INSERT FORCE LOGO

Digital device extraction – information for complainants and witnesses

We understand that a request to obtain personal or private information, either from your mobile telephone or digital device has the potential to cause anxiety. The purpose of this document is to explain why we may be making a request, what will happen to your data and to address some of the concerns that you may have. A list of other agencies who may offer support and advice is included at the end of this information sheet.

You may be asked to give your consent to download data from your device, such as text messages and emails.

Digital Devices - why we may need to look at your 'phone and other digital devices

The police have a responsibility to investigate crimes and gather all evidence that may be **relevant** to the case. "Relevant" means anything that has some bearing on any offence under investigation, or on the surrounding circumstances of the case. Investigations have to be thorough and the police have a legal duty to follow all reasonable lines of enquiry. These lines of enquiry will depend upon the individual circumstances of each case.

Mobile phones and other digital devices such as laptop computers, tablets and smart watches can provide important relevant information and help us investigate what happened. This may include the police looking at messages, photographs, emails and social media accounts stored on your device. We recognise that only the reasonable lines of enquiry should be pursued to avoid unnecessary intrusion into the personal lives of individuals.

You may be able to tell us where you think the relevant information is on your phone or other digital devices, or you may not. You will be asked about this during the initial stages of the investigation. This process may also be applied to the suspect's mobile phone and other relevant devices in order to establish if there is any data that might be relevant to the case.

Digital Processing Notice

Before obtaining data from your device(s), we will ask for your consent and request you sign a form called a 'Digital Processing Notice'. The form provides you with important information about how we store and protect the data obtained from your device(s) and it is important that you read it carefully. You will be given a copy of this form and we will retain it in line with legislation.

What we do with your digital device

There are essentially 3 levels of examination that can be applied to a device and this will affect what data is obtained. The data that can be extracted may vary by handset and the extraction software used. You will be provided with further information by the officer dealing with your case. However, the following broadly describes the level of extraction:

- **Level 1** – called a "logical extraction". This may provide almost all of the data you could see if you were to turn on the device and browse through it. It will **not** normally extract data that has been deleted from the device.

- **Level 2** – either a "logical" extraction using selected tools in a laboratory environment or a "physical" extraction, which recovers a copy of the data held on the memory chip of the device. "Physical" downloads can extract deleted data, although capabilities vary depending on the nature of the device and the operating system.

- **Level 3** – these are usually expert and bespoke methods to tackle complex issues or damaged devices.

Some technology will not be able to obtain material using parameters such as a specific time period, meaning even though we may only consider a limited number of messages relevant to the investigation, the tool may obtain all messages.

Depending on the nature of the investigation, data from your device may be downloaded at the police station and your device returned to you, or we may need to send it to a digital forensics laboratory, which will mean that we will need to keep your device for a longer period, including until the end of any criminal proceedings.

The investigating officer will explain to you what level(s) of examination will be applied to your device and how long we are likely to keep your device for.

The Crown Prosecution Service (CPS) is the body responsible for prosecuting criminal cases investigated by the police in England and Wales. Evidence gathered by the police will be handed over to the CPS, who prepares the case for court. Sometimes the CPS will advise the investigating officer about what data should be examined before a case is charged, and sometimes they may ask for further investigation to be conducted after a case has been charged.

This process can take some time and it may be that we need to keep your phone and any other devices for several months, or we may request it from you again at a later stage. We may be able to supply you with an alternative mobile phone.

What happens to the data obtained from your device?

Once data has been downloaded and reviewed, we divide the material into different categories:

- 'Used' material – this is data that we want to use as evidence in court if the case goes to trial;
- 'Unused' material – this means that it is relevant but does not form part of the evidence that the prosecution wants to rely on. If unused material may undermine the prosecution case, or assist the defence then it must be provided to the defence if there is to be a trial; and
- Material which is not relevant because it is not capable of having any bearing on the case - this is not used either as evidence, or disclosed as unused material but will be retained until the conclusion of criminal proceedings.

Data obtained from your mobile phone or other digital device may be used as evidence to support the prosecution case, which means that it will be shown to the suspect/defendant and used in court. If unused material could assist the defence or undermine the prosecution case then it will also be shown to the suspect/defendant.

If data obtained from your device has been or will be shown to the suspect/defendant, either as evidence or as disclosed unused material then we will inform you of this.

In some cases the court will make an order for you to release data; but this is rare and before this happens you will be given an opportunity to make representations at a court hearing.

What happens if we find evidence of other criminal offences?

If information is identified from your device that suggests the commission of a separate criminal offence, other than the offence(s) under investigation, the relevant data may be retained and investigated by the police. This data may be shared with other parties including, for example other police forces or a court in any criminal proceedings.

If your device contains information that may assist in the prevention or detection of crime, or protecting the vulnerable, then the police may process and retain this information on our intelligence management system and/or share that information with relevant parties/agencies, including other police forces or government agencies, including those outside of the UK.

What happens if I refuse consent for the police to access my data or information held about me?

If you do not provide consent for the police to access data from your device you will be given the opportunity to explain why. If you refuse permission for the police to investigate, or for the prosecution to disclose material which would enable the defendant to have a fair trial then it may not be possible for the investigation or prosecution to continue.

If a prosecution is able to continue then the defence representatives will be told of your refusal and a judge may order disclosure to take place. If this happens, you will be given the opportunity to make representations to the court about the reasons why you object.

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 (insert force details).

If you have a complaint regarding how the police have handled your data from your device 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

[INSERT POLICE FORCE] DIGITAL PROCESSING NOTICE

Crime Reference Number:

The police request your consent to take possession of your mobile phone or other digital device (laptop, iPad etc.) for the purpose of extracting information considered to be relevant to the investigation that you are involved with.

This form describes our data protection and safe storage responsibilities. Separate forms will be used for each device requiring examination. You will be provided with a copy of this form and it will be retained by the police until the conclusion of any related criminal proceedings.

This notice must be served alongside the information document entitled "Digital device extraction – information for complainants and witnesses" which explains the reason the police are requesting your digital devices(s), and how the data extracted may be used.

Please contact the investigating officer in your case should you wish to discuss further how we may use your data.

All information recovered in the course of a criminal investigation will be handled, stored and retained securely in accordance with the provisions of the Management of Police Information (MoPI). Further information on MoPI and other approved professional practice information can be found at the College of Policing Website (www.college.police.uk "APP"►*"Information Management"*).

We also have a duty to retain certain information. The retention period of the data we collect from your device will vary depending upon the severity of the offence investigated.

The officer investigating your case can print out relevant parts of MoPI for you if you have concerns, or email you the link to the appropriate parts of the website. This document can also be emailed with the following links: MoPI 2005

Retention period

"*APP"* ► *"Information Management"* ► "Retention, review and disposal" ► "Review schedule"

The police are under a legal obligation to pursue all reasonable lines of enquiry. To enable us to meet this obligation we are requesting access to your device and data on it as set out below.

In order to investigate the crime you are involved in, the police intend to extract the following data categories from the device e.g. call data, messages, email, contacts, applications (apps), internet browsing history etc.:
……
……
……
……
……
(Continue on a separate sheet if necessary.)

It is the intention of the investigating officer to use the following, or a combination of the following level of extraction. Should an alternative level of extraction become necessary in order to successfully recover data, the investigating officer will contact you with an update and further consent may be required.

- **Level 1** – called a “logical extraction”. This provides almost all of the data you could see if you turn on a device and browse through it. It will **not** normally extract data that has been deleted from the device.

☐ **Level 2** – either a “logical” extraction using selected tools in a laboratory environment or a “physical” extraction, which recovers a copy of the data held on the memory chip of the device. “Physical” downloads can extract deleted data, although capabilities vary depending on the nature of the device, and operating system.

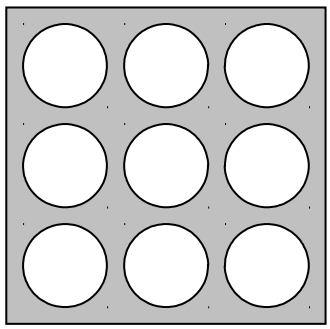
☐ **Level 3*** – these are usually expert and bespoke methods to tackle complex issues or damaged devices.

Each of these levels may extract data in addition to that listed above by the investigating officer. Additional data extracted but which is not relevant will be securely stored as described above.

The investigating officer will explain the technical capabilities or restrictions relating to the above level of extraction. This could, for example relate to whether the methods used are compatible with your device and what data can, or cannot be extracted.

The level of extraction will determine how long we may need to retain your device. The investigating officer will explain how long this is likely to be in your case.

*Although great care will be taken to avoid this, Level 3 extractions may result in damage to the digital device, or permanent loss of data.

<table>
<tr><td colspan="4">Device Details (to be completed by investigating officer):</td></tr>
<tr><td>Exhibit Ref:</td><td colspan="2"></td><td rowspan="6">Device Pattern Lock (indicate beginning and end)
  </td></tr>
<tr><td>Telephone No.:</td><td colspan="2"></td></tr>
<tr><td>Make/Model No.:</td><td></td><td>Memory Card Present:</td><td>Yes ☐
No ☐</td></tr>
<tr><td>Device PIN Code:</td><td colspan="3"></td></tr>
<tr><td colspan="3">If alternative lock methods are present (i.e. fingerprint/face or iris) please ask complainant/witness to disable these in advance.</td></tr>
<tr><td>General Description of Condition: (i.e. damage or faults, last used)</td><td colspan="3"></td></tr>
</table>

I have been given the “Digital device extraction – information for complainants and witnesses” form. I understand why the police are requesting my digital device and access to the data on it. I understand the process used to extract that data and I understand all relevant data (as determined by the investigating officer) will be handled, stored and retained as set out above.

The investigating officer will inform me if any of my data has been or will be disclosed to any suspect or their defence representative.

Name and DOB:	
Address inc. postcode and telephone number:	
Signature:	
Owner of device / parent or guardian details:	
Address inc. postcode and telephone number:	
Signature:	Date:

The police will not disclose your data to any party, including parents/guardians, other than as required for the purpose of criminal proceedings or to comply with a legal duty.

Ordinarily, the police seek the involvement of a parent/guardian of a complainant or witness under the age of 18. Any objection to the police informing a parent/guardian of this request will be recorded, together with any reasons given. The police will try and comply with your wishes but there may be circumstances when it will not be possible to do so.

Investigating Officer*			
Name:		Force ID Number:	
Rank/phone number:		Location/Unit:	
Signature:		Date:	

Data Controller:	Chief Constable of [INSERT POLICE FORCE]
Information Commissioner's Office Registration Number:	
Data Protection Officer Address:	
Should you wish to make a complaint in respect of how your information and data has be handled by the police, you can contact the Information Commissioners Office.	https://ico.org.uk/make-a-complaint/ 0303 123 1113

**Note for investigating officer: Please ensure a copy of this is provided to the complainant/witness and/or parent/guardian and/or owner of device.*