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 ensuring 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 Dyfed Powys Police Data Protection Policy.

https://www.dyfed-powys.police.uk/foi-ai/dyfed-powys-police/publication-scheme/our-policies-and-procedures/Policies/information-management-ICT/data-protection-policy/

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 accessed below:

https://www.dyfed-powys.police.uk/foi-ai/dyfed-powys-police/publication-scheme/our-policies-and-procedures/Policies/information-management-ICT/data-protection-policy/

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?

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

The Chief Constable of Dyfed- Powys Police is the overall data controller.
The Data Protection Officer for Dyfed Powys Police is Debby Jones.
Contact e-mail: dataprotection@dyfed-powys.pnn.police.uk
You can make a data protection request using this email address.

Under Section 45 Data Protection Act 2018, you are able to make data protection requests (also known as subject access requests or SARS). More information can be found on: https://ico.org.uk/your-data-matters/your-right-to-get-copies-of-your-data/

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:
https://www.dyfed-powys.police.uk/fo/feedback/complaints/complaints/

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