# Digital Device Examination and Agreement FAQ

## Q1. What is a Digital Device?

The term ‘digital device’ refers to any object capable of storing or transmitting electronic information and includes mobile telephones, tablets, and Sat-Nav devices.

## Q2. What is Digital Device Examination?

‘Digital Device Examination’ is the process of extracting and looking at the contents of a digital device such as a mobile telephone.

## Q3. Why does Police Scotland take and examine digital devices?

We take and examine devices where there is reasonable belief that they may contain evidence or information relating to a police investigation or incident.

Doing so must be necessary, proportionate, and reasonable in the circumstances; we cannot do it “just in case” there is anything of relevance on a device. There must be a reasonable belief that it may contain evidence or information relating to a police investigation or incident.

## Q4. What power do the police have to take and examine digital devices of victims and witnesses?

**Take** – Taking a device from a victim or witness for court and for the purpose of examination requires lawful authority of either;

* **AGREEMENT -** Where a victim or witness is willing to provide their device voluntarily.
* **COMMON LAW (Urgency) -** Taking the device immediately must be proportionate and necessary for example, evidence might be lost or destroyed.
* **WARRANT -** Where a court has allowed police to take the device.

**Examine** – The Data Protection Act 2018 allows police to keep and use information extracted from a device for the investigation, even if agreement is withdrawn for police to retain the device itself.

Further information on the Data Protection Act 2018, and police processing of personal data can be found within the Privacy Notices published on the [Police Scotland Web Site](https://www.scotland.police.uk/access-to-information/data-protection/privacy-notices).

## Q5. If the police ask for my agreement, do I have to give it?

No. Although your device can greatly assist an investigation, you can refuse or withdraw your agreement at any time. Sometimes we might need to use one of the other powers (warrant or common law) if you refuse agreement or withdraw it. This will depend on the investigation and what might be on the device.

## Q6. What happens if I refuse agreement, or provide agreement, then later withdraw it?

If we don’t use another power you will be able to keep your device, or it will be returned as soon as possible after we confirm agreement is withdrawn.

We will continue the investigation without your device, and still follow all other reasonable lines of enquiry.

Your decision at any stage will not affect how we treat you.

## Q7. How does Digital Device Examination work?

In most cases the digital device is connected to a computer running special software which can read the information stored on the device without changing it.

Depending on the case, examination may take place in a local police station using a ‘Cyber Kiosk’ or within a ‘Digital Forensic Hub’. In either case, the examination will be carried out by a specially trained police officer or staff member.

## Q8. What is a Cyber Kiosk?

For further information about Cyber Kiosks please see the [Cyber Kiosk FAQ](https://www.scotland.police.uk/spa-media/zqxibu3s/cyber-kiosk-faq.docx).

## Q9. What is a Digital Forensic Hub?

A Digital Forensic Hub is a department within Police Scotland which is staffed by police officers and police staff who have received specialist training in the examination of digital devices.

We currently have five Hubs situated throughout Scotland.

## Q10. The police have my device, what happens now?

If evidence is found, your device might be needed and kept as evidence for court. It will be powered off, securely packaged and stored and its movements recorded. The device will be submitted for examination and any relevant information prepared in a report as evidence for court.

Throughout this process we will: take the best possible care of your device; view only what is necessary, reasonable, justifiable and relevant, and hold your information securely.

## Q11. Once the police have my device, are checks made before examination takes place?

Yes – once a device has been taken a request has to be made for examination. All requests go through at least two levels of authorisation.

The request is initially reviewed by a supervising officer of at least the rank of Sergeant. This stage involves the supervisor assessing whether or not the examination is necessary, justified and proportionate. If approving the request the supervisor must confirm this in writing and then forward the request for further authorisation.

The second review is carried out by a specially trained officer or staff member who also has to assess necessity, justification and proportionality.

The device will only be examined if the request has been approved at both stages.

## Q12. Can the police bypass PIN codes and passwords?

Sometimes. The ability to bypass security measures such as PIN codes varies depending on the make and model of the device, the version of the operating system being used, and any security measures enforced by the manufacturer. A specific answer regarding this can only be given on a case-by-case basis. PIN codes or passwords will only be bypassed where absolutely necessary to progress the investigation.

## Q13. What information will the police take from my device?

The technology used will **copy** all available information from your device, but police will **only look** at what is necessary, justified, proportionate, and relevant to the investigation.

## Q14. Can deleted information be retrieved from my device?

Yes it can, but this will depend on the make and model of the device, and the operating system being used.

## Q15. Will the police use my device to access information stored on the internet?

No. All devices are isolated from mobile networks (mobile data) and the internet (including Wi-Fi) before examination. The examination only involves information on the device itself, including removable media such as SIM or Memory Cards.

## Q16. Do the police keep the copied information, and if so how long it is held?

If no evidence is found, no information will be kept.

If evidence is found on the device we are required by law to keep the copied information as follows:

* Serious, unresolved, cases - Stored until the case is resolved.
* Standard, unresolved, cases - Stored for current year + 2 years.
* All resolved cases and death investigations - Stored until disposal instructed by Procurator Fiscal (COPFS).

## Q17. What information from my device does the police look at?

We will **only** look at what is necessary, justified, proportionate, and relevant to the investigation.

## Q18. Who will examine my device and view my information?

The minimum number of people possible; only those officers or staff who need to view the information from your device will do so. In most cases this will be the device examiner and investigating officer, as they will be best placed to identify whether information is relevant or not.

In some instances assistance may be required, e.g. a translator or interpreter. This would be monitored and controlled by Police Scotland.

## Q19. Can I decide what the police look at?

We will be guided by the information you provide and will discuss with you what will be looked at. There may however be times that in order to do our job fairly, fully investigate and fulfil our legal requirements, we have to look beyond that. For example, if we receive new information which changes what is relevant to the enquiry.

## Q20. What happens if the police find evidence of another crime?

Although all examinations are specific to the incident under investigation, it is possible that we could find evidence relating to another crime. The action taken will depend on the seriousness and circumstances of the crime. It may be the case that we have a duty to investigate what we find and may have to report the circumstances to the Crown Office and Procurator Fiscal Service (COPFS).

## Q21. When will I get my device back?

Unfortunately we don’t know. If evidence is found on your device, it might not be returned until the court case has finished; it depends on the investigation and what evidence is recovered. We know how important your device is and will try to return it to you as soon as possible.

If no evidential material is found and your device is no longer required for the investigation it will be returned to you.

If evidence is found on your device, the decision regarding the return of the device rests with the police unless the circumstances have been reported to the Crown Office and Procurator Fiscal Service (COPFS) in which case the decision will lie with them.

## Q22. Do the police use digital device examination to identify lost and found property?

**No**. This is not a necessary or proportionate use of digital device examination and is against Police Scotland policy.

## Q23. Who pays for my contract when my device is with the police?

The responsibility for the payment of any contract remains with the account holder, Police Scotland cannot pay for a device contract. You may wish to cancel the contract or the network operator may be able to provide you with a replacement SIM Card to use in another handset whilst yours is with us.

## Q24. Why can’t the police just use the suspect or accused’s digital device?

Where a device has been used by a suspect or accused, we will try to get the device and retrieve the relevant information from it. At times however that is not possible; for example if the device has been hidden or destroyed, or the information can’t be accessed or has been deleted. There may therefore be times that even if we have recovered the accused or suspect/s device that we still need yours as evidence.

## Q25. Will the police share my information with the accused’s Lawyer?

Only information relevant to the investigation will be shared. Police must tell COPFS about the existence of all information relevant to the investigation that we find on a device, whether in support of a prosecution or not.

COPFS will then assess what information needs by law to be shown to the accused’s lawyer. This is called disclosure.

## Q26. What is ‘Disclosure’?

Disclosure is a legal process which must be followed in order to make sure court processes are fair and transparent. Disclosure applies to all evidence, not just digital evidence obtained from digital devices.

The process of disclosure is detailed within Part 6 of the Criminal Justice and

Licensing (Scotland) Act 2010, however can be summarised as follows:

Step 1: Police Scotland gathers evidence in relation to the ongoing investigation

Step 2: Police Scotland provide COPFS with details of any material which may be relevant to the case either for or against the accused (called revelation)

Step 3: COPFS consider the material and identify any which;

* would materially weaken or undermine the evidence likely to be used by the Prosecutor;
* would materially strengthen the accused’s case;
* is likely to form part of the evidence to be led by the Prosecutor. This process is called the Materiality Test.

Step 4: COPFS are legally required to disclose information identified during Step 3 to the defence (lawyer) representing the accused.

Further information regarding the disclosure process is available on the [COPFS website](https://www.copfs.gov.uk/).

## Q27. What is the Crown Office and Procurator Fiscal Service?

The Crown Office and Procurator Fiscal Service (COPFS) is Scotland’s prosecution service. They receive reports about crimes from the police and other reporting agencies and then decide what action to take, including whether to prosecute someone. They also look into deaths that need further explanation and investigate allegations of criminal conduct against police officers.

The main roles and responsibilities of COPFS are to:

* Investigate, prosecute and disrupt crime, including seizing the proceeds of crime
* Establish the cause of sudden, unexplained or suspicious deaths
* Investigate allegations of criminal conduct against police officers

**Q28. How can I contact COPFS?**

The general contact number is 0300 020 3000, however, up-to-date contact information can be found on the [COPFS website](https://www.copfs.gov.uk/in-your-community/our-offices).