

Meeting	SPA Policing Performance
Date	17 March 2022
Location	Video Conference
Title of Paper	Cyber Kiosk Update
Presented By	ACC Tim Mairs, Organised Crime, Counter Terrorism and Intelligence
Recommendation to Members	For Discussion
Appendix Attached	No

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).

This paper will specifically provide a progress report in relation to:

- Agenda item 2.3 – Cyber Kiosk Update

This paper highlights the timeline/roadmap relating to the automated production of management information concerning the number of devices returned to their owners.

Members are invited to discuss the contents of this paper.

1. BACKGROUND

- 1.1. A Cyber Kiosk, also known as a 'Digital Triage Device', is a desktop computer with specific software installed that enables specially trained Police Officers to view data stored on a mobile phone or tablet. The introduction of Cyber Kiosks across Police Scotland was supported by scrutiny prior to their roll out, which was completed in August 2020.
- 1.2. 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. This allows lines of enquiry to be progressed at a much earlier stage and potentially allows devices to be returned to owners where it is established the device(s) is not the subject of any other enquiry or does not require any forensic examination for fingerprint or DNA evidence.
- 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.
- 1.4. 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.
- 1.5. A commitment was made publicly that Management Information (MI) would be extracted from the Cybercrime Case Management System (CMS) on a monthly basis. As such, information is drawn directly and automatically from the system and thereafter formulated to provide MI in an easy-to-read format reporting on:
 - CRIME GROUP/TYPE
 - REASON / PURPOSE OF EXAMINATION
 - REGION / UNIT / DIVISION / KIOSK
 - STATUS OF OWNER
 - DEVICE TYPE
 - POWER OF SEIZURE
 - DECLINED FORMS
- 1.6. Police Scotland remains committed to demonstrating transparency 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. FURTHER DETAIL ON THE REPORT TOPIC

Cyber Kiosk Examination Request Form (ERF) Management

- 2.1. As previously detailed in papers concerning Cyber Kiosks and their use within Police Scotland, all examination requests are subject of a comprehensive assessment by specialist staff within the Cybercrime Gateway before any examination can proceed. This assessment concerns the necessity, legality, proportionality and justification of any examination as well as the category and extent of information requested: for example SMS text messages and the time period of interest to the enquiry.
- 2.2. Where the Cybercrime Gateway are not satisfied that all of these criteria have been fully evidenced, the ERF is **declined** and returned to the Enquiry Officer for amendment or cancellation.
- 2.3. In addition to assessing Cyber Kiosk ERFs, the Cybercrime Gateway proactively assess incoming requests for *full* Cybercrime examinations by Digital Forensic Hub analysts to identify opportunities where the use of a Cyber Kiosk would increase the speed at which the evidential significance of devices could be ascertained. The default position within Police Scotland is that all mobile telephones and portable devices are triaged using a Cyber Kiosk in the first instance, where permissible, to prevent devices being retained for any longer than absolutely necessary. It should be noted that in cases where there is sufficient evidence to charge an individual due to witness statements, forensic evidence etc., devices are not subject to a kiosk examination. Having every device subject to a Cyber Kiosk examination will ensure only devices requested by the Crown Office and Procurator Fiscal Service and suitable for examination will be passed to a hub.
- 2.4. In order to ensure that Cyber Kiosk examinations are progressed timeously, enhanced administrative measures have been introduced to provide guidance to Enquiry Officers and their Supervisors regarding Cyber Kiosk examinations which have not yet been undertaken. These measures have been developed to ensure that, following approval, Cyber Kiosk examinations are progressed timeously, with comprehensive support and guidance available regarding the initial request and subsequent examination processes.
- 2.5. 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. The Cybercrime Unit regularly liaise with Cyber Kiosk SPOCs regarding training and resource availability to identify any emerging concerns and opportunities for further development of Kiosk trained Officers. As we continue to emerge from COVID-19 restrictions and guidance in the workplace, there are plans to review how best we deliver continuous professional development (CPD) events across Scotland to encourage the sharing of best practice and experience amongst Kiosk operators.

Cyber Kiosk – Negative Examinations

- 2.6. Between 20 January 2020 and 28 February 2022, a total of **3475** Cybercrime ERFs were progressed using the 41 Cyber Kiosks located across Scotland, accounting for the digital forensic triage of over **6000** devices.¹
- 2.7. As of 28 February 2022, **1139** of these ERFs have been recorded as '**Negative**' meaning that of the devices examined from these ERFs, none contain material of evidential significance to the crime or incident under investigation. This equates to a total of **1899** devices which were thereafter *potentially* suitable for return to the owner having been assessed as not containing any evidential material (see Section 2.9).
- 2.8. A significant number of individual devices marked as negative as a single entity, will be part an ERF that has been marked as '**Positive**' as only one device within the request needs to contain evidential material for the case to be marked as '**Positive**'. This would potentially mean that the device may be kept by Police and not returned to the owner as part of a wider investigation. At this time it is not possible to accurately report on these devices without reviewing every individual case.

Cyber Kiosk - Return of Devices

- 2.9. It is important to note that the decision to return an item to the owner or next of kin is taken by the Enquiry Officer and not staff within Cybercrime and can be influenced by a number of factors in addition to the presence of digital evidence, such as the devices may be required for DNA / Fingerprint examination or a be part of a wider criminal investigation which remains ongoing.

¹ Data obtained from the Cybercrime Case Management System 1400 hours 3rd March 2022.

- 2.10. Furthermore, in circumstances where a report has been submitted to the Procurator Fiscal, for example a reported crime or a death investigation, devices can only be returned to the owner upon COPFS issuing a 'Productions Release Authorisation' confirming that proceedings have been concluded.
- 2.11. As the Cybercrime Case Management System operates in isolation from the production and crime recording applications used across Scotland, it is **not** currently possible to obtain information regarding devices which have been returned to their owners without manually querying each individual case and device and thereafter contacting the relevant Divisional production keeper to ascertain the current status of each device.
- 2.12. In May 2021, a manual 'dip-sample' was conducted in relation to devices which had been recorded as '**Negative**' to establish how many had been returned to the owner or next of kin. This showed that 86% of devices belonging to witnesses and victims of crime had been returned to the owner following a negative examination.²
- 2.13. The Cybercrime Unit continue to engage with the Core Operational Solutions (COS) team to ensure opportunities are maximised to automate this process as bespoke applications for production management and crime recording are introduced throughout Police Scotland.

Conclusion

- 2.14. The introduction of Cyber Kiosks across Police Scotland has provided the means by which the evidential significance of devices can be ascertained quicker than was previously possible within Digital Forensic Hubs. This is the case due to the ability to view the content of a device and confirm whether the device contains data which is of evidential value. This increase in efficiency allows Enquiry Officers to make informed decisions as to whether or not it is legal, necessary, proportionate and justified to retain devices and, where permissible, if the device contains no data of evidential value, return the device to the owner at the earliest opportunity.
- 2.15. At present Police Scotland uses two different systems to record information concerning recorded crimes and associated productions, including electronic devices seized for Cyber Kiosk triage.

² Previous paper "Digital Triage Device (Cyber Kiosk Update)" submitted to SPA Policing Performance Committee: <https://www.spa.police.uk/spa-media/zrghaih/rep-20210607-item-5-2-digital-triage-device-cyber-kiosks-update-doc-new.pdf>, page 5.

- 2.16. As there are multiple systems used, it is not currently possible to obtain accurate and comparable automated Management Information regarding devices which have been returned to their owner following Cyber Kiosk examination.
- 2.17. As part of the Digitally Enabled Policing Programme (DEPP), Core Operational Solutions (COS) is responsible for the delivery of a suite of applications (Unify) which are designed to streamline the recording and management of core operational information and supporting activity.
- 2.18. Police Scotland are in the process of delivering the production management aspect of this suite (Unify) across all areas, with an approximate completion by the end of **August 2022**. From that date forwards, for devices seized thereafter, the return rate of devices will be available through the appropriate management information queries being set up. Criminal Justice Service Division are the owners of the Management Information relevant to production system.
- 2.19. The introduction of this system will not allow for the retrospective creation of baseline information on the timescales involved in returning devices to owners and there is no pre DTD baseline data available for comparison.

3. FINANCIAL IMPLICATIONS

- 3.1. There are no financial implications with the report.

4. PERSONNEL IMPLICATIONS

- 4.1. There are no personnel implications with the report

5. LEGAL IMPLICATIONS

- 5.1. There are no legal implications with the report

6. REPUTATIONAL IMPLICATIONS

- 6.1. There are no reputational implications with the report.

7. SOCIAL IMPLICATIONS

- 7.1. There are no social implications with the 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 equalities implications with the report.

10. ENVIRONMENT IMPLICATIONS

- 10.1. There are no environmental implications with the report.

RECOMMENDATIONS

Members are invited to discuss the content of this report.