

Cyber Kiosk FAQ

Q1. What is a 'Cyber Kiosk'?

A Cyber Kiosk is a computer designed specifically to look at the contents of mobile telephones, tablets and any associated memory or SIM cards. It is not used for any other purpose and does not store any information from the device.

Q2. Why does Police Scotland use 'Cyber Kiosks'?

Cyber Kiosks are used by Police Scotland to quickly identify whether any of the digital devices detailed in Question 1 contain evidence or not. If they do not, we may be able to return the device to its owner.

Cyber Kiosks allow for a targeted search to be conducted on a device using specific criteria such as a date, time, telephone number or within particular areas of the device like text messages or photographs. This allows for evidence to be identified quickly using a focused review of the contents of the device.

Q3. Where are the 'Cyber Kiosks' located?

There will be 41 Cyber Kiosks located within Police Scotland buildings throughout Scotland. These are listed in the table below.

Area	Station	Division
East	Larbert	C
	Stirling	C
	Glenrothes	P
	Dunfermline	P
	Gayfield	E
	Fettes	E
	Corstorphine	E
	St Leonards	E
	Livingston	J
	Dalkeith	J
	Galashiels	J
	Stewart Street	G
West	Helen Street (x2)	G
	Shettleston	G

OFFICIAL

	East Kilbride	Q
	Motherwell	Q
	Hamilton	Q
	Coatbridge	Q
	Paisley	K
	Greenock	K
	Ayr	U
	Kilmarnock	U
	Saltcoats	U
	Dumbarton	L
	Clydebank	L
	Dumfries	V
	Stranraer	V
North	Divisional HQ	D
	Downfield Dundee	D
	Perth	D
	Arbroath	D
	Kittybrewster	A
	Queens Street	A
	Elgin	A
	Fraserburgh	A
	Inverurie	A
	Fort William	N
	Inverness, Burnett Rd	N
	Alness	N
	Wick	N

Q4. Who operates the ‘Cyber Kiosks’?

Cyber Kiosks are only operated by specially trained police officers or Cybercrime staff who have completed and passed the Cyber Kiosk training course.

Q5. What training is required to use a Cyber Kiosk?

Before officers are authorised to examine devices using a Cyber Kiosk they must successfully complete the training course which teaches how the Cyber Kiosks must be used in accordance with the [Police Scotland Digital Device Examination Principles](#). This training is certified by the manufacturer of the Cyber Kiosks.

Q6. How does a 'Cyber Kiosk' work?

Cyber Kiosks use special computer software to view information stored within digital devices in a way which does not change the information on the device. The process involves:

- Digital device being connected to the Cyber Kiosk.
- Trained operator specifies the information type(s) and time period(s) which the investigating officer has identified as being of relevance to their investigation.
- The Cyber Kiosk thereafter searches the device and displays any matching information on screen.
- Information is then reviewed by the operator and the investigating officer to establish if there is evidence present and further examination is required by a Digital Forensic Hub
- All device **information is deleted** from the Cyber Kiosk when the examination is completed.

Q7. What if evidence is found?

If evidence is found on a digital device during Cyber Kiosk examination then the device will be submitted to a Police Scotland Digital Forensic Hub for further examination. This allows the evidence to be saved and presented in a format which is suitable for use in Court.

Q8. What if no evidence is found?

If no evidence is found when a digital device is examined using a Cyber Kiosk, then this provides the opportunity for the device to be returned to the owner; provided that it is not required for another evidential purpose such as fingerprint analysis.

Q9. Where can I find more information about 'Cyber Kiosks'?

Further information can be found on the [Police Scotland Cyber Kiosk Internet Page](#). This includes additional information about the examination process and a video which may address any questions you have.

Q10. What information can be viewed using a 'Cyber Kiosk'?

This will depend on the make and model of the device being examined (Apple, Samsung, Sony etc.), the operating system being used (Apple iOS, Android) and the nature of the investigation, however some examples of the type of information which can be viewed include:

Calendar Entries • Call Logs • Contact Lists • Emails • Internet History
Pictures • SMS Text Messages • Social Networking Chat Messages
User Account Information • Videos

The specific information which is viewed using a Cyber Kiosk will change depending on the circumstances of the case; however it must **always** be necessary, relevant, proportionate and justified.

Q11. Will 'Cyber Kiosks' in Scotland be used only to examine mobile telephones, tablets and associated memory and SIM cards?

Yes, and there are a number of specific circumstances where the use of Cyber Kiosks would not be appropriate, such as:

- The device does not work.
- The enquiry may involve indecent images of children.
- It is a Complaint Against the Police, Professional Standards Department or Anti-Corruption Unit enquiry.
- A police officer or member of police staff has established through own observations that the device contains material relevant to the enquiry.
- The device is anything other than a tablet, mobile phone, or **associated** memory or SIM card. (E.g. NO Lap-tops / Hard Drives / USB Drives / Loose Memory Cards).
- The device is in a foreign language.

OFFICIAL

In these cases devices will be submitted directly to the Cybercrime Hubs for examination and Cyber Kiosks will not be used.

Q12. Will Police Scotland 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.

Q13. What information is stored on the 'Cyber Kiosk'?

No device information is retained on the Cyber Kiosk after examination. The examination process allows the examiner to view information stored within the device, however **all** information is securely deleted from the Cyber Kiosk at the end of the examination.

The only information which is kept is:

- When the examination took place
- Who conducted the examination
- The Kiosk that carried out the transaction
- The device make and model
- The type of examination (logical, physical)
- Whether the examination was successful or not
- The case reference number
- The reporting officer
- The crime type
- Status of the device owner

This information is used to monitor the use of Cyber Kiosks throughout Scotland and is for statistical use only; it contains **no** personal information relating to the owner/user of the digital device.