Home Office

Extraction of information from electronic devices: Draft Code of Practice

October 2021

This publication is available at https://www.gov.uk/government/collections/the-police-crime-sentencing-and-courts-bill

Any enquiries regarding this publication should be sent to us at PCSCExtractioncode@homeoffice.gov.uk.

Contents

Part 1: Introduction 3
Preamble 3
Introduction 3
Effect of the Code 5
What this Code does not cover 5
Part 2: Data Protection 6
Data processing for law enforcement purposes 7
Data processing for non-law enforcement purposes 9
Part 3: Exercise of these powers 11
[Section 36]: the power and the purposes for which it may be exercised 11
[Section 39]: the power and the purposes for which it may be exercised 12
Reasonable belief that information on the device is relevant 12
Necessity and proportionality 13
Proportionality and Risk of obtaining other information 14
Sanctioning use of the powers 15
Recording the use of these powers 16
Part 4: Voluntary provision of device and Agreement to extraction 17
Definition of voluntary provision and agreement 17
Withdrawal of agreement 19
[Section 37]: Cases where a device user is a child or adult without capacity 20
[Section 38]: Agreement where the device user is missing etc. 20
Part 5: Use of the [section 36] power with vulnerable people 21
Vulnerable victims of crime 21
What constitutes a vulnerable victim? 21
Agreement and vulnerable victims 23
Privacy impact and vulnerable victims 24
Safeguarding and vulnerable victims 24
Part 6: Children and Adults without capacity 26
Children 26

Who can, and cannot, make decisions for a child? 26
Views of the child 28
Adults without capacity 29
Who can, and cannot, make decisions for an adult without capacity? 29
Views of the adult who lacks capacity 32
Part 7: Extracting Information 34
Applicable devices 34
Type of extraction 34
Definitions 36
Annexes 39
Annex A – [Schedule 3] Authorised Persons 39
Annex B – Overview of the principles of Bater-James 41
Annex C – DPA and GDPR 41
Annex D – 'special catergory data' conditions for processing under UK GDPR 44

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 40 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 36(1) and 39(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 it[1].

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 victims and witnesses. This Code will ensure a greater understanding on the use of the powers and their application.

4. This Code does not supersede 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 digital evidence from a device, the guidance for that power will apply.

5. The power in [section 36 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 it[2]. The power may be exercised for the purposes of preventing, detecting, investigating or prosecuting crime[3]; helping to locate a missing person, or protecting a child or an at-risk adult[4] from neglect or

[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 36(10]) defines 'electronic device', 'information' and 'user'. [Section 36(11)] is clear that references to the extraction of information include its reproduction in any form.

[3] [Section 36(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 36(10)] defines 'adult' and 'child', and [section 36(4)] sets out when an adult is an 'at-risk adult'.

physical, mental or emotional harm. [Section 37] deals with the application of [section 36] in cases where a user of a device is a child or adult without capacity. [Section 38] deals with the application of [section 36] in three special cases, including where a person who was a user of the device is missing, that person was a user of the device immediately before they went missing and an authorised person reasonably believes that that person's life is at risk.

6. The power in [section 39 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 death[5].

7. [Section 42 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 36 power for any specified purpose (these authorised persons may not exercise the [section 39 power]);
   - [Part 3 of Schedule 3] names those authorised persons who may only exercise the power in [section 36] for the purposes of the prevention, detection, investigation or prosecution of crime (these authorised persons may not exercise the [section 36 power for other purposes or the section 39 power]).

8. In the case of both powers, an authorised person may only exercise the power if they reasonably believe that information stored on the device is relevant to a purpose for which that person may exercise the power. In addition, the authorised person must be satisfied that exercise of the power is necessary and proportionate to achieve that purpose. 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 is 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.

[5] [Section 39(2)] lists the relevant investigations and inquests, and [section 39(3)] makes clear that the power may be exercised for the purposes of determining whether such an investigation or inquest should be held.

Effect of the Code

9. When using or deciding whether to use the [section 36] power or the [section 39] power, an authorised person must have regard to this Code[6].

10. 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. The Code is admissible in evidence in criminal or civil proceedings. A court may take into account a failure to act in accordance with the Code, including in determining the admissibility of the evidence obtained from the data extraction in the proceedings[7].

11. Failure to comply with this code could result in a report being made to the Information Commissioner[8] and could also be considered in professional disciplinary hearings.

What this Code does not cover

12. 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]).
- Extraction of information from a device obtained using coercive or compulsory powers such as a search warrant, production order or statutory notice.
- Covert extraction of information from a device, for example, if it is necessary as part of the investigation to obtain evidence from a device without a user's knowledge.

[6] [Sections 36(8) and 39(7) of the Act.]

[7] [Section 40(7) and (8) of the Act.]

[8] Part 3 of the DPA 2018 introduces a duty on all organisations to report certain types of personal data breach to the Information Commissioner.

Part 2: Data Protection

13. Both the [section 36] power and the [section 39] power must be exercised in accordance with the following:

- **The European Convention on Human Rights ('the ECHR') (including Article 8).**
- **The Data Protection Act 2018 ('the DPA').**
- **The UK General Data Protection Regulation ('the UK GDPR')**

14. The authorised person must carefully consider whether the extraction of information in pursuance of the powers will be a justifiable interference with an individual's rights under Article 8 of the European Convention on Human Rights. Therefore, any interference must be in pursuance of a legitimate aim and conducted in a way that is proportionate and in accordance with the law.

15. The two different data 'processing' regimes of the DPA and UK GDPR must be carefully considered, and the relevant regime must be 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,[9] then Part 3 of the DPA will apply and otherwise Part 2 of the DPA read with the UK GDPR will apply to other general processing.

16. Article 4 of the UK GDPR 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".

[9] 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

Data processing for law enforcement purposes

General overview of DPA responsibilities

17. Part 3 of the DPA 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.

    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).

18. Authorised persons should refer to their own guidance on responsibilities under the DPA.

19. When the power in [section 36 of the Act] is used for the extraction of information for law enforcement purposes, for example the preventing, detecting, investigating or prosecuting crime, the authorised person must comply with the ECHR and part 3 of the DPA[10].

20. The DPA states that the processing of personal data for law enforcement purposes must be lawful and fair. It also states that the processing of personal data for any of

[10] See Part 3 of the DPA Act 2018 when processing personal data for law enforcement purposes

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.[11]

21. Section 35 of the DPA also applies when processing for law enforcement purposes is 'sensitive processing'[12]. In these circumstances, the processing is permitted only in the two cases set out in subsections (4) and (5).

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 place[13].

(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 place[14]

22. The Information Commissioner's Office report 'Mobile phone data extraction by police forces',[15] concludes that Consent is **highly unlikely to be an appropriate condition for processing 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 than consent. This is because of the challenges in ensuring that the person providing Consent understand how their data is going to be processed, because of the imbalance of power between the police and the individual that may make it hard for the person to refuse Consent and because Consent cannot always be withdrawn. Further, it is unlikely that all of those who should provide consent would be able to so as material on the device may relate to many other individuals.

[11] See s.30 DPA 2018 for the meaning of "competent authority".

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

[13] For example, the NPCC Digital Processing Notice (DPN).

[14] See footnote 15.

[15] ICO investigation into mobile phone data extraction by police in the UK | ICO

23. 'Strictly necessary' in this context means that the processing has to relate to a pressing social need, and you cannot reasonably achieve it through less intrusive means. This is a requirement that will not be met if you can achieve the purpose by some other reasonable means.

Data processing for non-law enforcement purposes

24. When the power in [section 36] or in [section 39 of the Act] is used for the extraction of information for non-law enforcement purposes, for example to help locate a missing person, protect a child or an at-risk adult from neglect or physical, mental or emotional harm, where is no criminal investigation element exists, or for the purposes of certain non-criminal investigations or inquests into the person's death[16], the authorised person must comply with ECHR and the UK GDPR[17](read with Part 2 of the DPA). When extracting information for non-law enforcement purposes, the seven principles under Article 5[18] of the UK GDPR need to be met and Article 6[19] 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'[20].

Relevant existing guidance

25. When exercising the [section 36] power for the purposes of preventing, detecting, investigating, or prosecuting crime, authorised persons should consider responsibilities for disclosure that may arise and should be familiar with the documentation listed below.

England and Wales

- Attorney General's Guidelines on Disclosure 2020 (Annex A, Digital Material)
- The Criminal Procedure and Investigations Act 1996 and Code of Practice

Scotland

- The Crown Office and Procurator Fiscal Service Disclosure Manual

Northern Ireland

- The Criminal Procedure and Investigations Act 1996 Code of Practice for Northern Ireland (Revised) 2005

[16] 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.

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

[18] See annex C for the seven UK GDPR principles in Article 5

[19] See annex D for the conditions that must be met under Article 6

[20] See annex D for an explanation of 'special category data' under UK GDPR.

- Further guidance on disclosure is also contained in the Public Prosecution Service Code for Prosecutors

Part 3: Exercise of these powers

[Section 36]: the power and the purposes for which it may be exercised

26. The power in [section 36] requires that a user of the device has voluntarily[21] provided it to an authorised person and has agreed to the extraction of information from it[22]. Where the power is being exercised for the purposes of preventing, detecting, investigating or prosecuting crime, this will commonly be a victim of, or a witness to, a crime. However, there is no barrier to a suspect or person of interest handing over their device and agreeing to the extraction of information from it.

27. If a device has multiple users, it is the responsibility of the authorised person to ensure that the person volunteering the device and agreeing to the information extraction from it, is a user of that device.

28. In many instances, if the person is a suspect and the authorised person wishes to seize the device to prevent loss or destruction of evidence then it is likely that a coercive power (for instance, in England and Wales, where a constable is lawfully on premises, section 19 of the Police and Criminal Evidence Act 1984) will be more appropriate. It is for the authorised person to determine in each instance if this is the appropriate power to use depending on the circumstances.

29. The power in [section 36] may also be used for the purposes of helping to locate a missing person.

30. Before exercising the [section 36] power to help locate a missing person, an authorised person should consult the College of Policing APP guidance on missing persons (police in England and Wales) or other appropriate organisational guidelines.

31. The power in [section 36] may also be used 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).

32. For guidance on the meaning of harm, **Authorised persons In England and Wales** should refer to page 107 of the Mental Capacity Act Code of Practice 2005(England and Wales).

[21] See point 61 for a definition of 'voluntary'.

[22] The only exceptions to this are where a user is a child or adult without capacity (in which case [section 37] applies) or where one of the conditions in [section 38] applies.

33. **In relation to Scotland**, the Adults with Incapacity (Scotland) Act 2000 applies.

34. **Authorised persons in Northern Ireland** should refer to The Mental Health (NI) Order 1986 Code of Practice and any relevant codes issued under the Mental Capacity Act (Northern Ireland) 2016.

[Section 39]: the power and the purposes for which it may be exercised

35. The power in [section 39] 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 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). This includes determining whether such an investigation or inquest should take place.

36. This is separate to the power in [section 36] which may also be used where a person has died provided the conditions in [section 36] are met.

Reasonable belief that information on the device is relevant

37. Whenever the use of these powers is considered there must be an identifiable basis that justifies the need to examine a digital device.

38. [Sections 36(5) and 39(4)] set out conditions for use of these powers. Paragraph (a) of both provisions state that an authorised person may only exercise the powers if:

    the authorised person reasonably believes that information stored on the electronic device is relevant to

    (i) in the case of the [section 36] power, a purpose within [section 36(2)] for which the authorised person may exercise the power or

    (ii) in the case of the [section 39] power, a purpose within [section 39(2)].

39. **Regardless of the purpose for which this power is being used, there is no presumption that a device should be inspected. Inspection of a device should take place only where there is a properly identifiable foundation for the inquiry. Devices should be treated no differently from documents in this respect**[23].

40. The test as to what is 'reasonable belief' is an objective one. Any decision to extract information from a device must be made having considered all pertinent information

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

available at the time, taking into account the provenance and the accuracy of the information available and based on more than suspicion.

41. In addition to establishing 'Reasonable belief' where the [section 36] power is used for the prevention, detection, investigation or prosecution of a crime, authorised persons are bound by the following, relevant guidance.

42. **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 inquiry whether they point towards or away from the suspect.

43. As noted in the Attorney General's Disclosure Guidelines 2020 'What is 'reasonable' will depend on the context of the case. A fair investigation (In this context 'investigation' could relate to any purpose in [section 36 or 39]) *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 inquiry 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*[24].

44. **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.

45. The disclosure manual 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*.

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

Necessity and proportionality

47. [Sections 36(5)(b) and 39(4)(b)] require that even when the authorised person reasonably believes that information stored on the device is relevant to a purpose as above, they must also be satisfied that the use of the [section 36 or section 39] power is necessary and proportionate to achieve the purpose.

48. 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. The authorised person should consider the

[24] Attorney_General_s_Guidelines_2020_FINAL_Effective_31Dec2020.pdf (publishing.service.gov.uk)

value of the information extracted for the relevant purpose and where possible ensure that the amount of the information extracted is minimised, balancing the need for the information against the interference with an individual's (or individuals') right to privacy. The authorised person should record their rationale as to why the information extraction is necessary and proportionate in the circumstances.

Proportionality and Risk of obtaining other information

49. Key considerations when deciding if the use of the powers is necessary and proportionate are the impact on privacy of the device user and collateral intrusion on privacy of third parties whose information may also be extracted. Before using these powers, authorised persons should consider whether there are other less intrusive ways of obtaining the required information that do not involve the extraction of data from a device that would avoid intruding on the privacy of the device user or that of any third party whose information may be visible.

50. 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

51. An authorised person should consider exploiting other lines of enquiry that can provide the relevant material through less intrusive means. The judgement 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 screen shots or making some other suitable record, may meet the needs of the case[25]. 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 the other means available would be unreasonable in the circumstances. 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.

52. [Section 36 (6)(7) and Section 39(5)(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, then in order for the use of either power to be proportionate, an authorised person

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

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.

53. 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 means to obtain it. For example, if the information required is an image or recording of an event that took place in an area where CCTV cameras operate, could it be gathered this way? Or if it is a message between a victim and a suspect can it be obtained from a device belonging to a suspect?

54. If, after considering the necessity, proportionality and risk of obtaining other information, the authorised person is satisfied that use 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 up to date with the technology options available in their organisations and ensure they use those that offer the most selective extraction of information.

Sanctioning use of the powers

55. 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.

56. This procedure should include information about:

- The grade or rank of individual who should sanction any use of the powers ('the sanctioning officer'). The sanctioning officer should be at least one grade or rank higher than that of the individual requesting the extraction.

- The documentation that the sanctioning officer should complete in order to allow extraction including the record of how the request meets the obligations on use of the power set out in [36(1)(6)(7) and 39(1)(5)(6)].

- The procedure and the documentation that the sanctioning officer should follow in the case of an urgent oral authorisation to use the powers. 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 conditions under [36(1)] of the power is met. This is authorisation is distinct from the conditions which still need to be fulfilled for the use of the [section 36] powers. The person sanctioning the power should make a written record of their authority and the reason for it at the earliest opportunity.

- Where the use of the [section 36] 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 must be provided in writing before the extraction is commenced. If agreement cannot be provided in writing, then agreement may be given orally, and the authorised person must record the agreement in writing.

Recording the use of these powers

57. Authorised persons should record the relevant information and their rationale for their decisions to use these powers in writing (or where a request has been refused) to include points noted above, the relevant information sought, why the use of these powers is necessary and proportionate and what alternative options for obtaining the information have been considered, and if any were identified why it was not reasonably practical to use them.

58. In addition, and as per part 4 of this code, an authorised person should also record information related to obtaining agreement from an individual to use these powers including confirmation that agreement has been freely given without coercion and that the individual has been made aware of their rights.

Part 4: Voluntary provision of device and Agreement to extraction

59. This section gives guidance on the requirements in [section 36(1) of the Act] that a device user (or another person, in accordance with [section 37]) has voluntarily provided the device and has agreed to the extraction of information from it. This section includes guidance on:

- 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 it is freely given,
- the right of an individual to refuse to agree,
- 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), and
- recording agreement.

Definition of voluntary provision and agreement

60. The individual (either the device user or the person voluntarily providing the device and agreeing to extraction on their behalf, pursuant to [section 37]) should confirm explicitly and unambiguously, preferably in writing, that they are handing over their device voluntarily and agreeing to the extraction of information from it.

61. Voluntary means that the individual has not been pressured or coerced in any way by anyone (including an authorised person) to provide the device, and that the device has not been seized using any other lawful power.

62. Agreement means that a person has freely made an informed and conscious decision, without coercion in any way by anyone (including an authorised person) to the extent and nature of information to be extracted from a digital device.

63. An authorised person should give the individual information about the process of the extraction of information from their device to ensure they are fully informed before they make their decision to voluntarily provide the device and agree to the extraction of information from it. This should include:

- what specified information on the device is required
- why that information is required and, where using the power in section 36 for the purpose of preventing, detecting, investigating or prosecuting crime, how the information supports a reasonable line of inquiry
- why the authorised person believes it is necessary and proportionate to use these powers
- how the information will be extracted
- what information will be extracted including if information other than that which is required will be taken
- what will be done with the information and who will see it
- how any collateral information obtained will be managed
- when the device is likely to be returned to the user
- the individual's right to privacy and their right to refuse and what this will mean, including that refusal does not automatically mean that the case cannot go forward
- the individual can make a complaint to the controller[26] if they feel the request for information is excessive or that they have been coerced into providing the device and giving agreement.[27]

64. This could be done by providing a copy of the Digital Processing Notice (DPN), issued by the National Police Chiefs' Council (NPCC), which can be amended to meet the needs of different authorities where necessary.

65. Authorised persons must not coerce individuals to provide devices or agree to extraction of information from them. Those decisions must be freely made, and a refusal to provide a device and agree to the extraction of information from it should not automatically result in the closure of any enquiry or complaint.

66. In all cases, the authorised person should seek written confirmation from the individual that they are providing the device voluntarily and agreeing to the extraction of information from it, in the form of a DPN. The authorised person should explain the

[26] Refer to your own organisation's data protection policy for who has controller responsibilities

[27] In these circumstances the matter should be referred to the person acting as the 'controller' and local complaint procedures should be followed. Where the issue is not resolved to the person's satisfaction, they should be referred to the Information Commissioner's Office (ICO).

contents of the DPN to the individual and ensure they fully understand what will happen to the device and the information on it.

67. If there are exceptional circumstances and it is not possible to obtain written confirmation, the authorised person should secure and record verbal confirmation.

68. A record should be kept, even if confirmation was provided verbally, as it may be needed later to help show that the device was provided voluntarily, and agreement was given without coercion.

69. Further details about cases where the user is a child or adult without capacity are explained in part 4 of this code.

Withdrawal of agreement

70. 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 37]), 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 data from it can withdraw that agreement.

71. It should be made clear that withdrawal of agreement relates to the return of the device but, if agreement is withdrawn after the extraction of information has taken place, it may not be possible to delete or return all information. This is because of legal duties under the CPIA[28], which include disclosing to the defence any material that undermines the prosecution case or assists the defence unless the information is sensitive[29]. The extracted information must only be retained as long as necessary in line with each authority's data retention policies and other relevant guidance, for example CPIA and MoPI[30].

72. 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, including points after which it may not be possible, should be included in your organisation's version of the DPN as appropriate.

[28] See Part II of the Criminal Procedure and Investigations Act 1996 for disclosure requirements.

[29] See the Criminal Procedure and Investigations Act 1996 for the definition of what is deemed sensitive within the Act.

[30] See Criminal Procedure and Investigations Act 1996 (section 23(1)) Code of Practice (publishing.service.gov.uk) for the length of time for which material is to be retained & the College of Policing APP on Retention, review and disposal (college.police.uk).

[Section 37]: Cases where a device user is a child or adult without capacity

73. A child[31] or adult without capacity is not able to voluntarily provide a device to an authorised person or agree to the extraction of information from it for the purposes of [section 36 of the Act].

74. An alternative individual will be responsible for making these decisions on behalf of the child or adult who lacks capacity, ensuring their best interests are taken into account.

75. Detailed guidance on use of these powers with children and adults without capacity is set out in part 4 of this code.

[Section 38]: Agreement where the device user is missing etc.

76. 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

77. 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 36] 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).

78. 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 36] power so as to extract information from the device, without seeking agreement from the device user or someone acting on their behalf.

[31] [Section 36(10), Chapter 3 of Part 2 defines what is a child for the purposes of the Act].

Part 5: Use of the [section 36] power with vulnerable people

Vulnerable victims of crime

79. The purpose of this section is to offer guidance on what authorised persons should consider when using the [section 36] power with those victims who may be vulnerable due to the trauma they have experienced and who may need more support to make an informed decision as to whether they volunteer their device and agree to the data extraction from it.

80. The Victims code[32] for England and Wales[33] 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.

81. In this section we will focus on vulnerable victims of crime, but in all cases where an authorised person is considering exercising the [section 36] power, they should consider if a person is vulnerable and whether they may need more support to decide whether to provide agreement for their information to be extracted.

What constitutes a vulnerable victim?

82. There is no single legal definition of 'vulnerable'. For the purposes of the [section 36] 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.

83. The College of Policing have described a vulnerable person as "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".[34]

84. Many 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

[32] Code of Practice for Victims of Crime in England and Wales (Victim's Code) - GOV.UK (www.gov.uk)

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

[34] From the College of Policing (for England, Wales) training called 'Vulnerability-Look Beyond the Obvious'.

concerned. The authorised person should be mindful of hidden vulnerabilities caused through disability, shock or trauma.

85. Where a victim 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, for example, from a family member, a friend, or in a case of a sexual offence, from an Independent Sexual Violence Advisor, where this service is available.

86. The following may be used as a guideline for determining if an adult is vulnerable and whether they require additional, independent support in order to make a fully informed decision as to whether they agree to the extraction of data from their device. 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 personal involvement in it. If you are unsure whether an adult or child is vulnerable, it may be appropriate to assume that a level of vulnerability exists, particularly for victims of sexual offences or in the case where someone has been physically or mentally harmed.

    Examples of a vulnerable victim may include the following:

- Someone who has been the victim of a traumatic crime such as rape or serious sexual assault, or another type of violent crime.
- Someone who has been the victim of domestic abuse
- 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

87. Children and adults any without capacity cannot give agreement but should be treated as vulnerable. Authorised persons should follow the guidance set out in Part 6: Children and Adults without capacity.

88. Authorised Persons must follow any existing legislation and internal guidance regarding vulnerable victims as appropriate to the specific case, in addition to this Code of Practice.

Agreement and vulnerable victims

89. Victims of crimes such as rape and other serious 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.

90. Detailed guidance on what information to give to individuals to ensure that they are able to provide free and unambiguous agreement can be found in Part 4: Voluntary provision of device and Agreement to extraction.

91. An authorised person may need to go further to support and appropriately account for the needs of a vulnerable victim when exercising this power, for example:

- If an individual is in shock[35] 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 for the individual to regain their capacity before asking them to make decisions on these issues. (See also 'fluctuating capacity')

- The authorised person should consider whether to include an independent advisor, social worker, friend, family member or any person who can provide comfort and support to the vulnerable victim.

- Although a vulnerable person may seek support on the decision to volunteer their device and agree to the extracting of information from it, the decision that the authorised person follows must be the victim's. Only in cases where a victim is a child or an adult without capacity can the authorised person proceed with the decision of a person other than the victim.

- Wherever it is possible to do so, the authorised person should ensure the vulnerable victim has sufficient time to make these decisions.

- If, as a result of their vulnerability, the individual cannot understand the DPN, the authorised person may need to explain the form in simple terms, via their support representative (a person referred to in bullet two above) if needed. The authorised person may have to read the DPN out loud to the vulnerable victim, if they are unable to read or comprehend the material on their own.

[35] Information about the impact of trauma can be found in Psychological Evidence Toolkit - A guide for Crown Prosecutors | The Crown Prosecution Service (cps.gov.uk)

- If language is an additional barrier to understanding what is being asked of the person, an interpreter should be made available.

92. 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 as a result of engaging in an investigative process.

93. 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 victims

94. It is highly likely that a person's electronic device will contain sensitive personal information about them or other persons. Authorised persons should act in the knowledge that agreeing to the extraction of this kind of information will be an incredibly difficult experience, particularly where the person is vulnerable.

95. In all cases, before exercising the [section 36] power an authorised person should consider other methods for obtaining the required information. This is particularly important when there might be an acute privacy impact on a vulnerable victim.

Safeguarding and vulnerable victims

96. When exercising this power in relation to a vulnerable victim, there are certain measures that should be taken to ensure they are adequately safeguarded. For example:

97. 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 but believe they are in a consenting relationship with their attacker. In cases such as these, the authorised person will need to work carefully with the vulnerable victim and any supportive representative (such as a social worker, family member, etc), 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. The use of alternative powers should only be considered in extreme circumstances when it is necessary for the victim's safety.

98. 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 can be intimidating and some victims may feel better able to think clearly and consider their options if the discussion takes place at their home or in a neutral venue.

99. In all cases, authorised persons should aim to return a device as quickly as possible. In the case of a rape victim, ideally this should be within 24 hours of the device being taken. This 24-hour period starts only once the reasonable lines of enquiry have been established and the authorised person has considered alternative means of following the line of enquiry or of obtaining the required information. Once these criteria have been met the authorised person can seek agreement from the victim to extract the information from their device.

100. The information extraction authorised must be restricted to the specific information required to address the reasonable line of enquiry. Where due to technical limitations, the information extracted goes beyond what is required for the line of enquiry, this must only take place with the device user's agreement.

101. 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.

102. 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.

103. 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 replacement devices as appropriate according to their organisation's best practice.

104. All individuals may be eligible for assistance from their mobile phone provider, per Ofcom's vulnerable customer guidelines.[36]

105. A vulnerable victim and, if appropriate, their support representative (independent advisor, family friend etc) should be referred to the relevant services (social services, counselling, etc) if ongoing professional support is necessary.

[36] Treating vulnerable customers fairly: A guide for phone, broadband and pay-tv providers (ofcom.org.uk)

Part 6: Children and Adults without capacity

106. This part sets out who can make decisions on behalf of a child or an adult without capacity and what must be considered by the Authorised Person and by the alternative individual.

Children

107. For the purposes of [Chapter 3 of Part 2 of the Act], a child is a person under the age of 16[37]. Even if a child is deemed as having capacity according to the Gillick competence test, another person (as described below) 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?

108. The following individuals can make the decisions where the device user is a child whilst acting in the child's best interest.

- **A parent or guardian of the child**

109. 'Parent' includes biological parents, adoptive parents, and persons who have been granted legal parental responsibility for the child.

110. **In Northern Ireland,** this may also include parent or guardian or other persons or bodies with parental responsibility for the child within the meaning of the Children (Northern Ireland) Order 1995.

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

112. **In Northern Ireland,** 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

[37] Section 36(10).

Article 159 (Appointment by Court) or Article 160 (Appointment by parent or guardian).

- **If the child is in care, a person representing the relevant authority or voluntary organisation**

113. This should, unless not possible in the circumstances, be a person known to the child, or someone who has worked directly with the child, such as a social worker.

- **A responsible person**

114. Another responsible person must only be used as a last resort if nobody else is available to make the decision on behalf of the child. Authorised persons must make sufficient effort to get in contact with a parent, guardian or person representing the relevant authority responsible for a child. Best practice is to wait for a parent or guardian to be available to make the decision.

115. If there is any doubt on the suitability of a responsible other, the authorised person should consider the necessity and proportionately of the use of these powers again and if appropriate delay until a parent, guardian, representative of the authority or organisation which cares for the child or suitable responsible other can be found. Alternatively, the authorised person may seek alternative ways of obtaining the relevant information or consider proceeding without the device being provided voluntarily and without agreement to extract information from it, in accordance with section 38).

116. Authorised persons listed in [Schedule 3][38],cannot be a responsible other person where they are able to exercise the [section 36] power.

117. The responsible person:

- must be aged 18 or over
- should not be a suspect or person of interest in relation to the enquiry for which the power is being used
- must not be an authorised person who may exercise the power for the purpose for which information is being sought
- should ideally have an existing caregiving relationship with the child

[38] See annex A [Schedule 3] Authorised persons for persons listed in parts, 1,2 and 3.

118. A person who is an authorised person, but who may not exercise the [section 36] 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 36] power for that purpose – they may only do so for the purposes of preventing, detecting, investigating or prosecuting crime.

Views of the child

119. Before exercising the [section 36] 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 maturity[39]. They must have the child's best interests in mind.

120. This means that authorised persons should involve children where possible, especially those who are older or more mature, in the conversation about what information will be extracted from the device, what will happen to their device and to their information. Authorised persons should allow children who are able, to read the DPN, (or similar processing notice), and obtain their views along with those of the person making the decisions.

121. However, ultimately the decisions on whether to provide the device and agree to extraction are for the parent, guardian, person representing the authority or organisation in whose care the child is, or another responsible person.

122. In these cases, where the powers have been used where the individual is a child, authorised persons should record all relevant decisions including:

- if the child has been asked for their views and, if so, 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, and if so, why not
- the decision the authorised person came to on use of these powers (or not) and why.

[39] [Section 37(4)].

Adults without capacity

123. 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 decide to do the things mentioned in [section 36(1)(a) and (b) of the Act] (i.e. 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.

124. 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 matters mentioned in [section 36(1)(a) and (b) of the Act]. In this regard authorised persons must have in mind the principles set out in this act and the Code of Practice. [40]

125. 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 do the things mentioned in [section 36(1)(a) and (b) of the Act]. In this regard authorised persons must have in mind the principles set out in section 7 of the Mental Capacity Act i.e. the section headed “Establishing what is in a person's best interests…” this act.

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

126. The following individuals can make the decisions where the device user is an adult without capacity whilst acting in the person’s best interest:

- **A parent or guardian of the adult who lacks capacity**

127. ‘Parent’ includes biological parents, adoptive parents, and persons who have been granted legal parental responsibility for the child.

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

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

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

- section 64 of the Adults with Incapacity Act (Scotland) 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.

130. **In relation to Northern Ireland,** the term 'Guardian' should be interpreted according to the Mental Health (Northern Ireland) Order 1986.

- **If the adult without capacity is in care, a person representing the relevant authority or voluntary organisation**

131. This applies to individuals, who are in the care of a relevant authority or voluntary organisation.

132. This should, unless not possible in the circumstances, be a person known to the adult without capacity, or someone who has worked directly with the adult without capacity.

- **A registered social worker**

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

134. **In relation to Wales,** "registered social worker" means a person registered as a social worker in a register maintained by the Care Council for Wales.

135. **In relation to Scotland, ,** authorised persons should follow guidance on the role of the registered social worker in statutory interventions. The term 'social worker' should be interpreted within the meaning given in section 77 of the Regulation of Care (Scotland) Act 2001.

136. **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 within the meaning of that term as given in the Health and Personal Social Services Act (Northern Ireland) 2001.

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

137. **In relation to England and Wales,** this means a person with a lasting power of attorney which gives an 'attorney' the powers to make decisions on behalf of an individual who lacks capacity. Authorised persons should follow the relevant guidance here.

138. **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 - gov.scot (www.gov.scot).

139. **In relation to Northern Ireland**, this means

- Persons appointed as an Attorney under an Enduring Power of Attorney, within the meaning of the Enduring Powers of Attorney (Northern Ireland) Order 1987.; and / or
- Following the commencement of Part 5 of the Mental Capacity Act (Northern Ireland) 2016, persons appointed as an Attorney under a Lasting Power of Attorney within the meaning of that Part.

- **A deputy**

140. **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).

141. **In Northern Ireland**, a deputy may be appointed under section 113 of the Mental Capacity Act (Northern Ireland) 2016[41].

- **A person under an intervention order (Scotland only)**

142. S.53 of the Adults with Incapacity Act (Scotland) 2000 which defines a person authorised under an intervention order

- **A responsible person**

143. Another responsible person must be the last resort if nobody else is available to make the decision on behalf of the adult without capacity. Authorised persons must make sufficient effort to get in contact with a person named above before turning to another responsible person. Best practice is to wait for a someone in (a) to (e) to be available to make the decision.

144. If there is any doubt on the suitability of a responsible other, the authorised person should consider the necessity and proportionately of the use of these powers again

[41] At the time of preparation of this code, section 113 had not yet been commenced.

and if appropriate delay until a representative of the authority or organisation which cares for the adult or suitable responsible other can be found. Alternatively, the authorised person may seek alternative ways of obtaining the relevant information or consider proceeding without the device being provided voluntarily and without agreement to extract information from it, in accordance with [section 38]).

145. The responsible person:

- must be aged 18 or over
- must not an authorised person who may exercise the power for the purpose for which information is being sought
- should not be a suspect or person of interest in relation to the enquiry for which the power is being used
- should ideally have an existing caregiving relationship with the adult.

146. Others involved in the enquiry for which the power is being used such as the suspect, or person of interest cannot make the decision on behalf of the adult without capacity. In cases where the adult's parent or guardian is the suspect or person of interest to the enquiry for which the power is being used, authorised persons must seek another responsible person's agreement to take the adult without capacity's device and extract information from it or consider if the purpose meets the criteria for use without agreement as set out in [section 38].

147. A person who is an authorised person, but who may not exercise the [section 36] power for the purpose for which information is being sought, may act as a responsible other.

Views of the adult who lacks capacity

148. Where an authorised person assesses that a device user is an adult without capacity, the decision 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). But, the authorised person must where possible seek and consider the views of the device user to inform their decision making.

149. Some people's ability to make decisions fluctuates because of a condition that they have. In such cases, if possible, the decision as to whether to voluntarily provide the device and agree to the extraction of information from it should be made by the person 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. This means that, if further decisions need to be

taken in their best interests, the authorised person can take the person's wishes and feelings into consideration.

150. In these cases, where the powers have been used where the individual is an adult without capacity, authorised persons should record all relevant decisions including:

- the basis of the assessment that the adult lacks capacity
- the steps taken to explain the process to them and to seek (where possible) their views
- if the adult without capacity has been asked for their views and, if so, what those views were
- if the adult without capacity's 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, and if so, why not
- the decision the authorised person came to on use of these powers (or not) and why.

Part 7: Extracting Information

151. These powers allow an authorised person to extract information which is stored on an electronic device. As detailed in section 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 extraction method that will allow for the most selective extraction possible to allow the least amount of information needed to support the purpose, to be extracted.

152. Information may include photos, videos, text messages or documents which are stored on the device as well as systems data such as file directories and location information.

Applicable devices

153. 'Electronic device' means any device on which information is capable of being stored electronically and includes any component of such a device[42]. This includes mobile phones, computers and USB sticks[43].

Type of extraction

154. Technical capabilities vary between authorised persons. It is for the authorised person and forensic practitioner (if used) to determine the technical method of extraction to obtain the required information, and to limit the extraction of other information, bearing in mind the technical capabilities available. Some technology allows specific types of information to be targeted and extracted alone. However, other technology requires the extracting of all recoverable content on a device to enable a more specific review post-extraction, either manually or using search tools.

155. In many cases the authorised person is likely to be the decision maker as to the purposes and the means of the processing of the data, in these circumstances they will be acting as the 'controller', as defined in the DPA and the UK GDPR[44].

[42] [Section 36(10)].

[43] A small, piece of equipment that you can connect to a computer or other piece of electronic equipment to copy and store information.

[44] See the DPA 2018 and UK GDPR for the definition and responsibilities of the 'controller' and the 'processor'.

156. In the case where the authorised person is not the decision maker as to the purposes and the means of the processing of the data, they may be acting as the 'processor' as defined in the DPA and the UK GDPR[45], even if they are making technical decisions about how to process the data.

157. Authorised persons must ensure information extraction is not excessive, minimising intrusion into the device user's privacy and the privacy of others. Devices such as mobile phones can contain a lot of sensitive personal information which is often not relevant to the purpose for which extraction is required. Wherever it is possible to do so, bearing in mind the technology available to the authorised person, they should only extract the information which they require. For example, if an authorised person only needs to see photos taken on a certain date, they should aim to extract only those. This limits the impact on the device user's and others' privacy and means that there will be less information to analyse, therefore speeding up the enquiry or investigation.

158. In some cases, extracting a larger subset of information may be necessary to understand the specific information which the authorised person seeks to view. For example, viewing an entire conversation can put one message in context, and this may aid authorities to put together crucial evidence for their enquiry.

159. It is also important to note that some applications (such as some messaging applications) encrypt the information which is stored on the device. Each message will be stored in a database on the device along with all the other messages from the application. In order to view one individual message, it is likely that the authorised person would need to extract the full database and process the encrypted content in order to produce a readable version of the messages. This version can then be searched for a specific message. Any decisions on retention or deletion of the remaining information should be considered in line with relevant disclosure guidelines.[46]

160. 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.[47] Authorised persons in Scotland can find guidance in the Crown Office and Procurator Fiscal Service Disclosure Manual and authorised persons in Northern Ireland should refer to the Public Protection Service Code for Prosecutors.

[45] See the DPA 2018 and UK GDPR for the definition and responsibilities of the 'controller' and the 'processor'.

[46] For England and Wales -The Attorney General guidance on disclosure, for NI the Public Prosecution Service Code for Prosecutors' and for Scotland the COPFS Disclosure Manual Disclosure Manual - Page 3 (copfs.gov.uk)

[47] 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)

Definitions

Adult - a person aged 16 or over

Adult without capacity – an individual is without capacity if they are aged 16 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).

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 victim or witness, 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 16 years

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) the Care Council for 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)).

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.

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)

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).

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 data from the electronic device.

The authorised persons able to use the powers in [sections 36 and 39 of the Act] are listed in [Schedule 3 to the Act].

[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 36] 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 39] power, an investigation or inquest into a death.

Authorities listed in [**Part 2** of the Schedule] may exercise the [section 36] power for any specified purpose (these authorised persons may not exercise the [section 39] 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 36] power for the following specified purpose, (these authorised persons may not exercise the [section 36] power for other purposes or the [section 39] 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 36 OR 39]
A constable of a police force in England and Wales.
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 36] 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 36] 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)
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.
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, inquiry 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 inquiry.

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 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 DPA and UK GDPR for persons acting in their capacity as a 'controller' or a 'processor'.

'Controllers' exercise overall control over the purposes and means of the processing of personal data. In other words, you are acting as a 'controller' if you decide what data to process and why[48].

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

[48] See the DPA 2018 and UK GDPR for more details.

from the controller, if even if you make some technical decisions about how you process the data[49].

'Sensitive processing' under 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 document 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 document[50] in place.

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:

- necessary for judicial and statutory purposes – for reasons of substantial public interest;
- necessary for the administration of justice;
- necessary to protect the vital interests of the data subject or another individual;
- necessary for the safeguarding of children and of individuals at risk;
- personal data already in the public domain (manifestly made public);
- necessary for legal claims;
- necessary for when a court acts in its judicial capacity;
- necessary for the purpose of preventing fraud; and
- necessary for archiving, research or statistical purposes.

You must be able to demonstrate that the processing is strictly necessary and satisfy one of the conditions in Schedule 8. Strictly necessary in this context means that the

[49] See the DPA 2018 and UK GDPR for more details.

[50] For example, the NPCC Digital Processing Notice (DPN)

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, summarised below.

Article 5(1) requires that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) 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');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) 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');

(e) 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');

(f) 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')."

Article 5(2) adds that:

"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

Article 6 of the UK GDPR defines the lawful basis on which you can process 'special category data' whilst Article 9 defines the conditions for processing[51].

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

The UK GDPR defines 'special category data' as:

a) personal data revealing racial or ethnic origin;
b) personal data revealing political opinions;
c) personal data revealing religious or philosophical beliefs;
d) personal data revealing trade union membership;
e) genetic data;
f) biometric data (where used for identification purposes);
g) data concerning health;
h) data concerning a person's sex life; and
i) 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:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) 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;
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e) 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;
f) 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:

1. 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.

2. Paragraph 1 shall not apply if one of the following applies:

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

a) 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;

b) 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;

c) 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;

d) 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;

e) processing relates to personal data which are manifestly made public by the data subject;

f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g) 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;

h) 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;

i) 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;

j) 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.

[Final page of the guidance is intentionally left blank]