



<b>Meeting</b>	<b>SPA Policing Performance Committee</b>
<b>Date</b>	<b>7 December 2022</b>
<b>Location</b>	<b>Video Conference</b>
<b>Title of Paper</b>	<b>Cyber Kiosk Update</b>
<b>Presented By</b>	<b>ACC Andy Freeburn, Organised Crime, CT and Intel</b>
<b>Recommendation to Members</b>	<b>For Discussion</b>
<b>Appendix Attached</b>	<b>No</b>

**PURPOSE**

The purpose of this briefing paper is to provide the Scottish Police Authority (SPA) Policing Performance Committee with an update regarding the use of Cyber Kiosks within Police Scotland and the associated Management Information (MI).

Members are invited to discuss the contents of the report.

## **1 BACKGROUND**

- 1.1. The purpose of this paper is to provide an update to the Committee in respect of Cyber Kiosks. Police Scotland last reported to the Committee in March 2022 where updates were provided on the background to Cyber Kiosks, how requests were managed, how devices were examined and the return of devices.
- 1.2 As the Committee are aware Cyber Kiosks, also known as a 'Digital Triage Devices', are desktop computers with specific software that enables specially trained Police Officers to view data stored on a mobile phone or tablet.
- 1.3 A total of 41 Cyber Kiosks were installed during a phased rollout which commenced in January 2020 in the Forth Valley (C) and Fife (P) Divisions and concluded in August 2020 in the Highlands and Islands (N), North East (A) and Tayside (D) Divisions. Dedicated Cyber Kiosk single point of contact (SPOC) Officers within management ranks are present in all Divisions, having responsibility for ensuring the security and upkeep of their respective Cyber Kiosks and maintaining records of trained Officers in their area.
- 1.4 Cyber Kiosks provide a triage capability which allows the contents of a digital device associated with a Police investigation or incident to be assessed to establish if evidence is present.
- 1.5 Since the conclusion of the rollout, governance and oversight of Cyber Kiosks within Police Scotland has been managed by SCD Cybercrime Digital Forensics, who have provided support in relation to maintenance, software updates and the dissemination of advice and guidance bulletins to Police Officers and staff across Scotland.
- 1.6 Police Scotland remains committed to demonstrating transparency and strict accountability in relation to the use of Cyber Kiosks, producing monthly management information detailing how many Cyber Kiosk examinations have been progressed in the previous month.

## **2 RECENT MEDIA REPORTING**

- 2.1. In early October 2022, Cyber Kiosks were the subject of negative newspaper headlines including claims that police were "Hacking" devices. This suggests an unlawful or unethical approach which is entirely inaccurate.

- 2.2. Police only utilise the technology provided by Cyber Kiosks by consent or with lawful authority, i.e. with a warrant at the direction of the COPFS or a specific legislative power.
- 2.3. The press headlines intimated that Police Scotland were seizing phones from victims of rape and sexual assault without their consent. We are committed to delivering a victim-centred, trauma informed approach and make every effort to obtain consent prior to taking possession of digital devices from a victim, however there are some circumstances when we are unable to do so. Within our statutory duty to investigate crime, we must secure all available evidence, whether inculpatory or exculpatory.
- 2.4. Police Scotland have also recently provided a detailed response to the Convener of the Criminal Justice Committee on this subject and provided reassurance around our robust governance and oversight processes to effectively manage all requests for the examination of a digital device.
- 2.5. We were also privileged to host the Convener of the Criminal Justice Committee at our newly opened Cyber facility in Aberdeen where the end to end process of digital forensics examinations was demonstrated. Officials and a Member of the SPA have also recently availed of an opportunity to visit our Cyber facility at Newbridge and met our staff and we welcome this continued oversight and engagement.
- 2.6. Police Scotland have continued to witness an increased proportion of threats, risks and harms moving to an online space and digital material is often critically important to our investigations. We completely understand the need to ensure public confidence and appropriate safeguards in utilising such technologies, however the challenge is to balance this against our statutory obligations to keep the public safe and make best use of available technologies to assist us in this mission.
- 2.7. In a number of recent UK conferences relating to cyber investigations, Police Scotland has been seen as an exemplar in not just balancing the legal implications of the police use of technology, but also the associated ethical considerations for victims and the public. This is fundamental to our considerations in applying our organisational values of fairness, integrity and respect and upholding human rights.
- 2.8. A summary of the figures shared with the Criminal Justice Committee is outlined below. The table below depicts information

indicating the number of devices taken from victims and is broken down for Rape and Sexual Assault.

	2019 <sup>1</sup>	2020	2021	2022
<b>Rape</b>				
Devices	70	157	108	93
<i>Devices (with consent)</i>	50	131	94	78
<b>Sexual Assault</b>				
Devices	17	36	22	23
<i>Devices (with consent)</i>	10	26	20	13

1 – Data are from 01 July 2019 onwards.  
Source: Cybercrime Case Management System

- 2.9. The cumulative total of all devices taken for rape and sexual assault since the advent of digital triage devices is therefore 526, of which 104 were seized through other lawful authority, i.e. in less than 20% of cases.
- 2.10. This is even smaller percentage (2%), when broken down against the total number of rape and sexual assault offences being investigated by Police Scotland during this time frame.
- 2.11. Whilst we are committed to delivering a victim-centred, trauma informed approach and make every effort to obtain consent prior to taking possession of digital devices from a victim, there are some circumstances when we are unable to do so. Within our statutory duty to investigate crime, we must secure all available evidence, whether inculpatory or exculpatory. We would seek to assure the Committee that taking such devices in the absence of consent is only conducted when the strict tests of proportionality and necessity are met and under a legal power.

**Policing, Crime, Sentencing and Courts Act 2022**

- 2.12 A further development to update the Committee on is the introduction of new legislation on 8 November 2022, entitled the Policing, Crime, Sentencing and Courts Act 2022. This legislation establishes a framework for the seizure of digital devices and the extraction of data which ensures that where consent is provided to

examine a device, the wishes of the owner are taken into consideration.

- 2.13 This legislation also ensures that the rights of children (under 18 years of age) and those unable to provide consent through capacity issues are met. This very much complements Police Scotland's current governance processes and provides further reassurance that the extraction of private data from devices is in accordance with current legislation.
- 2.14 Police Scotland has worked in collaboration with the Crown Office and Procurator Fiscals Service (COPFS) to provide guidance to the public which is available on our website and also to officers and staff through training products available internally on our intranet site.

### **Cyber Kiosk – Next Steps**

- 2.15 As envisaged during the introduction of Cyber Kiosks, Police Scotland wish to continue to review and enhance the service to the public. An example of this is that the 41 systems are currently not 'networked'. This is an extremely inefficient process meaning that important software and security updates and the capture of management cannot be performed remotely and can only be conducted by physically travelling round the 41 locations. Prior to making any changes in such processes we will be fully exploring and documenting any impact around human rights, ethics and data privacy, which will be conducted in consultation with the SPA.
- 2.16 Cyber Kiosks will also significantly benefit from developments to the the Police Scotland IT network, which will facilitate the rollout of a single national system to effectively record and monitor the movement of case-related productions (UNIFI). This system will deliver the capability to effectively record and monitor the movement of case-related productions and track them from the point of seizure, through to any examination processes, presentation at court and ultimate return to the owner. It will also apply to seized mobile phone devices and provide much-needed management information to allow Police Scotland to understand blockages and remedy any inefficient practices and processes. This element of work is being progressed as part of our 'Policing in a Digital World' programme and is due for completion in by the end of 2023.
- 2.17 The ability of Cyber Kiosks to provide an evidential product at the point of first opportunity is also being further explored as it should be noted that some of the issues arising from the slower return of

devices could be remedied by using the full capabilities of the system. This would mean that investigators could print or download relevant product at triage stage meaning that the majority of devices could be returned to the owner immediately. Once again, any such changes to these processes would only be conducted following rigorous assessment and engagement to ensure that any such benefits would not compromise the standards, safeguards and public confidence which we know is essential to maintain in the police use of technology.

## **Conclusion**

2.18 It is hoped that this update provides the Committee with continued assurance of our ongoing efforts to meet the requisite safeguards in using such technologies, whilst fulfilling our statutory obligations. Most of all, we wish to deliver for the victims of serious and sexual crime, in a world where we must compete with criminals who are harming and exploiting the public through these technologies.

## **3 FINANCIAL IMPLICATIONS**

3.1. There are no financial implications in this report.

## **4 PERSONNEL IMPLICATIONS**

4.1. There are no personnel implications in this report.

## **5 LEGAL IMPLICATIONS**

5.1. There are no legal implications in this report.

## **6 REPUTATIONAL IMPLICATIONS**

6.1. There are no reputational implications in this report.

## **7 SOCIAL IMPLICATIONS**

7.1. There are no social implications in this report.

## **8 COMMUNITY IMPACT**

8.1 It is anticipated that the ongoing publication of Management Information (MI) in respect of the use of Kiosks will provide a reassurance for our communities that the use of Cyber Kiosks within Police Scotland continues to be subject of robust governance and scrutiny.

## **9 EQUALITIES IMPLICATIONS**

9.1. There are no equality implications in this report.

## **10 ENVIRONMENT IMPLICATIONS**

10.1. There are no environmental implications in this report.

### **RECOMMENDATIONS**

Members are invited to acknowledge and discuss this report.