can be found here (insert link to CPS guidelines on communications evidence)

What is the lawful basis for taking the device and processing the personal information?

We take possession of devices belonging to witnesses with their agreement. This agreement is often referred to as 'common law consent'. There are limited circumstances in which a lawful power of seizure may also be used to take possession of the device of a witness (see next question). Once we have possession of the device we will process the personal data on it in accordance with Part 3 of the Data Protection Act 2018. This allows us to process personal data when it is required for a law enforcement purpose. There are conditions attached. As we expect to process sensitive personal data we will only acquire data from the device when it is 'strictly necessary' to do so for the law enforcement purpose. We need to meet one of the conditions set out in Schedule 8 DPA 2018. The conditions most likely to be met are:

- necessary for judicial and statutory purposes – for reasons of substantial public interest;
- necessary for the administration of justice;
- necessary for the safeguarding of children and of individuals at risk.

We must demonstrate that we have considered alternative, less intrusive means of achieving the same law enforcement purpose.

Do I need the agreement of the witness to take possession of their device?

DPNa

You should always engage with the witness to seek their agreement before taking possession of their device. See the question below for what to do when the witness does not agree to hand over their device.

There are limited circumstances in which you can take possession of the device without the agreement of the witness. You will need to use a lawful power of seizure to do this and should do this only when there is an identifiable basis for believing the device owner, or someone else, is at risk of harm and that the risk cannot be mitigated by less intrusive means. This should be done only once the steps detailing what must be done when a witness does not agree to hand over the device (set out below) have been followed.

If you have lawfully seized a device (e.g. during the execution of a warrant) and you later find that it belongs to a witness, you should seek the agreement of the witness and complete a DPNa before examining the device. If the witness refuses to give their agreement, you should proceed only when there is an identifiable basis for believing that the device owner, or someone else, is at risk of harm and that the risk cannot be mitigated by less intrusive means.

Whose agreement do I need if the witness is a child or vulnerable adult?

You should always include the child or vulnerable adult in the decision making and their views must be considered. You should ensure that an appropriate adult is present when these discussions take place and the agreement should be between all parties. Where the child or vulnerable adult does not have the capacity to make the decision, the agreement can be with the appropriate adult alone.

If the witness agrees, how should I review the material?

Once you have identified that it is a reasonable line of enquiry, and the witness has agreed to provide their device, you need to consider how the material is to be reviewed.

Your approach should be incremental, starting with the least intrusive method where appropriate. To reduce the inconvenience to the witness you should keep the device for only so long as is necessary. You should consider:

- What material do I want to review? Can I do this without taking the device from the witness?
- Have I already obtained the same material from the suspect's device? If so, do I still need to examine the witness's device? Is corroboration required?
- Manual examinations of devices, including screen shots, may be considered in certain circumstances.
- If you are unsure which method of capture to use, seek forensic advice.
- You should consider a manual examination, including screenshots, without taking the device away only when:
 1. There is minimal material and it is unlikely to be of significant evidential value;
 2. Material on devices could be lost if not captured immediately;
 3. Volatile material is present, i.e. data that might be lost if the device is turned off; or

DPNa

4. Having carefully sought to persuade the witness to provide their device, reassured them of its handling and explained to them the potential consequences of refusing to provide it, you find the witness still chooses not to do so, leaving screenshots as the only available option to secure some record of the material. This might be the case if the witness will not allow you to take the device but will allow screenshots to be taken.

- If you capture material using manual examination, you should make clear in the case file: (1) that this method was used; and (2) your reasons for believing that screenshots provide the only remaining way of recording the material in the circumstances.
- If you capture material using manual examination because this is all the witness will agree to, you should make clear in the case file your efforts to persuade the witness to provide their device and their reasons for not doing so. This should be included in their witness statement.
- If the conditions for manual examination are not met then you will need forensically to acquire the material from the device belonging to the witness. The contents should be acquired with minimum inconvenience and the device returned without unnecessary delay.
- You should acquire and/or search only for the material you believe will be relevant to the case. Wherever possible, you should also specify the time-frame that is likely to be relevant, and set specific start and end dates before searching for and/or acquiring material. If you are using search terms to review the material, these must be recorded. You should advise the witness that you have set these parameters, together with your rationale.
- Technology used to acquire material from devices is developing all the time, as are the devices themselves. Some technology will enable specific types of material to be targeted. However, some require the copying or acquisition of recoverable content on a device to enable a more specific review either manually or using search tools. Whatever technology is used, you must seek only material that enables the review of what is strictly necessary as identified on this form and agreed with the witness.
- Wherever possible, you should delete any material acquired from a device that is outside of the parameters agreed with the witness. This includes material that has not been reviewed following the deployment of search tools.
- If you need to expand the parameters agreed with the witness you should seek to reacquire their device and complete a new DPNa.
- It may not be possible to delete material from the master copy if it is inextricably linked to relevant material and/or doing so would adversely affect the provenance and/or integrity of the material should it be subject to challenge at a later date. This may be the case if the material is held on a disc or encrypted file, for example.
- In these circumstances any working copy created should consist only of the material deemed to be relevant.
- The master copy must be kept securely. Additional safeguarding measures to prevent inappropriate access, review or disclosure of the material should be implemented and highlighted within (insert force) Sensitive Processing Appropriate Policy Document.
Force to insert a link to this document.

What if I find evidence of unrelated criminal activity on the device?

7

OFFICIAL - SENSITIVE (when completed)

September 2021

DPNa

You should take a proportionate approach to any evidence of unrelated criminal activity you find on the device. Before initiating an investigation into such activity you should consider very carefully:

1. The seriousness of the offence you are investigating set against the seriousness of the unrelated criminal activity. It is most unlikely to be proportionate, for example, to investigate references in messages to drug use, when dealing with a victim of sexual assault;
2. Whether there is risk of harm to any person as a result of the unrelated criminality;
3. The risk that a witness might disengage if they perceive there to be a likelihood of their being pursued for relatively minor offences and the consequences of this for public safety if as a result an offender is not brought to justice;
4. Whether the information about the unrelated criminal activity is capable of having a bearing on the initial offence being investigated. If so, this information must be revealed to the prosecutor. It will not be disclosed to the defence unless the disclosure test is met;
5. If you are investigating a sexual offence you should seek the authority of a Detective Chief Inspectorⁱⁱ before investigating unrelated criminal activity.

What should I tell the witness about the process?

You should provide the witness with the DPNb 'witness information sheet.' It is important that you communicate clearly and ensure the witness understands their right to privacy and where they can access further information. Whilst this sets out general information you need to tell the victim or witness the following, which will be relevant to their case:

- The legal basis and justification for processing to take place (that the acquisition is performed in pursuance of a reasonable line of enquiry in accordance with the CPIA 1996 as described in this form); explain what material you are seeking, which areas of their device will be looked at, and what particular dates or time-period you will be reviewing, as set out in this form;
- Reassure the witness that their device will be examined only to the extent necessary to pursue the reasonable line of enquiry and that otherwise the contents will not be looked at;
- Tell the witness the length of time they will be without their device (which should be kept to a minimum) using your best estimate;
- Give the witness a copy of the first three pages of this form once complete;
- Keep the witness informed as to the use of their information throughout the course of the investigation, according to the extent to which the witness wishes to be provided with updates. This should be agreed and recorded in your crime report/enquiry log;
- Explain that the relevant material will be revealed to the prosecutor only if investigative/charging advice is sought or the offender is charged with an offence.
- Explain that material will be provided to the defence only if it meets the strict test for disclosure and that it will be served in a suitably redacted form to ensure that personal details or other irrelevant information are not unnecessarily revealed (e.g. photographs, addresses or full telephone numbers).

- Tell the witness about their right to privacy and signpost them to the Sensitive Processing Appropriate Policy Document.

What if the witness does not agree to provide their device or to allow specific material to be extracted?

If this happens, it is important to understand the reasons. Offer reassurance in line with the guidance above. It is important to ensure that the witness is not, and does not feel, unduly pressured. If you are concerned that the witness does not fully understand the process, consider the use of an appropriate adult or intermediary. If the witness maintains their position, record their reasons. You should seek to take a statement from the witness explaining in detail what material exists and why they will not allow the police to examine their device. This statement should then be included in any file that is submitted to the CPS and, if applicable, disclosed to the Defence.

Explain to the witness that if the police are unable to pursue this enquiry:

1. it might be impossible to pursue the investigation;
2. a witness summons might be issued; or
3. a prosecution might be unable to proceed.

Explain to the victim or witness that they must not delete potentially relevant material from their device and that if they do so this might prevent the police from carrying out a fair investigation which could result in the investigation being closed. You should record that this information has been given (you can endorse this Form DPNa).

Decisions as to the progression of a case must be based on whether the suspect can still have a fair trial without a line of enquiry being completed. The police should not close a case only because a witness has not provided their device for examination. You should continue to follow all reasonable lines of enquiry. Decision making should take into account all of the evidence available.

Service Police Investigations Only

- i. Where this notice requires the authority of an Inspector to authorise forensic analysis of a device, an Authorising Service Police Officer is to be of or above the rank of Lieutenant (Royal Navy), Captain (Army or Royal Marines) or Flight Lieutenant (Royal Air Force).*
- ii. Where this notice requires the authority of a Detective Chief Inspector to further investigate unrelated criminal activity, no person shall act as an Authorising Service Police Officer unless they are a Service Police Officer of or above the rank of Lieutenant Commander (Royal Navy), Major (Army or Royal Marines) or Squadron Leader (Royal Air Force).*

[Insert force logo]

Victim/witness FAQ

Digital Processing Notice b (DPNb)

Throughout this form the term 'witness' is used to include both victims and witnesses.

This form contains important information. Please read the contents carefully and to the end of the document. If you have any questions, please ask the officer(s) you are in contact with for the purposes of the investigation.

We have begun an investigation into an allegation of crime and there is a need to examine a digital device in your possession or control. We must investigate to find all relevant material that could have a bearing on the case, whether it points towards or away from the suspect. This notice sets out the approach we will take.

We understand that requesting your personal or private information, either from your mobile phone or other digital device, has the potential to cause anxiety. Investigators need to balance ensuring a fair trial for the accused against any intrusion into the private life of a victim or witness. The purpose of this document is to explain:

- the legal basis upon which we can look at your device;
- when we will ask to look at your device;
- how we will look at it;
- what will happen to the data we copy, retain and review;
- what might happen if you do not agree to us looking at your device and data; and
- your information/privacy rights

Can you explain the law that allows you to take my device?

We will take possession of your device with your agreement. This agreement is often referred to as 'common law consent'. Once we have possession of your device we will process the personal data on it in accordance with Part 3 of the Data Protection Act 2018. This section allows us to process personal data when it is necessary for a law enforcement purpose. There are conditions attached to this. As we expect to process sensitive personal data we will acquire material from your device only when it is proportionate and 'strictly necessary' to do so for that law enforcement purpose. We also need to meet one of the conditions set out in Schedule 8 DPA 2018. The most likely conditions that will be met are:

- necessary for judicial and statutory purposes – for reasons of substantial public interest;
- necessary for the administration of justice;
- necessary for the safeguarding of children and of individuals at risk;

It is possible that we will be in lawful possession of your device without your agreement. For example, it may have been seized under another power. In these circumstances we will always ask for your agreement before acquiring the data from the device. If you do not agree, we will not acquire the data unless there is an identifiable basis for believing that you, or another individual, is at risk of harm and we cannot manage that risk through less intrusive means. In these circumstances we may acquire the data from your device without your agreement. We will tell you when this happens unless to do so would increase the risk to you or others.

DPNb

When we are not in possession of your device and you do not agree to provide it, we will not seek to acquire it through other powers unless there is an identifiable risk of harm to you or to others.

Can I withdraw my agreement once I have provided my device to the police?

If you have changed your mind, you should discuss this with the officer in the case and explain the reasons to him/her. Depending on your case circumstances, we may decide to proceed without your agreement where there is a risk of harm to you or others that cannot be managed through less intrusive means. The officer in the case will explain the reasons to you unless to do so would put you or others at an increased risk.

Why do the police need my device?

We have a legal duty to carry out all reasonable lines of enquiry when investigating a crime.

We must not seek to review a witness's digital material without good cause. The request to inspect digital material must have a proper basis in every case. This means that there must be reasonable grounds to believe that it may reveal material relevant to the investigation or the likely issues at trial.

We should not routinely obtain devices from witnesses. We must have a properly identifiable basis for believing that relevant material will be found on your device. The officer who is with you will inform you of this basis and record it on a form called DPNa. That form will also tell you what material we are seeking from your device (see further below). You will be provided with a copy of this form.

Our request to review the material on your device must be proportionate. We will consider whether there are other ways to obtain the material we need before asking you to hand over your device. The alternative methods that have been considered and rejected will also be recorded in form DPNa.

Do I have to give the police my device?

No. We will ask you to agree to hand over your device but you do not have to. If you decide not to give us the device we will ask you to provide reasons and work with you to address your concerns. Our aim is to reassure you of the good reasons for extracting material and that the extracted material will be kept secure. However, the decision is yours and you do not have to provide your device. Should you decide not to provide your device, it is important that we understand your reasons because we may need to explain them if the case goes to trial.

As explained above, however, if there is a risk of harm to you or others we may use other lawful powers to take possession of your device.

What will happen if I do not agree to give the police my device?

It is your decision whether you want to provide your device to us. If you decide not to allow us to examine material on your device then you will be asked not to delete any material on it, as this risks preventing a fair investigation of the case.

There are potential consequences if you do not provide your device. These include:

1. it may not be possible to pursue the investigation;
2. a witness summons may be issued – this is a document issued by the court that will require you to give evidence at court or provide your device to the court; or
3. a prosecution may be unable to proceed.

This is because the court needs to be sure that the suspect will still be able to have a fair trial if they are charged with any offences. We will explore other options to follow the reasonable line of enquiry. For example, it may be possible to recover material from the suspect's device or there could be other ways to prove a particular point, such as examining CCTV, to find evidence that a person was present at a scene of the crime. If, because the material on your device has not been examined, it is not possible to follow a particular reasonable line of enquiry, any review of the case will take this into account. Whether a fair trial is still possible will depend on the circumstances of each case.

How long will the police keep my device for?

We will keep your device for the minimum amount of time necessary. The length of time will be determined by a number of factors and the officer to whom you give your device will give you an indication of how long this will be. If, for any reason, this length of time changes then you will be kept informed.

Will the police look at everything on my device?

The investigator will look only at the material they deem relevant to the investigation.

If possible we will obtain the material we need without taking your device from you.

If that is not possible then the device may need to be downloaded or copied. The investigator will take your device away to do this. The contents should be acquired with minimum inconvenience to you and your device returned without unnecessary delay.

Wherever possible we will acquire only the material we believe may be relevant so that we can review it. The investigator will make it clear in form DPNa what material they are looking for and why. You will be provided with a copy.

If technology does not allow us to target only the relevant material, we may have to copy more material than we need. If this happens, the investigator will set clear parameters to satisfy the reasonable line of enquiry and review material only within those parameters. This could include reviewing within specific dates, focused enquiries using search terms or only reviewing particular message threads. The investigator will make a record of the parameters they have set and why they have set them. Material outside of those parameters will not be looked at.

What will the police do with the material they take from my device? Who will they give it to?

Before the suspect is charged with an offence.

The suspect does not have a general right to examine the contents of your device. They are, however, likely to be told about or shown material from your device that is evidence of the offence. This is so they have an opportunity to respond to this evidence and will usually take place in a recorded suspect interview.

DPNb

In certain cases, material will be provided to the Crown Prosecution Service in order for them to decide whether the suspect should be charged with an offence. Only relevant material is provided to the prosecutor for this purpose.

After the suspect is charged with an offence.

Once the suspect has been charged to court they are referred to as the defendant. The defendant does not have a general right to examine the contents of your device. The circumstances in which a defendant will see material from your phone or other digital device is explained below.

When we recover material from your phone it will fall into one of three categories:

Evidence

This is the material that the prosecution will use in Court in order to prove the offence. The defendant will see this material. You will be told which material from this category has been, or will be, disclosed to the defendant. It will be disclosed in a suitably edited form to ensure that personal details or other irrelevant information are not unnecessarily revealed (e.g. photographs, addresses or full telephone numbers).

Unused material

This is material that is relevant to the investigation, any person being investigated or the surrounding circumstances of the case but not being relied upon to prove the offence in court. There is a duty on prosecutors to disclose material from this category to the defendant if it assists their defence or undermines the prosecution case. A Crown Prosecution Service lawyer will make a decision about whether to disclose unused material and you will be told which material from this category has been, or will be, disclosed to the defendant. It will be edited to ensure that personal details or other irrelevant information are not unnecessarily revealed (e.g. photographs, addresses or full telephone numbers).

Non-relevant material

This is everything else that does not fit in the first two categories. The defendant will not see this material. In some cases where we have been able precisely to target only the relevant material, there will not be anything in this category. Where we have had to acquire more than we need, we will delete this material wherever possible and as soon as possible. This includes material that has not been looked at because it was not within the parameters set by the officer.

There may be occasions when it is impossible to separate this material from material that falls into the first two categories. If this is the case, it will be dealt with as highlighted within (insert force) Sensitive Processing Appropriate Policy Document. **Force to insert a link to this document**.

In the event that we identify unrelated criminal activity on your device, we will deal with this in a proportionate way. It is most unlikely to be proportionate, for example, to investigate references in messages to drug use, when you have been the victim of a serious offence. When deciding whether further investigation is necessary officers will consider:

1. The seriousness of the offence being investigated set against the seriousness of the unrelated criminal activity;
2. Whether there is risk of harm to any person as a result of the unrelated criminality;

3. Whether the information about the unrelated criminal activity is capable of having a bearing on the initial offence being investigated. If so, this information must be revealed to the prosecutor. It will not be disclosed to the defence unless the disclosure test is met.

How will I know what has been shared and with whom?

We will tell you. The investigator to whom you hand your device will agree a contact plan with you. This will include how often you wish to be kept informed and at what stages of the investigation. If you would like to know what material has been retained and when it is shared, this will form part of that plan.

How will my data be kept secure?

You may be particularly concerned about the security of any data which is copied and stored whilst the criminal investigation is ongoing. Here we briefly explain our commitment to keeping your data secure but you can find further details in the Sensitive Processing Appropriate Policy Document referenced above, and in the Management of Police Information (MoPI) Authorised Professional Practice (APP) policy document issued by the College of Policing and available on their website (the link is included below).

Any data that is downloaded from your device is kept on the [INSERT NAME OF FORCE] (insert how the material is stored – secure database, DVDs, encrypted USBs etc). It will be handled, stored and retained securely in accordance with the provisions of the Management of Police Information (MoPI) APP and, in the case of sensitive data, the Sensitive Processing Appropriate Policy Document. It will not be stored for any longer than necessary.

Further details regarding privacy information, including your rights under data protection legislation, are set out in the Sensitive Processing Appropriate Policy Document

The Sensitive Processing Appropriate Policy Document can be found at <http://www.INSERT>.

The Management of Police Information (MoPI) APP can be found at the College of Policing website <http://www.college.police.uk>.

Data Protection – what are my rights?

The Data Protection Act 2018 affords you certain rights. It also mandates that we tell you certain things, which we have set out below.

The Data Controller for this force is ***force to enter data controller***

The Data Protection Officer for this force is ***force to enter Data Protection Officer***

Under Section 45 Data Protection Act 2018, you are able to make data protection requests (also known as subject access requests or SARs). More information can be found on the ICO website [Your right of access | ICO](#)

You can make a data protection request by ***force to insert contact details***

Further questions or complaints

DPNb

If you have any further questions or you have a complaint, please speak to the officer in charge of your case.

Alternatively, you can contact our Professional Standards Department (insert force details).

If you have a complaint regarding how the police have handled your data from your device device(s), you have the right to complain to the Information Commissioners Office, who are the UK's independent body set up to uphold information rights. They can be contacted through their website on <https://ico.org.uk/make-a-complaint/> or 0303 123 1113.

National Support Agencies

- Victim Support 0808 1689 111/0808 1689 293 or www.victimsupport.org.uk
- Rape Crisis 0808 802 9999 or www.rapecrisis.org.uk
- SAMM 0845 782 3440 or 0121 472 2912 www.samm.org.uk
- Citizens Advice Bureau www.citizensadvice.org.uk
- UK Government Website www.gov.uk/find-a-community-support-group-or-organisation

Insert Force Logo
Digital Processing Notice (DPNc)
(Device taken from suspect)

Complete one form per device

Crime Report No:	
-------------------------	--

OIC Details	
Station / Department / Team	
Name & Shoulder No	

Device Details																				
Exhibit Ref																				
Property Ref																				
Make of Device	Model																			
Device Pass Code																				
SIM Pin Code																				
Description of device condition																				
Device Security Protection – Place X in appropriate column	Protected – give details in box above	<table border="1" style="width: 100px; height: 100px;"> <tr> <td colspan="3" style="text-align: center;">Device Pattern Lock</td> </tr> <tr> <td align="center">○</td> <td align="center">○</td> <td align="center">○</td> </tr> <tr> <td align="center">○</td> <td align="center">○</td> <td align="center">○</td> </tr> <tr> <td align="center">○</td> <td align="center">○</td> <td align="center">○</td> </tr> <tr> <td align="center">○</td> <td colspan="2"></td> </tr> <tr> <td colspan="3" style="text-align: center;">Indicate beginning and end</td> </tr> </table>	Device Pattern Lock			○	○	○	○	○	○	○	○	○	○			Indicate beginning and end		
	Device Pattern Lock																			
	○		○	○																
	○		○	○																
○	○	○																		
○																				
Indicate beginning and end																				
Not Protected																				
Subject refused to provide																				
Not requested - provide your rationale																				

DPNc

I have reasonable grounds to believe that an examination of the device may find material relevant to the investigation or the likely issues at trial (it is a reasonable line of enquiry) because:

Explain your reasonable grounds:

I consider that it is proportionate and strictly necessary to extract only the following material from the device in order to progress this reasonable line of enquiry because:

What material are you looking for and why is it strictly necessary to extract that material from the device? Be specific. For example: Whatsapp messages between person A and person B between set dates in which the offence is discussed. Explain why the material is strictly necessary in the light of the reasonable line of enquiry you have identified above.

The material I am seeking to extract pursuant to the reasonable line of enquiry is (provide relevant dates, or start and end dates, where possible):

The material is strictly necessary because:

Collateral Intrusion:

To what extent is there a risk of collateral intrusion and what steps, if any, have been taken or can be taken to mitigate this?

Collateral intrusion relates to the personal data of third parties on the device.

DPNc

Suspect Details	
Name:	DOB:
Address:	
Bail Date: (if applicable)	

AUTHORISATION FOR FORENSIC ANALYSIS
THIS MUST BE AUTHORISED PRIOR TO ACQUISITION

To be completed by the authorising Inspector

Authority Required from	INSPECTOR
Is the device lawfully in police possession?	YES / NO If no, detail below what action you have taken
Has the device been interfered with or interrogated in any way? (By police)	YES/NO Explain:
I have considered this request for mobile device extraction and the specific information requested as set out above.	
I am satisfied that the request is a reasonable line of enquiry and strictly necessary based on the circumstances of the case. Yes/No	
I am satisfied that the officer requesting the extraction has considered less intrusive means of pursuing the reasonable line of enquiry. Yes/No	
I authorise/reject the request.	
Name	Signature
Time & Date authorised	

3

OFFICIAL - SENSITIVE (when completed)

September 2021

Suspect information notice

Why do the police need my device?

We have a legal duty to carry out all reasonable lines of enquiry when investigating a crime. We must look for all evidence that supports a case against a person as well as information or material that might undermine the case or support the suspected person.

Acquiring material from your device has been considered as a reasonable line of enquiry in this case – that means that there is an identifiable basis for believing that material is held on your device that is relevant to the investigation.

Do I have to give my device to the police?

There are two ways the police can take possession of your device.

1. Use of a lawful power of seizure.

The law permits us to seize your device from you in certain circumstances. The law also provides a power of search to locate the device in certain circumstances. The lawful powers used to search for and seize your device should be explained to you by the officer seizing it if practicable. You are not entitled to refuse when officers are exercising their powers of search and/or seizure lawfully and by doing so you may be committing further offences.

2. Taking the device with agreement.

We may ask you voluntarily to provide us with your device, even when powers of seizure are available. If your agreement is forthcoming we will take possession of your device. This may occur, for example, if you are suspected of committing an offence but you are not being arrested.

Once we have possession of the device we will process the personal data on it in accordance with Part 3 of the Data Protection Act 2018. This section allows us to process personal data when it is required for a law enforcement purpose. There are conditions attached to this. As we expect to process sensitive personal data we will only acquire data from the device when it is 'strictly necessary' to do so for that law enforcement purpose. We also need to meet one of the conditions set out in Schedule 8 DPA 2018. The most likely conditions that will be met are:

- necessary for judicial and statutory purposes – for reasons of substantial public interest;
- necessary for the administration of justice;
- necessary for the safeguarding of children and of individuals at risk.

How long will you keep my device for?

This will depend on the case circumstances. Often the officer seizing or taking possession of your device will not know this information. You will be provided with the details of the officer in the case, who will inform you of how long s/he expects to keep your device for.

Will the police look at everything on my device?

Officers will look only at the material they deem relevant to the investigation.

Wherever possible we will acquire only the material we believe may be relevant, so that we can review it. The investigator will be required to record the material they are looking for and why they are looking for it before the extraction takes place. We may not give you this information as to do so may prejudice the investigation.

If technology does not allow us precisely to target only the relevant material, we may have to copy more material than we need. If this happens, the investigator will set clear parameters to satisfy the reasonable line of enquiry and review material only within those parameters. This could include reviewing within specific dates, focused enquiries using search terms or only reviewing particular message threads. The investigator will make a record of the parameters they have set and why they have set them. Material outside of these parameters will not be looked at.

What will the police do with the material they take from my device? Who will they give it to?

If we make the decision to take no further action in your case then we will not share the material from it with anyone else, unless we identify an unrelated risk to any individual or we identify evidence of unrelated offences. We will tell you when we have done this unless to do would put anyone at risk or prejudice an ongoing investigation.

There may be exceptional circumstances when the information collected may be shared for other purposes. This might be in relation to civil matters before a family court or if you make a complaint about the handling of the investigation relating to your case, for example. Any sharing will be assessed in relation to necessity.

The decision to charge certain categories of offence rests with the Crown Prosecution Service. We will share relevant material with the prosecutor when requesting a charging decision for such offences.

Should you be charged with an offence, the material on your device will fall into one of three categories:

Evidence

This is the material that the prosecution will use in court in order to prove the offence. This material will be served on you/your defence team by the prosecution.

Unused material

This is material that is relevant to the investigation, any person being investigated or the surrounding circumstances of the case but not being relied upon to prove the offence in court. There is a duty on prosecutors to disclose material from this category to the defendant if it assists their defence or undermines the prosecution case.

Non-relevant material

This is everything else that not in the first two categories. In some cases where we have been able precisely to target only the relevant material, there will not be anything in this category. Where we have had to acquire more than we need, we will delete this material wherever

possible and as soon as possible. This includes material that has not been looked at because it was not within the parameters set by the officer.

There may be occasions when it is impossible to separate this material from material that falls into the first two categories. If this is the case, it will be dealt with as highlighted within (insert force) Sensitive Processing Appropriate Policy Document. ****Force to insert a link to this document****.

How will my data be kept secure?

You may be particularly concerned about the security of any data which is downloaded and stored during and after the investigation. Here we briefly explain our commitment to keeping your data secure, but you can find further details in the Sensitive Processing Appropriate Policy Document referenced above, and in the Management of Police Information (MoPI) Authorised Professional Practice (APP) policy document issued by the College of Policing and available on their website (the link is included below).

Any data that is downloaded from your device is kept on the [INSERT NAME OF FORCE] (insert how the material is stored – secure database, DVDs, encrypted USBs etc). It will be handled, stored and retained securely in accordance with the provisions of the Management of Police Information (MoPI) APP and, in the case of sensitive data, the Sensitive Processing Appropriate Policy Document. It will not be stored for longer than is necessary.

Further details regarding privacy information, including your rights under data protection legislation, are set out in the Sensitive Processing Appropriate Policy Document

The Sensitive Processing Appropriate Policy Document can be found at <http://www.INSERT>.

The Management of Police Information (MoPI) APP can be found at the College of Policing website <http://www.college.police.uk>.

Data Protection – what are my rights?

The Data Protection Act 2018 affords you certain rights. It also mandates that we tell you certain things, which we have set out below.

The Data Controller for this force is ****force to enter data controller****

The Data Protection Officer for this force is ****force to enter Data Protection Officer****

Under Section 45 Data Protection Act 2018, you are able to make data protection requests (also known as subject access requests or SARS). More information can be found on the ICO website [Your right of access | ICO](#)

You can make a data protection request by ****force to insert contact details****

Further questions or complaints

If you have any further questions or you have a complaint, please speak to the investigating officer in charge of your case.

Alternatively, you can contact our Professional Standards Department (insert force details).

DPNc

If you have a complaint regarding how the police have handled your data from your device device(s), you have the right to complain to the Information Commissioners Office, who are the UK's independent body set up to uphold information rights. They can be contacted through their website on <https://ico.org.uk/make-a-complaint/> or 0303 123 1113.

