



Victim/witness FAQ

Digital Processing Notice b (DPNb)

Throughout this form the term 'witness' is used to include both victims and witnesses.

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.

The police have begun an investigation into an allegation of crime and there is a need to examine a digital device in your possession or control. The police must investigate to find all relevant material that could have a bearing on the case, whether it points towards the suspect or away. This notice sets out the approach we will take.

We understand that requesting your personal or private information, either from your mobile phone or other digital device, has the potential to cause anxiety. Investigators need to balance ensuring a fair trial for the accused against any intrusion into the private life of a victim or witness. The purpose of this document is to explain when we will ask to look at your device, how we will look it, what will happen to the data we copy, retain and review, and what the potential consequences are if you do not agree to the police looking at your device and data.

Why do the police need my device?

We have a legal duty to carry out all reasonable lines of enquiry when investigating a crime. We must look for all evidence that supports a case against a person as well as information or material that might undermine the case or support the suspected person.

We must not seek to review a witness's digital material without good cause. The request to inspect digital material, in every case, must have a proper basis. This means that there must be reasonable grounds to believe that it may reveal material relevant to the investigation or the likely issues at trial.

We should not routinely obtain devices from witnesses. We must have a properly identifiable basis for believing that relevant material will be found on your device. 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 material we are seeking from your device (see further below). You will be provided with a copy of this form.

We will also consider whether there are other ways to obtain the material we need before asking you to hand over your device. Which alternative methods have been considered and rejected will also be recorded in form DPNa.

Do I have to give the police my device?

No. We will ask you to agree to hand over your 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 material and that the extracted material will be kept securely. However the decision is yours and you do not have

to provide your device. It is important we understand your reasons if you decide not to provide your device because we will need to explain them if the case goes to trial.

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 material on your device then you will be asked not to delete any material on it, as this risks preventing a fair investigation of the case.

There are potential consequences if you do not provide your device. These include:

1. it may be impossible to pursue the investigation;
2. 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
3. a prosecution may be unable to proceed.

This is because the court needs to be sure that the 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 material from the suspect'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 it is not possible to follow a particular reasonable line of enquiry because the material on your device has not been examined, any review of the case will have to take this into account. Whether a fair trial is still possible will depend on the circumstances of each case.

How long will the police keep my device for?

The police 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 your device will give you an indication of how long this period will be. If for any reason this length of time changes then you will be kept informed.

Will the police look at everything on my device?

No.

If possible we will obtain the material we need without taking your device from you.

If that is not possible then the device may need to be downloaded or copied. The investigator will take your device away to do this. The contents should be extracted with minimum inconvenience to you and your device returned without unnecessary delay.

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

If technology doesn't allow us to target only the relevant material, we may have to copy more material than we need. If this happens, the investigator will set clear parameters to satisfy the reasonable line of enquiry and review material 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. Material outside of those parameters will not be looked at.

What will the police do with the material they take from my device? Who will they give it to?

Before the suspect is charged with an offence.

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

After the suspect is charged with an offence.

Once the 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 your device. The circumstances in which a defendant will see material from your phone or other digital device is explained below.

When we recover material from your phone it will fall into one of three categories:

Evidence

This is the material that the prosecution will use in Court in order to prove the offence. The defendant will see this material. You will be told which material 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 (eg. photographs, addresses or full telephone numbers).

Unused material

This is material that is relevant to the offence, 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 material from this category to the defendant if it assists their defence or undermines the prosecution case. You will be told which material 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 (eg. photographs, addresses or full telephone numbers).

Non-relevant material

This is everything else that does not fit in the first two categories. The defendant will not see this material. In some cases where we have been able to target the relevant material only, there will not be anything in this category. Where we have had to retain more than we need, we will delete this material wherever possible and as soon as possible. This includes material 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 material from material that falls into the first two categories. If this is the case, it will be dealt with as highlighted within Staffordshire Police Sensitive Processing Appropriate Policy Document. <https://www.staffordshire.police.uk/hyq/fpnstaffordshire/privacy-notice/>.

In the event that we identify unrelated criminal activity on your 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 you have 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.

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

We will tell you. The investigator to whom you hand your 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 material has been retained and when it is shared this will form part of that plan.

How will my data be kept secure?

You may be particularly concerned about the security of any data which is downloaded and stored whilst the criminal investigation is ongoing. Here we briefly explain our commitment to keeping your data secure, but you can find further details in the Sensitive Processing Appropriate Policy Document referenced above, and in the Management of Police Information (MoPI) Authorised Professional Practice (APP) policy document issued by the College of Policing and available on their website (the link is included below).

Any data that is downloaded from your device is kept on the [Staffordshire Police secured servers. It will be handled, stored and retained securely in accordance with the provisions of the Management of Police Information (MoPI) APP and, in the case of sensitive data, the Sensitive Processing Appropriate Policy Document.

The Sensitive Processing Appropriate Policy Document can be found at <https://www.staffordshire.police.uk/hyg/fpnstaffordshire/privacy-notice/>.

The Management of Police Information (MoPI) APP can be found at the College of Policing website <http://www.college.police.uk>.

Further questions or complaints

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

Alternatively, you can contact our Professional Standards Department at Staffordshire Police HQ, Weston Road, Stafford, Staffordshire. ST18 0YY.

If you have any issues over the handling of your data you should in the first case contact the Data Protection Officer for Staffordshire Police. SPDPO@staffordshire.pnn.police.uk, or at Staffordshire Police HQ, Information Governance and Assurance Department, Weston Road, Stafford, Staffordshire. ST18 0YY

The Data Controller for Staffordshire Police is the Chief Constable of Staffordshire Police.

If you have still 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 on <https://ico.org.uk/make-a-complaint/> 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