



**HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE**

Response Date: 13/06/2025

2025/511 - Digital extraction policies and practices in RASSO investigations

In response to your recent request for information regarding;

We are conducting research into police practices concerning the extraction of digital data from victims of rape and serious sexual offences (RASSO), particularly in light of the updated statutory framework introduced by the Police, Crime, Sentencing and Courts Act 2022 and the associated Code of Practice.

Specifically, we request disclosure of the following information:

1. Policies and guidance

a. Please provide copies of any current internal policies, procedures, guidance documents, or internal forms used by your force in relation to the extraction of digital data from victims or witnesses in RASSO investigations.

DPNa, DPNb, DPNc, LIMA Application.

Please find attached copies of DPNa and DPNb.

DPNa - This is to be completed when a device is taken from a victim or witness. It also serves as a guidance document to police investigators who are taking possession of the device.

DPNb - This notice should be provided to victims and witnesses when police take possession of their device.

DPNc - This is to be completed when a device is taken from a suspect.

b. Please provide copies of any standard forms, information packs, or other materials provided to victims or witnesses when requesting access to their mobile phones or proposing a download of their data.

Please find attached copies of DPNa and DPNb.

2. Compliance with new legal framework

a. Has your force adopted the new Code of Practice issued under section 37 of the Police, Crime, Sentencing and Courts Act 2022? If so, please provide the date of adoption and any associated implementation documents.

DPNa,b,c - Section 37 of the Police, Crime, Sentencing and Courts Act 2022 allows authorized persons to extract information from electronic devices used by a victim or witness if they voluntarily provide the device and consent to the extraction. This power can be used for purposes such as preventing, detecting, investigating, or prosecuting crime, locating a missing person, or protecting vulnerable individuals from harm. We do not hold the date of adoption, we've used them for quite some time.

Pencadlys yr Heddlu,
Glan-y-Don, Bae Colwyn LL29 8AW
www.heddlugogleddcymru.police.uk

Police Headquarters,
Glan-y-Don, Colwyn Bay LL29 8AW
www.northwales.police.uk

b. Has your force issued any training or operational guidance to officers on the use of the Code and the new statutory framework? If so, please provide details (including training materials if available).

We have been using the DPNa forms for some time now. Guidance is sent out by Digital Forensic Unit (DFU) and there is a Sharepoint page containing instructions and useful information.

This is not currently covered in detail regarding the individual forms in Initial Training.

3. Technology and digital extraction tools

- a. What tools or software systems are currently used by your force to extract digital data from mobile phones in the context of RASSO investigations? Are these tools used consistently across all RASSO cases?**
- b. Are these tools configured to allow selective extraction (i.e. only of relevant material), or are they routinely used for full downloads?**
- c. Has your force conducted any audits or reviews of the use of digital extraction tools since the introduction of the new legislation and Code of Practice?**

a. Two software systems are used consistently across RASSO DFU follow SOPs. Concerns have been raised in disclosing the names of the software systems in to the public domain. A Freedom of Information Act request is not a private transaction. Both the request itself, and any information disclosed, are considered suitable for open publication. This is because, under Freedom of Information, any information disclosed is released into the wider public domain, effectively to the world and not just to one individual.

Therefore, Section 31 (1) (a) Law Enforcement is to be considered as part of the Public Interest Test. A Public Interest Test has been carried out to weigh up the reasons for and against disclosure of the information requested, to ensure the release is in the interest of the public as a whole and not just the applicant.

Section s31(1) Law Enforcement

Section 31 (1) is a prejudice based qualified exemption, therefore there is a requirement to articulate the harm that would be caused in confirming or not that the information is held as well as carrying out a public interest test.

The Harm Test process requires North Wales Police to consider any possible harm that might arise as a result of placing the requested information into the public domain. This process considers the potential harm to:

- Individuals
- The community as a whole
- North Wales Police and the wider policing service
- Other bodies

Harm in respect of s31(1) Law Enforcement

To disclose particular policing tool of this type used by North Wales Police as part of an investigative process could reveal operational tactics linked to policing, compromise police investigations and/or adversely affect the ability of North Wales Police and others to safeguard national security.

It is well established that police forces utilise Digital Forensic techniques in order to counteract criminal behaviour, detect crime, and assist in the apprehension and prosecution of offenders. Modern day policing is intelligence led and law enforcement depends upon the development of intelligence and the gathering and security of evidence in order to disrupt criminal behaviour and bring offenders to justice. As criminals adapt and exploit new technology, the police need to respond by overcoming hi-tech barriers in order to meet their responsibilities. In this case the information relates to a service provider and by extension their products for the extraction of data from devices.

By revealing specific tactical information such as requested within this request, it would undermine the process of preventing or detecting crime and the apprehension of prosecution of offenders. When considered on a Force by Force basis, a malign individual could identify those most critical to the Law-and-Order sector and specifically target those providing the most assistance. This would have a huge impact on the effective delivery of operational law enforcement as it would leave companies open to further cyberattacks which could have devastating consequences for law enforcement.

Public Interest Test:

Factors favouring Disclosure – Providing the names of software would provide the public with information about technologies and North Wales Police capabilities. This would reinforce the wider commitment to openness and transparency with the general public and facilitate public debate. Furthermore, owing to the inherent link between transparency and public confidence, would likely to improve the general public's confidence. Over time, an increase in public confidence would be likely to improve public engagement with the police. This would, in turn, lead to an improvement in our ability to both prevent and detect crime, and apprehend and prosecute offenders.

Factors favouring Non-Disclosure – Disclosing the names of Software used would provide our capabilities to persons intent on disrupting their work, with information that would assist them to do so. In this case, for the reasons outlined in the evidenced harm, the effectiveness of current and future strategies when carrying out investigations and gathering evidence may be compromised. The safety of the public is of paramount importance to policing purposes, and any increase in crime would place the public at risk of harm. When the current or future law enforcement role of the force may be compromised by the release of information, the effectiveness of the force will be reduced. The personal safety of individuals is of paramount importance to the Police Service and must be considered in response of every release. A disclosure under Freedom of Information is a release to the world and, in this case, disclosing tactical information relating to the extraction of data from computers and other devices, would undermine the evidence gathering process of any investigative inquiry relating to offences, some of which may be serious cases such as murder or rape.

Balance Test

Having considered the reasons why North Wales Police should disclose the software systems used, although openness and transparency is at the forefront when considering the public interest, in this case disclosure relating to Digital tools used by the police for investigative purposes would not be in the public interest.

The public entrust the Police Service to make appropriate decisions with regard to their safety and protection and the only way of reducing risk is to be cautious with any information that is released. Disclosing the systems used would reveal specific policing activity in the digital sphere of investigations and would assist those intent on causing harm. This would directly harm the ability of the force to investigate crime. This could also reveal police capabilities, compromise police investigations and/or otherwise. I have attached considerable weight to these interests as the primary role of the Police Service is to both prevent and detect crime and apprehend those responsible for committing criminal offences.

Therefore, at this moment in time, it is our opinion that for these issues the balance test for confirming, nor denying, that information is held is made out.

Therefore, in accordance with the Freedom of Information Act 2000, this letter acts as a Refusal Notice under section 17 (1) of the legislation.

- b. Predominately complete full extractions but DFU only supply what is justified and proportionate to the frontline.
- c. No information held

4. Oversight and accountability

- a. Does your force have a panel or mechanism for reviewing RASSO cases where a victim or witness has challenged a request for access to their digital data? If so, does that panel or mechanism remain in place?

Frontline officers should only request a device where the victim cannot supply the data by other means e.g. via NICE Investigation citizen link. We wouldn't seize if they didn't consent.

- b. Does your force collect internal data on how many times digital data has been extracted from victims or witnesses in RASSO cases in the past two calendar years? If yes, please provide those figures.

Calendar Year	Count of DPNa
2023	59
2024	51
2025	7
Grand Total	117

Fiscal Year	Count of DPNa
2022	12
2023	59
2024	45
2025	1
Grand Total	117

- c. Has your force received any complaints about mobile phone data extraction practices from victims or witnesses in RASSO investigations during the last two years? If so, please provide the number of such complaints.

No

THIS INFORMATION HAS BEEN PROVIDED IN RESPONSE TO A REQUEST
UNDER THE FREEDOM OF INFORMATION ACT 2000, AND IS CORRECT AS AT 30/05/2025



HEDDLU GOGLEDD CYMRU NORTH WALES POLICE

**Police, Crime, Sentencing and
Courts Act 2022,
Part 2, Chapter 3 Electronic Device Extraction
User
Digital Processing Notice (DPNa)**

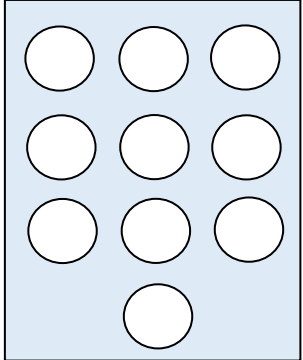
To be completed by the officer taking possession of the electronic device.

*A separate form must be completed for each device.
Provide a copy of section 1 to the user /person providing agreement once
complete.*

*Throughout this form the term 'user' means the person who ordinarily uses the
device.*

Section 1 Device information

Crime report No:		
OIC Details		
Station / Department / Team		
Name & Shoulder No		
Device Details		
Exhibit Ref		Device

Property Ref				Pattern Lock Indicate beginning and end
Telephone No(s)				
Make of Device		Model		
Data Card present	Yes/No	No of Cards		
SIM Present	Yes/No	SIM PIN Code		
Device Pass Code				
Description of device condition (i.e. damage or faults, last used)				

The purpose and power

(This section explains the lawful power being used to extract the required information)

Lawful power being utilised	Sub-section	Indicate which sub-section you are utilising.	Has the user or their representative agreed to provide the device for extraction (yes/no)?
Police, Crime, Sentencing and Courts Act 2022 Section 37(1).	(2)(a) Preventing, detecting, investigating or prosecuting crime.		
	(2)(b) Helping to locate a missing person.		
	(2)(c) Protecting a child or an at-risk adult from		
Note: An adult is an at-risk adult if you reasonably believe that they are experiencing, or at risk of, neglect or physical, mental or			

emotional harm, and they are unable to protect themselves against the neglect of harm or the risk of it.	neglect or physical, mental or emotional harm.		
--	--	--	--

When the user has not agreed / is unavailable/ is unable to provide the device and/or to the extraction, indicate which of the following conditions are met: (mark with an X)

Police, Crime, Sentencing and Courts Act 2022 Section 40(1).	Condition A – a person who was a user of the electronic device has died and the person was a user of the device immediately before their death.	
	Condition B - a user of the electronic device is a child or an adult without capacity, and you reasonably believe that the user's life is at risk or there is a risk of serious harm to the user. Note, Harm may also include financial abuse or coercive control	
	Condition C - a person who was a user of the electronic device is missing, they were a user of the device immediately before they went missing, and you reasonably believe that the person's life is at risk or there is a risk of serious harm to the person. Note, you must reasonably believe they were a user of the device	

Indicate here if you are utilising the alternative power under Section 41:

Extraction of information from electronic devices for investigations of death:	
--	--

• A person who was a user of the electronic device has died, and the person was a user of the device immediately before their death. (‘Immediately before they died’ means that they were the user of the device around the time of their death.) This power may be exercised only for the purposes of an investigation into the person’s death under Chapter 1 of Part 1 of the Coroners and Justice Act 2009.	
---	--

The information

(This section explains what information is sought and why it is strictly necessary and proportionate to obtain it for the investigation/purpose)

What information is requested from the device?
<i>What information are you looking for? Be specific. For example, WhatsApp messages between person A and person B between set dates in which the offence is discussed.</i>

I reasonably believe that information stored on the electronic device is relevant to a reasonable line of enquiry / the purpose because:
<i>Explain the offence(s) under investigation or the circumstances, and the basis for your belief that information is on the device. This will either be to follow a reasonable line of enquiry if investigating a crime, or for the purpose of extraction, i.e. locating a missing person or protecting a child or at risk adult:</i>

Why it is strictly necessary and proportionate to extract the information

Explain why the information is strictly necessary in light of the reasonable lines of enquiry or the purpose you have identified above.

You must have considered the risk of obtaining other information that is not being targeted and collateral intrusion.

Explain what alternative less intrusive methods of obtaining this information have been considered, and if available, why it is not practicable to use them. Specify how the information will be reviewed to minimise intrusion, yet secures the information sufficiently. Always consider an incremental approach where possible, and extraction from a suspect's device should always be considered first.

Confidential material

You must assess whether there is a risk of obtaining confidential information.
(See FAQs for an explanation and guidance on confidential information)

Has the device user been asked whether there is likely to be confidential information on the user's device? if so, what was their response?

Do you expect to find confidential information on the device? If so, how will you proceed?

Extraction time period:

Record how long the user is likely to be without their device

The time-period the user will be without their device will be dependent on force capability and capacity. If you cannot be precise, you must provide the device user with an approximate time-period.

Volunteered devices and agreement

(This section is where the device user agreement is recorded - see below for children or adults without capacity)

User of device			
Name:		DOB:	
Declaration	I have voluntarily provided the digital device, and; I have agreed to the extraction of information specified within this notice from it. I am aware I am entitled to a copy of section 1 and a DPNb. I am aware that I can refuse this request and that the enquiry will not be brought to end merely because of this refusal.		
Signature:			
Time/date:			

If utilising Section 37 powers and the user of the device has given oral agreement only (due to physical impairment or lack of literacy skills), you must record that here

Note, you should ask whether they wish to have another person present, such as a family member or friend, to ensure the oral discussion accurately reflects what is in the written notice

Reason for requiring oral authorisation and confirmation that it has been given.	
Time/date:	

Volunteered devices and agreement on behalf of a child or an adult without capacity

(This section is where the agreement is recorded on behalf of a child or an adult without capacity)

The alternative Individual where the device user is a child or an adult without capacity			
Name:		DOB:	
Declaration	I have voluntarily provided the digital device, and; I have agreed to the extraction of information specified within this notice from it. I am aware I am entitled to a copy of section 1 and a DPNb. I am aware that I can refuse this request and that the enquiry will not be brought to end merely because of this refusal.		
Signature:			
Time/date:			

Views of a child or adult without capacity In cases where the user is a child, you should record: • if the child was asked for their views, what those views were;

- if the child's views differed from the views of the person providing the device and agreeing to the extraction of information from it;
- if the child was not asked their views, why not;
- the decision the alternative person came to on use of the power and why.

In cases where the user is an adult without capacity, you should record:

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

Device not volunteered and agreement not given

(This section is to record the reasons the user or the alternative individual gave if they refused to volunteer the device or provide agreement for extraction.)

Record the reasons that the user / the alternative individual gave for not volunteering their device or agreeing to extraction. This section only needs to be completed when you utilise a condition under Section 40.

Urgent Oral Sanction

(This section is where the authorised person records why an urgent oral authority to examine a device is needed and the decision from the sanctioning officer).

An urgent oral sanction can only be sought when there is a real and immediate risk of serious harm to a person and the other requirements for use of the power in Section 37 are met. For the conditions that need to be met to examine a device urgently without the agreement of the device user, see section 40 of the PCSC Act.

Urgent oral sanction sought and why it is urgent
<i>Record what the risk is and the reason for seeking urgent sanctioning of extraction.</i>

Sanctioning Officer response to an urgent oral request
<i>If the Sanctioning Officer gave urgent oral authorisation for extraction, then record the extent of that extraction and the details of the Sanctioning officer.</i>

Section 2

Sanctioning the Extraction

To be completed by the authorising Inspector

Authority Required from	Inspector
-------------------------	-----------

Authority to extract	
Is the device lawfully in police possession? (Does the PCSC Act allow for extraction in the given circumstances)	Yes/No If no, detail below what action you have taken
Has the device been interfered with or interrogated in any way? (By police)	Yes/No Explain:
Did you urgently sanction an extraction? (Note, this is available when there is a real and immediate risk of serious harm to a person)	Yes/No
If the device user has provided oral agreement only, confirm here whether you consider this appropriate and why.	

I have considered the following in relation to this authorisation:

- Section 1 is completed accurately and contains the required information and considerations;
- Less intrusive means of obtaining the required information have been appropriately considered, and where precluded, an appropriate explanation provided;
- Whether a DPNb has been provided to the device user and/or the alternative individual providing agreement;
- Whether the right support was provided to the device user so that I can be confident that the person providing agreement fully understood the request, and that the device was lawfully volunteered and agreement freely given

(Note, if you orally sanctioned extraction you should record the reason why, and what extent of extraction was sanctioned)

Having considered the above I authorise/reject this request for extraction:

Comment here

Name		Signature	
Time & Date authorised			

Section 3

Guidance for officer completing the form – FAQs

What does extraction mean?

If you are utilising the PCSC Act, then the term 'extraction' includes the reproduction of digital information or data from a device in any form. This includes taking screenshots by any method, which would include making a written note or taking a photograph.

Extraction does not mean receiving copies of digital information, such as a screenshot taken by the device user and sent to you by e-mail, for example.

When can I extract information from the device of a user?

You must have a reasonable belief that information on the device is relevant to a reasonable line of enquiry / the purpose.

The test as to what is 'reasonable belief' is an objective one. Any decision to extract information from a device should consider all pertinent information available at the time, taking into account the provenance and the accuracy of the information available and should be based on more than mere suspicion or speculation.

For the purposes of preventing, detecting, investigating, or prosecuting crime you must reasonably believe that information on the device is relevant to a reasonable line of enquiry.

If exercising the power to help locate a missing person, for the purposes of protecting a child, or an at risk adult from neglect or physical, mental or emotional harm, or for investigating a person's death, you must reasonably believe that information stored on the device is relevant to that purpose

Further guidance on communications evidence can be found here:

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

What is the lawful basis for taking possession of the device and extracting the information?

You will be relying on the electronic device extraction power in Part 2, Chapter 3 of the Police, Crime, Sentencing and Courts Act 2022. This Act is applicable to the extraction from an 'electronic device', which means any device on which information is capable of being stored electronically and includes any component of such a device. (Data on the 'cloud' is not included).

The law allows you to take possession of the device when the device user has provided their agreement for you to do so. However, the device user must be informed of the information you are seeking from the device before they agree to provide it.

The powers in Section 37 may be used for the purpose of:

- 37(2)(a) Preventing, detecting, investigating or prosecuting crime;
- 37(2)(b) Helping to locate a missing person, or;
- 37(2)(c) Protecting a child or an at-risk adult from neglect or physical, mental or emotional harm.

If agreement has not been provided by the device user or representative, you can only extract information from it when one of the conditions A-C applies (as set out in the table in section 1 above). If one of the conditions exists, you can take possession of the device to extract the information.

Data Protection Act 2018

The PCSC Act allows for law and non-law enforcement purposes.

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

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

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

If extracting for non-law enforcement purposes – for example, to help locate a missing person or to protect a child or an at-risk adult from neglect or physical, mental or emotional harm (where no criminal element exists), or for the purposes of certain non-criminal investigations or inquests into the person's death - you will process under the UK GDPR. When extracting information for non-law enforcement purposes, the seven principles under Article 5 of the UK GDPR need to be met and Article 6 of the UK GDPR defines the lawful basis on which you can process the data. As we expect to process 'special category data' Article 9 of the UK GDPR also applies.

In every case when assessing if it is necessary and proportionate to extract information and process information you should balance the benefit of extraction with the likely intrusion into the users privacy and the privacy of others whose information is stored on their device.

When should I use the PCSC Act?

It is expected that the digital device extraction power contained in the PCSC Act will be utilised when forensically extracting information from personally held digital devices. Whilst there are other use cases, this will usually be devices provided by victims and witnesses.

If merely making a note or taking a photograph of information from a device screen that has been volunteered to you, then it is unlikely there will be a need to make use of any power in these circumstances. However, if making a note or taking an image of 'personal information' as defined by the UK GDPR, then there must be observation of Data processing legislation.

Where can I obtain further information about how I should utilise the PCSC power?

The DPNa and DPNb adhere to the Code of Practice that accompanies the PCSC Act. The Code of Practice can be accessed here:

[Extraction of Information from electronic devices: code of practice](#)

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

Yes, unless the conditions under s40 apply. You will need the device user, or their representative (in the case of child or adult without capacity), to volunteer the device and agree to the information extraction.

This agreement must be signed for on this DPNa, unless they cannot sign because of their physical impairment or lack of literacy skills, then agreement may be given orally. In this instance the device user should be asked whether they wish to have another person present, such as a family member or friend, to ensure the oral discussion accurately reflects what is in the written notice. You must record the agreement in the space provided.

You must not have placed any undue pressure on them and be satisfied that they have not been coerced by anyone. 'Undue pressure' means making the person feel as though they do not have a choice about volunteering the device and agreeing to extraction.

The NPCC position is that the PCSC Act should be used when dealing with digital devices belonging to victims and witnesses. There should be limited circumstances when alternative coercive powers are used on victims and witnesses and only when you reasonably believe that life is at risk, or there is a risk of serious harm, and that the risk cannot be mitigated by less intrusive means. When alternative powers are used a DPNc should be completed instead of this notice.

In all cases, you must consider the individual's needs and vulnerabilities and take the action necessary to provide them with the support needed to understand what it is they are being asked to agree to and why. 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. Remember that the user may be supported by a number of different professionals during this process, for example, a language interpreter, an intermediary, an Independent Domestic Violence Advisor (IDVA), or an Independent Sexual Violence Advisor.

Whose agreement do I need if the user is a child or adult without capacity?

A child or an adult without capacity is not able to voluntarily provide a device or agree to the extraction of information from it for the purposes of Section 37 of the Act.

An alternative individual will be responsible for making these decisions on behalf of the child or adult without capacity.

For a child (anyone under the age of 18):

A parent or guardian, or a person representing a relevant authority or voluntary organisation, or if those are unavailable, as a last resort a responsible person, who must be 18 or over.

For an adult without capacity:

A person is an adult without capacity if, within the meaning of the Mental Capacity Act 2005, they lack capacity. You should adhere to the principles in Section 1 of the Mental Capacity Act 2005.

A parent or guardian, or a person representing a relevant authority or voluntary organisation, registered social worker, someone who has power of attorney, a deputy appointed under section 16 of the Mental Capacity Act 2005 or if those are unavailable, as a last resort a responsible person, who must be 18 or over.

For both a child and adult without capacity:

Unless inappropriate to do so, you must contact a parent, guardian or person representing the relevant authority or voluntary organisation, (or in the case of an adult without capacity, a registered social worker, someone who has power of attorney or a deputy appointed under section 16 of the Mental Capacity Act 2005) before turning to another responsible person.

Best practice is to wait for such a person to be available to make the decisions.

Where the decisions have been made on behalf of the child or an adult without capacity by a responsible person, you must, unless you consider it is inappropriate to do so, notify a parent or guardian that the power has been used and for what purpose. This notification should be made as soon as possible. Where it is not appropriate to notify a parent or guardian because they are a suspect in the investigation, or where you believe that revealing information has been extracted will put the user at risk, you should consider notifying another parent or guardian.

Before exercising the Section 37 power, you must, so far as it is reasonably practicable to do so, ascertain the views of the user and have regard to any views so ascertained, taking account of the child's age and maturity / conditions that affect their capacity.

You should ensure that an explanation has been provided to the user as to what will happen to their information and device and that, whilst their views will be taken into account, it is only an adult who can make decisions on their behalf. You should confirm that the person making the decisions on behalf of the user is aware of their views, and has taken into account the views they have on this matter. The adult may still decide to provide (or to not provide) the device and agree (or not agree) to the extraction of information from it having had regard to the views of the child's / adult without capacity, and when doing so, they must be acting in the best interests of the child / adult without capacity.

If the user agrees, how should I review the information?

Once you have identified that it is a reasonable line of enquiry, and either the user has agreed to extraction or you are utilising a condition A –C, you need to consider how you will review the information.

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

- What information do I want to review? Can I do this without taking the device from the user?
- Have I already obtained the same information from a suspect's device? If so, do I still need to examine the user's device? Is corroboration required?

- Manual examinations of devices, including screen shots, may be considered in certain circumstances.
- If you are unsure which method of capture to use, seek forensic advice.
- You should consider a manual examination, including screenshots, without taking the device away only when:
 1. There is minimal information and it is unlikely to be of significant evidential value;
 2. Information on devices could be lost if not captured immediately;
 3. Volatile information is present, i.e. data that might be lost if the device is turned off, or;
 4. Having carefully sought to persuade the user to provide their device, reassured them of its handling and explained to them the potential consequences of refusing to provide it, you find the user still chooses not to do so, leaving screenshots as the only available option to secure some record of the information. This might be the case if the user will not allow you to take the device but will allow screenshots to be taken.
- If you capture information using manual examination, you should make clear in the case file: (1) that this method was used; and (2) your reasons for believing that screenshots provide the only remaining way of recording the information in the circumstances.
- If you capture information using manual examination because this is all the user will agree to, you should make clear in the case file your efforts to persuade the user to provide their device and their reasons for not doing so. This should be included in their witness statement, if one is provided.
- If the conditions for manual examination are not met then you will need forensically to extract the information from the device belonging to the user. The contents should be extracted with minimum inconvenience and the device returned without unnecessary delay.
- You should extract and/or search only for the information relevant to the line of enquiry / purpose. Wherever possible, you should also specify the time-frame that is likely to be relevant, and set specific start and end dates before searching for and/or acquiring information. If you are using search terms to review the information, these must be recorded. You should advise the user that you have set these parameters, together with your rationale.
- Technology used to acquire information from devices is developing all the time, as are the devices themselves. Some technology will enable specific types of information to be targeted. However, some requires the copying or acquisition of recoverable content on a device to enable a more specific review either manually or using search tools. Whatever technology is used, you must seek only information that enables the review of what is strictly necessary as identified on this form and agreed with the user.
- Wherever possible, you should delete any information acquired from a device that is outside of the parameters agreed with the user. This includes

information that has not been reviewed following the deployment of search tools.

- If you need to complete another extraction as the parameters agreed with the user have changed, you should seek to reacquire their device and complete a new DPNa.
- It may not be possible to delete information from the master copy if it is inextricably linked to relevant information and/or doing so would adversely affect the provenance and/or integrity of the information should it be subject to challenge at a later date. This may be the case if the information is held on a disc or encrypted file, for example.
- In these circumstances any working copy created should consist only of the information deemed to be relevant.
- The master copy must be kept securely. Additional safeguarding measures to prevent inappropriate access, review or disclosure of the information should be implemented and highlighted within the <insert Sensitive Processing Appropriate Policy Document>

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

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

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

What should I tell the user about the process?

You should provide the user with the DPNb 'user information sheet.' It is important that you communicate clearly and ensure the user understands their right to privacy

and where they can access further information. Whilst this sets out general information you need to tell the user the following, which will be relevant to the case:

- The legal basis and justification for processing to take place (that for crime the extraction is performed in pursuance of a reasonable line of enquiry in accordance with the CPIA 1996 and which power is being used); explain what information you are seeking, which areas of their device will be looked at, and what particular dates or time-period you will be reviewing, as set out in this form;
- Reassure the user that their device will be examined only to the extent necessary to pursue the reasonable line of enquiry and that otherwise the contents will not be looked at;
- Tell the user the length of time they will be without their device (which should be kept to a minimum) using your best estimate;
- Give the user a copy of section 1 of this form once complete if the device *has been volunteered and agreement obtained*. (If utilising condition B or C in Section 40 then only a DPNb needs to be provided);
- Keep the user informed as to the use of their information throughout the course of the investigation, according to the extent to which the user wishes to be provided with updates. This should be agreed and recorded in your crime report/enquiry log;
- If investigating crime, explain that the relevant information will be revealed to a prosecutor only if investigative/charging advice is sought or an offender is charged with an offence;
- If investigating crime, explain that information will be provided to the defence only if it meets the strict test for disclosure and that it will be served in a suitably redacted form to ensure that personal details or other irrelevant information are not unnecessarily revealed (e.g. photographs, addresses or full telephone numbers);
- Tell the user about their right to privacy and signpost them to the Sensitive Processing Appropriate Policy Document.

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

If this happens, it is important to understand the reasons. Offer reassurance in line with the guidance above. It is important to ensure that the user is not, and does not feel, unduly pressured. If you are concerned that the user does not fully understand the process, consider the use of a support service or an intermediary. If the user maintains their position, record their reasons.

Section 40 condition B of the PCSC Act allows you to take possession of the device to complete extraction if a user of the electronic device is a child or an adult without capacity, and you reasonably believe that the user's life is at risk or there is a risk of

serious harm to the user. (Harm may also include financial abuse or coercive control).

Alternatively you can consider other powers, however the use of coercive powers to obtain devices containing personal or sensitive information from victims and witnesses, for example the powers of seizure under PACE, should be rare, and when you reasonably believe that life is at risk, or there is a risk of serious harm. If an alternative power is used complete a DPNa, not a DPNa.

If the device is not volunteered or obtained when investigating crime, explain to a victim or witness that if the police are unable to pursue this enquiry:

1. a witness summons might be issued, or;
2. a prosecution might be unable to proceed.

Explain to the user that they must not delete potentially relevant information from their device and that if they do so this might prevent the police from carrying out a fair investigation which could result in the investigation being closed. You should record that this information has been given.

If investigating crime, you should seek to take a statement from the user explaining in detail what information exists and why they will not allow the police to examine their device. This statement should then be included in any file that is submitted to the CPS and, if applicable, disclosed to the Defence.

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

How do I manage a device that has been seized before the PCSC Act could be considered or utilised?

There may be occasions when the Police come into lawful possession of a device, and it is later established to belong to a victim or witness of crime. An example of this is a phone seized during a house search, or from a suspect upon arrest.

In these circumstances you should approach the victim or witness with a view to obtaining agreement to extract information in line with Section 37(2)(a). Should agreement be forthcoming then you would revert to utilising the PCSC Act and complete this DPNa form.

Should the victim or witness not agree, then there would be reliance on the original power for seizing the device and you should complete a DPNa as appropriate.

The NPCC expect that continued retention of a victim or witness' device and extraction against their agreement should only occur when you reasonably believe that life is at risk, or there is a risk of serious harm.

When can I utilise S41 for Death Investigations

You can utilise S41 when conducting a non-criminal investigation into a death on behalf of the Coroner.

The purpose of an investigation into a person's death is to ascertain:

- (a) who the deceased was;
- (b) how, when and where the deceased came by his or her death;

The purpose of extracting information from the device must be in order to ascertain information to support (a) or (b).

What is 'confidential material' and how do I approach it?

'Confidential information' is:

- Confidential journalistic information - information created or acquired for the purposes of journalism which is held in confidence (or which, in the case of information in a communication, the sender holds in confidence or intends the recipient to hold in confidence).
- Protected information, which is:
 - Items subject to legal privilege - Certain communications between a professional legal adviser and their client (or between such a person and others).
 - Personal records and other information acquired or created during the course of a trade, business, profession or occupation (or for the purposes of any office) which are held in confidence.

If you are not intentionally seeking confidential information, you must nevertheless assess whether there is a risk of obtaining confidential information if you carry out extraction of data from the user's device. This will require you to explain to the user what 'confidential material' is, and ask the user whether there is confidential information on their device. You must also apply your own mind to the question of whether there is a risk that extraction will include confidential information.

If you assess there to be no risk of obtaining confidential information then you may continue with the extraction.

If you think that there is a risk of obtaining confidential information, you should go on to consider four further matters:

- (1) The type of confidential information likely to be stored on the device
- (2) The amount of confidential information likely to be stored on the device
- (3) The potential relevance of that information to the purpose(s) for which you are extracting the information.
- (4) Whether there are other means of obtaining the information sought which do not risk obtaining confidential information and be satisfied that (i) there are not, or (ii) if there are, it is not reasonably practicable to use them.

You must determine whether the confidential information is likely to be relevant to the reasonable line of enquiry that you are pursuing. For example, where a victim of a sexual assault has correspondence on their device with a solicitor relating to the sale of a property, this is confidential information, but is not relevant to the investigation. However, correspondence between the device user and a legal professional regarding a criminal allegation made by the victim which the police are investigating is confidential information and may be relevant to the investigation.

If your conclusion is that there is a risk of obtaining confidential information which is not likely to be relevant to the reasonable line of enquiry that you are pursuing and that the amount of confidential information is likely to be large, then you should follow the guidance in paragraphs 29 – 33 of the Attorney General's Guidelines on Disclosure Annex A.

If your conclusion is that there is a risk of obtaining confidential information which is not likely to be relevant to the reasonable line of enquiry that you are pursuing but that the amount of confidential information is likely to be minimal, then you may proceed with the extraction.

If your conclusion is that there is a risk of obtaining confidential information which is likely to be relevant to the reasonable line of enquiry that you are pursuing, then, you are not allowed to utilise this power whilst that information is privileged or held in confidence. In no circumstances should an authorised person ask a device user to waive their right to confidentiality for the purposes of obtaining confidential information. If a device user expresses their wish to do so, the authorised person should advise that this decision is only taken after the device user has received legal advice. However, if the device user waives the privilege or confidence of the protected material, then you may use this Act to extract it.

There may be occasions when confidential information is unintentionally obtained and reviewed during an extraction. Depending on what the information is, you should proceed as follows:

- If the confidential information accidentally obtained is irrelevant to the case, it must be deleted or redacted as soon as is practically possible.

- If the confidential information is relevant to the case, you should follow Force guidance regarding what to do in this scenario. For example, for some types of confidential information, it may be necessary to send all the extracted information for review by a lawyer independent from the police.

In all cases where it is known that confidential information has been obtained from the device without the device user's knowledge, you should inform them at the earliest opportunity of what has been extracted and the actions that have been taken to protect their information, unless there is a lawful reason not to.

Service Police Investigations Only

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



**HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE**

**Police, Crime, Sentencing and Courts Act 2022,
Part 2, Chapter 3 Electronic Device Extraction
User Information Sheet
Digital Processing Notice (DPNb)**

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

We understand that requesting personal or private information, either from a mobile phone or another electronic device, has the potential to cause anxiety. The purpose of this document is to explain:

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

Why do the police need the device?

For a criminal investigation, we have a legal duty to carry out all reasonable lines of enquiry, whether it points towards or away from the suspect. What is reasonable in each case will depend on the particular circumstances.

For a non-criminal investigation we will need to find information relevant to the purpose of extraction.

We must not seek to review an electronic device without good cause. The request to inspect a device must have a proper basis in every case. This means that there must be reasonable grounds to believe that information stored on the device is relevant to a reasonable line of enquiry or purpose of extraction.

The officer who is with you will inform you of this basis and record it on a form called DPNa. That form will also tell you what information we are seeking from the device (see further below). You will be provided with a copy of this form.

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

When investigating criminal offences, investigators must ensure a fair trial for the accused whilst minimising any intrusion into the private life of the device user.

If circumstances change, we may need to extract additional information from the device at a later date. If this is the case, we will explain what additional information we are seeking and will obtain further agreement from you before any extraction takes place.

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

We will be using the digital device extraction power in Part 2, Chapter 3 of the Police, Crime, Sentencing and Courts Act 2022.

The powers in Section 37 may be used for the purpose of:

- 37(2)(a) preventing, detecting, investigating or prosecuting crime;
- 37(2)(b) helping to locate a missing person, or;
- 37(2)(c) protecting a child or an at-risk adult from neglect or physical, mental or emotional harm.

Unless a Condition A-C (explained below) applies, the device must have been volunteered by you, and subsequent extraction agreed.

The PCSC Act allows for law and non-law enforcement purposes.

If extracting for law enforcement purposes, we will subsequently process the personal data (information) on it in accordance with Part 3 of the Data Protection Act

2018. This allows us to process personal data when it is required for a law enforcement purpose. There are conditions attached. As we expect to process sensitive personal data we will only acquire data from the device when it is 'strictly necessary' to do so for the law enforcement purpose. We need to meet one of the conditions set out in Schedule 8 DPA 2018. The conditions most likely to be met are:

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

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

If extracting for non-law enforcement purposes –to help locate a missing person or to protect a child or an at-risk adult from neglect or physical, mental or emotional harm - we will process under the UK GDPR. When extracting information for non-law enforcement purposes, the seven principles under Article 5 of the UK GDPR need to be met and Article 6 of the UK GDPR defines the lawful basis on which we can process the data. As we expect to process 'special category data' Article 9 of the UK GDPR also applies.

In every case when assessing if it is necessary and proportionate to extract information and process information we will balance the benefit of extraction with the likely intrusion on the user's privacy and the privacy of others whose information is stored on their device.

If you do not agree, we will not acquire the information unless we can satisfy one of the below conditions:

Condition A – a person who was a user of the electronic device has died and the person was a user of the device immediately before their death;

Condition B - a user of the electronic device is a child or an adult without capacity, and we reasonably believe that the user's life is at risk or there is a risk of serious harm to the user;

Condition C - a person who was a user of the electronic device is missing, they were a user of the device immediately before they went missing, and we reasonably believe that the person's life is at risk or there is a risk of serious harm to the person.

Otherwise, we will not use another power of seizure and examination unless there is an identifiable basis for believing that you, a user, or another individual, is at risk of harm and we cannot manage that risk through less intrusive means. In these circumstances we may acquire the information from the device without the user's or your agreement, and without utilising the PCSC Act. We will tell you when this happens unless to do so would increase the risk to you or others.

It is possible that we will be in lawful possession of the device without agreement. For example, it may have been seized from a house search. In these circumstances we will always ask for agreement before acquiring the data from the device under the PCSC Act.

Do I have to give the police my device?

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

If you do refuse to volunteer to hand over a device and agree to extraction, we will not bring the investigation to an end merely because of this refusal.

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

You may withdraw your agreement any point before the extraction takes place, and the device will be returned. However, where the extraction has already taken place for a criminal investigation, the requirements of disclosure may mean that some of the information obtained may be disclosed to the CPS or the defence where it is relevant.

If you have changed your mind, you should discuss this with the officer in the case and explain the reasons to them.

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

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

There are potential consequences for a criminal investigation if you do not provide your device. These include:

1. A witness summons may be issued – this is a document issued by the court that will require you to give evidence at court or provide your device to the court, or;
2. A prosecution may be unable to proceed.

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

However, if you do refuse to volunteer to hand over a device and agree to extraction, we will not bring the investigation to an end merely because of this refusal.

How long will the police keep the device for?

We will keep your device for the minimum amount of time necessary. The length of time will be determined by a number of factors and the officer to whom you give the device will give you an indication of how long this will be and record this on the DPNa.

If, for any reason, this length of time changes then you will be kept informed

Will the police look at everything on my device?

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

The least intrusive means of obtaining the information available will be considered. We will minimise collateral intrusion on the others whose information may also be extracted.

If possible we will obtain the information we need without taking your device from you. If this is not possible, the investigator may need to take the device in order to

extract the information. The content should be acquired with minimum inconvenience to you and the device returned without unnecessary delay.

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

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

In a criminal investigation, what will the police do with the information they take from my device? Who will they give it to?

Before a suspect is charged with an offence.

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

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

After a suspect is charged with an offence.

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

When we recover information from a device it will fall into one of three categories:

Evidence

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

Relevant information

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

Non-relevant information

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

There may be occasions when it is impossible to separate this information from information that falls into the first two categories. If this is the case, it will be dealt with as highlighted within the <force> <Sensitive Processing Appropriate Policy Document>

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

1. The seriousness of the offence being investigated set against the seriousness of the unrelated criminal activity;
2. Whether there is risk of harm to any person as a result of the unrelated criminality;
3. Whether the information about the unrelated criminal activity is capable of having a bearing on the initial offence being investigated. If so, this information must be revealed to the prosecutor. It will not be disclosed to the defence unless the disclosure test is met.

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

We will tell you. The investigator to whom you hand the device will agree a contact plan with you. This will include how often you wish to be kept informed and at what

stages of the investigation. If you would like to know what information has been retained and when it is shared, this will form part of that plan.

How will my data be kept secure and how long will it be retained?

Any personal data must be used and stored securely. The storage, retention and disposal of information extracted from a device will be managed in line with data protection legislation and will be retained for no longer than necessary.

We follow the rules in the 'Information Security: Information Assurance College of Policing Authorised Professional Practice (APP)' and, in the case of sensitive data, our Sensitive Processing Appropriate Policy Document.

You can find out more about what we do with your personal data, and your rights under data protection legislation, by reading our Sensitive Processing Appropriate Policy Document which can be requested from freedomofinformationteam@northwales.police.uk

The Information Security: Information Assurance College of Policing Authorised Professional Practice (APP)' can be accessed below:

<[Information assurance | College of Policing](#)>

Data Protection – what are my rights?

We have to follow the rules in the Data Protection Act 2018 and UK GDPR when we use your personal data. The law also gives you rights over your data. The privacy notice for North Wales Police tells you how we use your personal data and about your rights. The privacy notice can be accessed below:

<https://www.northwales.police.uk/advice/advice-and-information/data-pro/data-protection/> or request a copy by calling 101.

You can ask for access to the personal data we hold about you, known as a Subject Access Request (SAR). More information can be found on the Information Commissioners Office (ICO) website.

Further questions or complaints

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

Alternatively, you can contact our Professional Standards Department on the link below.

<https://www.northwales.police.uk/fo/feedback/>

If you have a complaint regarding how the police have handled your data from your device(s), you have the right to complain to the Information Commissioners Office, who are the UK's independent body set up to uphold information rights. They can be contacted through their website by dialling or 0303 123 1113.

National Support Agencies

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