**Insert Force Logo**

**Digital Processing Notice (DPNc)**

**(Device taken from suspect)**

*Complete one form per device*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Crime Report No:** |  | | | |
| |  |  | | --- | --- | | **OIC Details** | | | **Station / Department / Team** |  | | **Name & Shoulder No** |  | | | | | |
| **Device Details** | | | | | |
| **Exhibit Ref** |  | | | **Device Pattern**  **Lock**  **Indicate beginning**  **and end** | |
| **Property Ref** |  | | |
| **Make of Device** |  | **Model** |  |
| **Device Pass Code** |  | | |
| **SIM Pin Code** |  | | |
| **Description of device condition** |  | | |
| **Device Security Protection – Place X in appropriate column** | **Protected – give details in box above** | | |  | |
| **Not Protected** | | |  | |
| **Subject refused to provide** | | |  | |
| **Not requested - provide your rationale** | | |  | |

|  |
| --- |
| **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:**  *Explain your reasonable grounds:* |
|  |

|  |
| --- |
| **I consider that is it proportionate and strictly necessary to extract only the following material from the device in order to progress this reasonable line of enquiry because:**  *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. Explain why the material is strictly necessary in the light of the reasonable line 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:* |

|  |
| --- |
| **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.* |

|  |  |  |  |
| --- | --- | --- | --- |
| **Suspect Details** | | | |
| **Name:** |  | **DOB**: |  |
| **Address:** |  | | |
| **Bail Date:**  **(if applicable)** |  | | |

**AUTHORISATION FOR FORENSIC ANALYSIS**

**THIS MUST BE AUTHORISED PRIOR TO ACQUISITION**

***To be completed by the authorising Inspector***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Authority Required from** | | | **INSPECTOR** | | |
| **Is the device lawfully in police possession?** | | | **YES / NO**  If no, detail below what action you have taken | | |
| **Has the device been interfered with or interrogated in any way? (By police)** | | | **YES/NO**  Explain: | | |
| **I have considered this request for mobile device extraction and the specific information requested as set out above.**  **I am satisfied that the request is a reasonable line of enquiry and strictly necessary based on the circumstances of the case. Yes/No**  **I am satisfied that the officer requesting the extraction has considered less intrusive means of pursuing the reasonable line of enquiry. Yes/No**  **I authorise/reject the request.** | | | | | |
| **Name** |  | | | **Signature** |  |
| **Time & Date authorised** | |  | | | |

**Suspect information notice**

**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.

Acquiring material from your device has been considered as a reasonable line of enquiry in this case – that means that there is an identifiable basis for believing that material is held on your device that is relevant to the investigation.

**Do I have to give my device to the police?**

There are two ways the police can take possession of your device.

1. Use of a lawful power of seizure.

The law permits us to seize your device from you in certain circumstances. The law also provides a power of search to locate the device in certain circumstances. The lawful powers used to search for and seize your device should be explained to you by the officer seizing it if practicable. You are not entitled to refuse when officers are exercising their powers of search and/or seizure lawfully and by doing so you may be committing further offences.

1. Taking the device with agreement.

We may ask you voluntarily to provide us with your device, even when powers of seizure are available. If you agreement is forthcoming we will take possession of your device. This may occur, for example, if you are suspected of committing an offence but you are not being arrested.

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 section allows us to process personal data when it is required for a law enforcement purpose. There are conditions attached to this. 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 that law enforcement purpose. We also need to meet one of the conditions set out in Schedule 8 DPA 2018. The most likely conditions that will 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.

**How long will you keep my device for?**

This will depend on the case circumstances. Often the officer seizing or taking possession of your device will not know this information. You will be provided with the details of the officer in the case, who will inform you of how long s/he expects to keep your device for.

**Will the police look at everything on my device?**

Officers will look only at the material they deem relevant to the investigation.

Wherever possible we will acquire only the material we believe may be relevant, so that we can review it. The investigator will be required to record the material they are looking for and why they are looking for it before the extraction takes place. We may not give you this information as to do so may prejudice the investigation.

If technology does not allow us precisely 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 these 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?**

If we make the decision to take no further action in your case then we will not share the material from it with anyone else, unless we identify an unrelated risk to any individual or we identify evidence of unrelated offences. We will tell you when we have done this unless to do would put anyone at risk or prejudice an ongoing investigation.

There may be exceptional circumstances when the information collected may be shared for other purposes. This might be in relation to civil matters before a family court or if you make a complaint about the handling of the investigation relating to your case, for example. Any sharing will be assessed in relation to necessity.

The decision to charge certain categories of offence rests with the Crown Prosecution Service. We will share relevant material with the prosecutor when requesting a charging decision for such offences.

Should you be charged with an offence, the material on your device 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. This material will be served on you/your defence team by the prosecution.

Unused material

This is material 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 material from this category to the defendant if it assists their defence or undermines the prosecution case.

Non-relevant material

This is everything else that not in the first two categories. In some cases where we have been able precisely to target only the relevant material, there will not be anything in this category. Where we have had to acquire 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 (insert force) Sensitive Processing Appropriate Policy Document. \*\*Force to insert a link to this document\*\*.

**How will my data be kept secure?**

You may be particularly concerned about the security of any data which is downloaded and stored during and after the investigation. 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 [INSERT NAME OF FORCE] (insert how the material is stored – secure database, DVDs, encrypted USBs etc)]. 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. It will not be stored for longer than is necessary.

Further details regarding privacy information, including your rights under data protection legislation, are set out in the Sensitive Processing Appropriate Policy Document

The Sensitive Processing Appropriate Policy Document can be found at http://www.INSERT.

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

**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 Data Controller for this force is \*\**force to enter data controller*\*\*

The Data Protection Officer for this force is \*\**force to enter Data Protection Officer\*\**

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 the ICO website [Your right of access | ICO](https://ico.org.uk/your-data-matters/your-right-to-get-copies-of-your-data/)

You can make a data protection request by \*\**force to insert contact details\*\**

**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.