

Reminder | Digital Processing Notices (DPN)

29th December 2023

In 2022 a new set of Digital Processing Notices (DPN) was launched in line with the guidance from the College of Policing and the National Police Chiefs' Council (NPCC).

DPN improves how police colleagues obtain digital evidence during investigations and gives a greater assurance to victims and all those involved in the process. It will also help police and prosecutors balance the need to follow all reasonable lines of enquiry with the need to respect the privacy of victims and witnesses, while meeting disclosure obligations.

The new notices also address a number of the recommendations set out in the Information Commissioner's report into mobile phone data extraction published in June 2020.

This is a legal requirement and support on how to do this can be found on the Niche Library.

The forms can be found on the [Forms Database](#) and in the [Disclosure Hub Library](#):

- [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.

Officers must follow the below principles when extracting digital data from a personal device:

- Only extract data if it is strictly proportionate, necessary and reasonable.
- Where data is extracted details about the data will be given to the device owner.
- Request permission from owner of the device (unless using a lawful power of seizure).
- The device owner has the right to refuse permission (unless using a lawful power of seizure).
- Any information or material irrelevant to the investigation will be deleted without undue delay.
- Investigators will consider risk of harm and any issues which could have adverse impact on the device owner.
- Investigators will review the retention of digital devices and the extracted data at regular intervals.
- Investigators will not disclose personal information unless it is strictly necessary to do so.
- All actions including information provided, permission given, decisions and approvals given about the extraction of data will be recorded.
- **Officers should seek authorisation from an inspector before downloading information.**

Interim Digital Processing Notices

4th February 2021

A new interim set of Digital Processing Forms have been launched for use when there is an investigation that requires the examination of a Digital Device from a Victim or Witness. This is following the recent Court of Appeal judgement, Bater-James and Mohammed [2020].

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. Devices should not routinely be obtained from victims and witnesses.

DPNa – The Digital Processing Authorisation form is completed by the officer and contains guidance for completing the form and information to be provided to the victim/witness, when requesting examination of their digital device. This is available on Niche and Force Intranet.

DPNb – Victim/Witness FAQ. This form should be provided to the victim/witness and contains important information regarding their data and digital device for the purposes of the investigation. This can be accessed via Single Online Home and also the Force Intranet.

The change to the forms sets out some clear principles that should be followed when approaching mobile phone extraction in relation to victims and witnesses.

Officers must follow the below principles when extracting digital data from a personal device:

- Only extract data if it is strictly necessary.
- Where data is extracted details about the data will be given to the device owner.
- Request permission from owner of the device.
- The device owner has the right to refuse permission.
- Any information or material irrelevant to the investigation will be deleted without undue delay.
- Investigators will consider risk of harm and any issues which could have adverse impact on the device owner.
- Investigators will review the retention of digital devices and the extracted data at regular intervals.
- Investigators will not disclose personal information unless it is strictly necessary to do so.
- All actions including information provided, permission given, decisions and approvals given about the extraction of data will be recorded.
- Officers should seek authorisation from an inspector before downloading information.

Whilst these forms address the immediate findings from 'Bater James' further work by the NPCC and College of Policing to produce advice and guidance addressing the Information Commissioner's investigation report into mobile phone extraction will follow.

Digital Processing Notices (DPN) | What you need to know

6th July 2022

Amended Digital Processing Notices in force from 11 July (Now includes digital devices from suspects)

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

Digital Processing Notice (DPN) and supporting information to gain permission for searching digital devices was launched across police forces in England and Wales in September 2021. From **Monday 11 July**, Staffordshire Police will be ready to start using these updated notices across our investigations with supporting Niche processes ready to use, including a new notice for suspects, the DPNc

DPN improves how police colleagues obtain digital evidence during investigations and gives a greater assurance to victims and all those involved in the process. It will also help police and prosecutors balance the need to follow all reasonable lines of enquiry with the need to respect the privacy of victims and witnesses, while meeting disclosure obligations.

The new notices also address a number of the recommendations set out in the Information Commissioner's report into mobile phone data extraction published in June 2020.

This is a legal requirement and support on how to do this can be found on the Niche Library.

The forms can be found on the [Forms Database](#) and in the [Disclosure Hub Library](#):

- [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.

Officers must follow the below principles when extracting digital data from a personal device:

- Only extract data if it is strictly proportionate, necessary and reasonable.
- Where data is extracted details about the data will be given to the device owner.
- Request permission from owner of the device (unless using a lawful power of seizure).
- The device owner has the right to refuse permission (unless using a lawful power of seizure).
- Any information or material irrelevant to the investigation will be deleted without undue delay.
- Investigators will consider risk of harm and any issues which could have adverse impact on the device owner.
- Investigators will review the retention of digital devices and the extracted data at regular intervals.

- Investigators will not disclose personal information unless it is strictly necessary to do so.
- All actions including information provided, permission given, decisions and approvals given about the extraction of data will be recorded.
- **Officers should seek authorisation from an inspector before downloading information.**

The College of Policing APP for extraction of material from digital devices [can be accessed here](#) and to support, a poster explaining the two step process to acquire digital evidence has been shared. [You can view it here](#). This includes step 1 – acquiring the device using informed agreement and step 2 – extracting the material for law enforcement purposes under the DPA 2018 using Scan, Analyse, Respond and Assess principles.

National Police Chiefs' Council lead for Disclosure, Assistant Chief Constable Tim De Meyer, said:

"It is fundamental to our criminal justice system that the police must pursue all reasonable lines of enquiry and that the prosecution must disclose to the defence any material that undermines the case for the prosecution or assists the case for the accused.

"The new Digital Processing Notices are the result of over a year of work across the criminal justice system. I am grateful to the Victims' Commissioner and the many other stakeholders representing victims' interests, whose advice and scrutiny has enabled us to develop these much improved notices.

"Searches of digital devices should not be automatic and will happen only when the investigating officer or prosecutor considers there to be a need to access information to pursue a reasonable line of enquiry. We will explain this process fully to victims and witnesses."

New Digital Processing Notices (DPN) are now available for use

11th July 2022

From today (Monday 11 July), Staffordshire Police have implemented the new Digital Processing Notices (DPN) in line with the guidance from the College of Policing and the National Police Chiefs' Council (NPCC).

DPN improves how police colleagues obtain digital evidence during investigations and gives a greater assurance to victims and all those involved in the process. It will also help police and prosecutors balance the need to follow all reasonable lines of enquiry with the need to respect the privacy of victims and witnesses, while meeting disclosure obligations.

The new notices also address a number of the recommendations set out in the Information Commissioner's report into mobile phone data extraction published in June 2020.

This is a legal requirement and support on how to do this can be found on the Niche Library.

The forms can be found on the [Forms Database](#) and in the [Disclosure Hub Library](#):

- **[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.

Officers must follow the below principles when extracting digital data from a personal device:

- Only extract data if it is strictly proportionate, necessary and reasonable.
- Where data is extracted details about the data will be given to the device owner.
- Request permission from owner of the device (unless using a lawful power of seizure).
- The device owner has the right to refuse permission (unless using a lawful power of seizure).
- Any information or material irrelevant to the investigation will be deleted without undue delay.
- Investigators will consider risk of harm and any issues which could have adverse impact on the device owner.
- Investigators will review the retention of digital devices and the extracted data at regular intervals.
- Investigators will not disclose personal information unless it is strictly necessary to do so.
- All actions including information provided, permission given, decisions and approvals given about the extraction of data will be recorded.
- **Officers should seek authorisation from an inspector before downloading information.**