



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

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

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

|                         |  |
|-------------------------|--|
| <b>Crime Report No:</b> |  |
|-------------------------|--|

|                                    |  |
|------------------------------------|--|
| <b>OIC Details</b>                 |  |
| <b>Station / Department / Team</b> |  |
| <b>Name &amp; Shoulder No</b>      |  |

|                                                                           |                                                                                                  |                         |  |                                                                                                                                                                      |  |  |  |  |  |  |  |  |  |
|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|-------------------------|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|--|--|--|--|
| <b>Device Details</b>                                                     |                                                                                                  |                         |  |                                                                                                                                                                      |  |  |  |  |  |  |  |  |  |
| <b>Exhibit Ref</b>                                                        |                                                                                                  |                         |  | <b>Device Pattern Lock</b><br><table border="1"><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr></table> |  |  |  |  |  |  |  |  |  |
|                                                                           |                                                                                                  |                         |  |                                                                                                                                                                      |  |  |  |  |  |  |  |  |  |
|                                                                           |                                                                                                  |                         |  |                                                                                                                                                                      |  |  |  |  |  |  |  |  |  |
|                                                                           |                                                                                                  |                         |  |                                                                                                                                                                      |  |  |  |  |  |  |  |  |  |
| <b>Telephone No(s)</b>                                                    |                                                                                                  |                         |  |                                                                                                                                                                      |  |  |  |  |  |  |  |  |  |
| <b>Make of Device</b>                                                     |                                                                                                  | <b>Model</b>            |  |                                                                                                                                                                      |  |  |  |  |  |  |  |  |  |
| <b>Data Card Present</b>                                                  |                                                                                                  | <b>No of Cards</b>      |  |                                                                                                                                                                      |  |  |  |  |  |  |  |  |  |
| <b>IMEI No.</b>                                                           |                                                                                                  |                         |  |                                                                                                                                                                      |  |  |  |  |  |  |  |  |  |
| <b>SIM PIN Code</b>                                                       |                                                                                                  | <b>Device Pass Code</b> |  | <b>Indicate beginning and end</b>                                                                                                                                    |  |  |  |  |  |  |  |  |  |
| <b>Alternative Lock Methods</b>                                           | If alternative lock methods are present (e.g. fingerprint or iris) please ask witness to disable |                         |  |                                                                                                                                                                      |  |  |  |  |  |  |  |  |  |
| <b>Description of device condition (e.g. damage or faults, last used)</b> |                                                                                                  |                         |  |                                                                                                                                                                      |  |  |  |  |  |  |  |  |  |

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

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

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

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

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

*The material is strictly necessary because:*

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

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

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

**Collateral Intrusion:**

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

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

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

**Signature :**

**Time/date:**

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

**AUTHORISATION FOR FORENSIC ANALYSIS**  
**THIS MUST BE AUTHORISED PRIOR TO ACQUISITION**

*To be completed by the authorising Inspector*

|                                                                                    |                                                |
|------------------------------------------------------------------------------------|------------------------------------------------|
| <b>Authority Required from</b>                                                     | <b>INSPECTOR</b>                               |
| <b>Is the device lawfully in police possession?</b>                                | If no, detail below what action you have taken |
| <b>Has the device been interfered with or interrogated in any way? (By police)</b> | Explain:                                       |

|                                                                                                                                                                    |  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| <input type="checkbox"/> I have considered this request for mobile device extraction and the specific information requested as set out above.                      |  |
| <input type="checkbox"/> I am satisfied that the request is a reasonable line of enquiry and strictly necessary based on the circumstances of the case.            |  |
| <input type="checkbox"/> I am satisfied that the officer requesting the extraction has considered less intrusive means of pursuing the reasonable line of enquiry. |  |
| I Please Select the request.<br>                                                |  |
| <b>Name</b>                                                                                                                                                        |  |
| <b>Time &amp; Date authorised</b>                                                                                                                                  |  |

## **Guidance for officer completing the form – FAQs**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

### **What should I tell the witness about the process?**

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

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

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

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

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

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

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

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

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

## **Service Police Investigations Only**

- 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).*
- 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).*