SCOTTISH POLICE AUTHORITY
ÙGHDARRAS POILIS NA H-ALBA

Agenda Item 2.1

Meeting	**SPA Policing Performance Committee**
Date	**12 September 2023**
Location	**Video Conference**
Title of Paper	**Cyber Kiosk Update**
Presented By	**ACC Andy Freeburn - Organised Crime, CT and Intel**
Recommendation to Members	**For Discussion**
Appendix Attached	**Yes** **Appendix A – Cyber Kiosk Location Chart** **Appendix B – Cyber Kiosk ERF Process** **Appendix C – Cyber Kiosk Management Information July 2023**

PURPOSE

The purpose of this briefing paper is to provide the Scottish Police Authority (SPA) Policing Performance Committee with an update regarding the current use of Cyber Kiosks within Police Scotland including the Management Information (MI) published on a monthly basis and the proposed networking of Cyber Kiosks.

This paper will also seek to address action PPC 20221207-004 - **Cyber Kiosks –** Police Scotland to bring a paper to a future committee which provides further detail on the necessity and proportionality of the model, including safeguards, risks and efficiency improvements.

Members are invited to discuss the content of this report and agree regularity of future 'Policing in a Digital World Programme' reporting.

1. BACKGROUND

1.1. A Digital Triage Device, also known as a 'Cyber Kiosk', is a desktop computer with specific software installed which 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 significant scrutiny encompassing engagement with Stakeholder Groups, External Reference Groups and legal opinion by both Senior Counsel and Crown Office and Procurator Fiscal Service (COPFS) prior to their roll out, which was completed in August 2020.

1.2. Police Scotland use Cyber Kiosks solely to provide an initial triage capability which allows the contents of a digital device associated with a criminal investigation or incident to be assessed to establish if evidence is present. This capability allows lines of enquiry to be identified and progressed at a much earlier stage than would have been possible prior to the introduction of Cyber Kiosks. This process can negate the need for full digital forensic examination at a digital forensic hub, minimising intrusion and providing a better service to victims in particular and public.

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 **(Appendix A- Cyber Kiosk Location Chart)**. Police Scotland have maintained the original 41 Kiosks.

1.4 Police Scotland have continued to witness an increased proportion of threats, risks and harms moving to an online space and digital material is more critically important to investigations than ever before. Police Scotland have learned from the roll out of Cyber Kiosks and consequently developed a Rights Based Pathway to enhance our ability to assess new technology and the associated ethical considerations for victims and the public.

1.5 We absolutely understand the need to ensure public confidence is maintained and the appropriate safeguards are in place when utilising such technologies. However the challenge we must meet is to balance our statutory obligations to keep the public safe and make the best use of available technologies to assist us in this mission. This is fundamental to our considerations in applying our organisational values of fairness, integrity and respect and upholding human rights.

1.6 Since the conclusion of the rollout, management 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.

1.7 The request to use a Cyber Kiosk is assessed on a case by case basis by the Cybercrime Gateway staff. They determine the legality, necessity, justification and proportionality of *each* examination *prior* to their approval for its use. It is the responsibility of the Cybercrime Gateway to assess every Kiosk examination in line with Police Scotland's Digital Device Examination Principles and satisfy themselves that the following conditions are met:

- Triage is in relation to an investigation or incident,
- The device was lawfully obtained,
- The examination is lawful,
- If authority is by virtue of consent,
- The device has been lodged,
- Collateral intrusion is minimised to support evidence for the investigation.

The full authorisation process is documented in **Appendix B – Cyber Kiosk ERF Process.**

1.8. As part of the introduction of Kiosks public commitment was made to publish data relating to the use of Cyber Kiosks. This information is referred to as Management Information (MI) and is publicly available on the Police Scotland web site in an easy-to-read format reporting on:

- Status of Owner/Power of Seizure – Devices seized using Common Law Powers,
- Status of Owner/Power of Seizure – Devices seized under warrant,
- Status of Owner/Power of Seizure – Devices seized using statutory powers,
- Status of Owner/Power of Seizure – Devices seized voluntarily (with authority of the owner),
- Reason for Device Examination,
- Cyber Kiosk Examination Requests – Declined,
- Cyber Kiosk Examination Requests – Completed,
- Cyber Kiosk Examination Requests – Crime Group.

Appendix C - Cyber Kiosk Management Information for July 2023

2. CYBER KIOSK PROCESSES

2.1 A very small number of Kiosk examinations are of victim and witness devices. This is supported by statistical analysis, documented in Appendix C, which shows that in July 2023, of 401 devices seized only 16 belonged to victims and witnesses. Of those 16, nine were seized under common law and seven with consent of the owner. There were none seized under warrant or statutory power.

2.2 The reason for a victim or witness device being in the minority is that Cyber Kiosk are used exclusively to establish whether a device contains evidentially relevant material. Therefore in circumstances where the enquiry officer has been shown content and is thereby satisfied that relevant material is contained on the device, Kiosk examination would not be appropriate and the device would instead go to the Digital Forensic hub for examination and extraction of evidential material. In this way we can support victims more effectively rather than placing the device in the queue for lab examination, the examination is generally done by arrangement; the Victim or Witness attending at a Digital Forensic Hub at their earliest convenience.

CURRENT CYBER KIOSK PERFORMANCE

2.3 The Management Information (MI) which is published on a monthly basis in respect of use of Cyber Kiosks is detailed and robust.

2.4 Although a Kiosk examination can assist with insight into the evidential value of a device, the decision on whether a device can be returned to the owner on conclusion of Kiosk examination depends on other criminal justice process factors; depending on the stage in the criminal justice process the decision will rest either with the enquiry officer, or the COPFS – never the Kiosk operator.

2.5 With respect to the return of devices, recent Crown Office and Procurator Fiscal Service (COPFS) guidance provides:

'In terms of this guidance prosecutors are under an obligation that where a device can appropriately be returned to its user they should do so at the earliest opportunity. Before a case has been reported Police Scotland have to decide whether it can be returned. Once a case has been marked for prosecutorial action the responsibility for determining whether to return the devices lies with the prosecutor.

Some of the following factors will be taken into account when deciding whether a device can be returned.

- *Whether there is an alternative way to secure the required information,*
- *Whether all of the relevant information has already been extracted from the device,*
- *Whether the device itself is required as evidence,*
- *The significance of the information,*
- *The views of the child witness (where the device belongs to a child),*
- *The reasons for the request.*

It will not be appropriate to return a device where it may prejudice the defence or where the device contains illegal images or has been used in the commission of an offence.'

2.6 Details relating to the return of devices to owners is therefore not recorded on the Kiosk, CMS, or other Cybercrime system, and not published as part of Kiosk MI.

2.7 There is currently no single search across Police Scotland systems that can establish when devices that have undergone Kiosk examination have been returned to their owner. The national roll out of Core Operating Solutions (COS) includes a productions module. That system currently identifies if a production is a mobile phone and if it is retained or disposed of, but not how it has been disposed, for example, destroyed or returned to owner. Future enhancements may include the type of disposal and disposal instructor (Police / COPFS) but this enhancement if required will not be developed until the end of 2024 at the earliest due to other priorities. The inability to measure this was an omission in the delivery of Cyber Kiosks and something that we have learned from, for example in how we have recently implemented other technologies such as CAID FM.

2.8 Management Information relating to the use of Cyber Kiosks is currently drawn from two main sources; the Cybercrime Case Management System (CMS), and the Cyber Kiosks themselves.

2.9 The CMS sits on the Police Scotland network and is a system used to record details of device examinations from initial request, through approval process and to examination outcome. The information on the CMS includes, but is not limited to, the number and type of devices being examined, and the Cyber Kiosk at which the examination took place.

2.10 Through the use of analytical tools, MI from the CMS relating to use of Kiosks can be readily collated, analysed and presented in the agreed format, ready for publication on the Police Scotland web-site. The MI gleaned from the CMS can be cross referred with the MI on the Cyber Kiosks themselves for audit and quality assurance purposes. However currently the Cyber Kiosks are standalone with no connection to the Police Scotland network. The only way to collect the MI for comparison is through manual extraction at each Kiosk location.

2.11 The MI extraction can only be carried out by *qualified Cybercrime Digital Forensic staff*, with monthly extraction involving considerable travel to reach each of the 41 Cyber Kiosk locations. With significant geographical spread of the Kiosks – from Dumfries in the South of Scotland, to Wick in the North - this travel represents significant staff abstraction and travel costs, particularly with some locations being so far from the Cybercrime Hubs as to require overnight accommodation.

2.12 It is worth noting that the Kiosk visits also serve as an opportunity to quality check the Kiosks and associated equipment, and opportunity to carry out any required software updates; however, the absence of networking to allow remote access to the Kiosks via the Digital Forensic hubs means that any maintenance, upgrades, or other problem solving required out-with the visits, ultimately result in further in-person attendance at a Kiosk.

CYBER KIOSKS 2

2.13 The proposal for the networking of Cyber Kiosks is borne from the clear efficiency improvements which the remote collation of MI and updating of software, via the Digital Forensic hubs, could bring to Digital Forensics. This would ensure that highly skilled staff are being tasked to deliver the service provision which Digital Forensics provides to Police Scotland and the wider criminal justice process is as efficient as possible. There would also be the associated financial savings and the crucial improvement of the welfare of those staff currently travelling significant distances each month for a task which could be completed at their current places of work.

2.14 **The networking of the Cyber Kiosks would not in any way change the management, safeguards, practices, processes and procedures currently in place. No additional data other than that which is collected currently by physically attending at each Kiosk would be obtained by the networking. No content of any device being examined would be transferred remotely from the Cyber Kiosk to any of the Digital Forensic hubs or other locations. As such the networking of Kiosk does not in any way introduce an increased 'risk' to either the owner of the device or to Police Scotland.**

2.15 In essence the only change which the networking of Cyber Kiosks proposes is the fact that there would no longer be a requirement to physically visit 41 locations.

2.16 At the current time the technical feasibility of the networking of the Cyber Kiosks is being explored by Police Scotland Digital Division. This encompasses assurances that Police Scotland current technical architecture is suitable to facilitate the requirements of networking of Cyber Kiosks and if required establish associated costs and requirements to facilitate this.

2.17 When the appropriate technical solution has been identified the networking of Cyber Kiosks will then undertake the 'Rights Based Pathway' to ensure that it is subject to the robust process and procedures previously endorsed by the SPA.

CYBER KIOSKS - THE FUTURE

2.18 In addition to the MI currently published on a monthly basis, it is the intention of Police Scotland to develop a public facing Code of Practice to articulate our commitments to the public in respect of the use of Cyber Kiosks.

2.19 It is known within UK Law Enforcement that the use of Cyber Kiosks is wider than in Scotland and thereby facilitates further efficiencies to Digital Forensics beyond networking. In furtherance of this, Police Scotland, through the Policing in a Digital World Programme in conjunction with Digital Forensics, will continue to engage with Law Enforcement Agencies across the UK and internationally to benchmark that use.

2.20 Any future expansion of the technical capabilities of Cyber Kiosks will be carefully considered with any proposed increase in capability being explored robustly, lawfully and adhering to the 'Rights Based Pathway'. In addition, Police Scotland will review and explore opportunities with other programmes in Police Scotland, in particular the Digital Evidence Sharing Capability (DESC), to understand the ability to integrate and provide further efficiencies in the sharing of Digital Evidence.

SUMMARY

2.21 In summary, Cyber Kiosks 2 will deliver efficiency and improvement to Digital Forensics, whilst maintaining transparency on their use through production of MI data, safeguarding the processes and risks surrounding the use of Cyber Kiosk. Future development and use of the capabilities of Cyber Kiosks will be fully explored utilising the "Rights Based Pathway" and it is proposed that this will be regularly reported to future SPA Policing Performance Committees alongside wider developments in the Policing in a Digital World Programme.

3. FINANCIAL IMPLICATIONS

3.1 There are financial implications for Police Scotland due to the technical infrastructure which will be required to network Cyber Kiosks. As this work is in it's infancy at the current time the cost of this is undefined at present.

3.2 There would be financial savings realised through networking due to the current requirements to travel to 41 locations with associated costs of fuel and accommodation no longer being required.

4. PERSONNEL IMPLICATIONS

4.1 There would be benefits to Police Scotland personnel as Digital Forensic staff would no longer be required to reside away from their home address or travelling hours in vehicles when obtaining Cyber Kiosk MI.

5. LEGAL IMPLICATIONS

5.1 There are no legal implications with the report.

6. REPUTATIONAL IMPLICATIONS

6.1 As there is no expansion of capability of Cyber Kiosks by networking there should be no reputational implications. That being said there has been continual media interest in Cyber Kiosks and on occasion inaccurate reporting. There is a likelihood that the media will continue to maintain an interest in Cyber Kiosk use by Police Scotland moving forward.

7. SOCIAL IMPLICATIONS

7.1 There are no social implications in this report.

8. COMMUNITY IMPACT

8.1 There are no community implications in this report.

9. EQUALITIES IMPLICATIONS

9.1 There are no equality implications in this report.

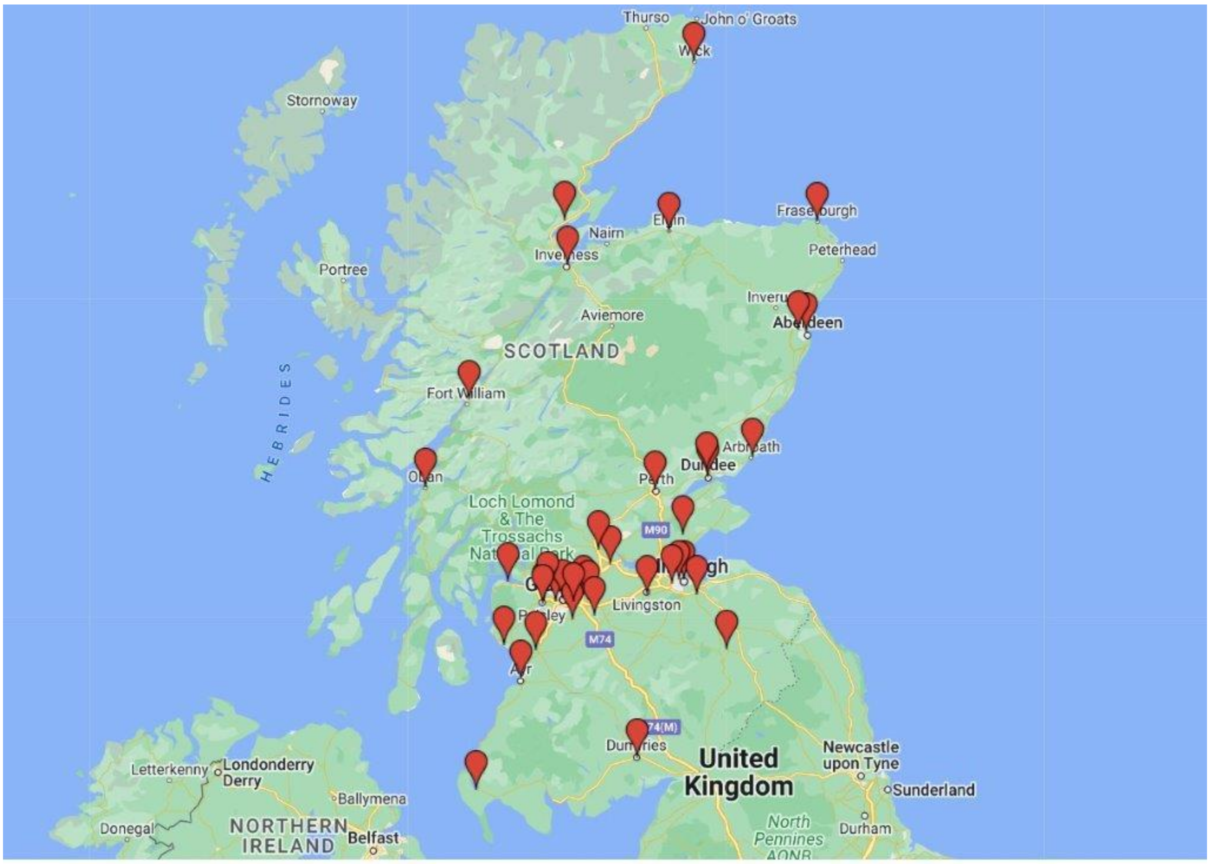
10. ENVIRONMENT IMPLICATIONS

10.1 There are positive environmental implications in this report as Police vehicles would no longer be making unnecessary journeys totalling hundreds of miles on a monthly basis.

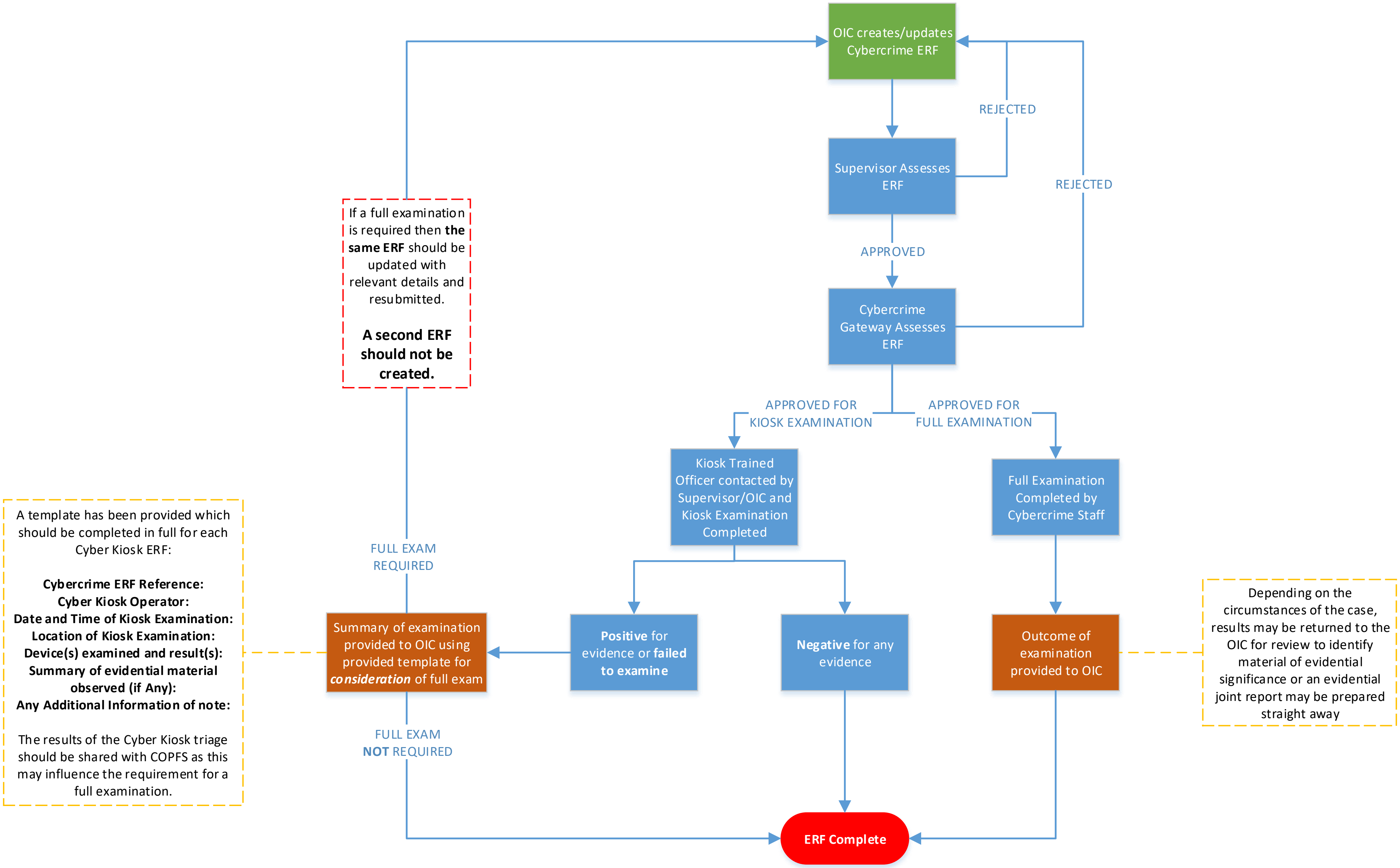
RECOMMENDATIONS

Members are invited to discuss the content of this report and agree regularity of future 'Policing in a Digital World Programme' reporting.

Appendix A- Cyber Kiosk Location Chart



SCD Cybercrime – Cybercrime ERF Process Flow



OIC creates/updates Cybercrime ERF

Supervisor Assesses ERF

REJECTED

APPROVED

Cybercrime Gateway Assesses ERF

REJECTED

APPROVED FOR KIOSK EXAMINATION

APPROVED FOR FULL EXAMINATION

Kiosk Trained Officer contacted by Supervisor/OIC and Kiosk Examination Completed

Full Examination Completed by Cybercrime Staff

Positive for evidence or **failed to examine**

Negative for any evidence

Outcome of examination provided to OIC

Summary of examination provided to OIC using provided template for ***consideration*** of full exam

FULL EXAM REQUIRED

FULL EXAM **NOT** REQUIRED

ERF Complete

If a full examination is required then **the same ERF** should be updated with relevant details and resubmitted.

A second ERF should not be created.

A template has been provided which should be completed in full for each Cyber Kiosk ERF:

Cybercrime ERF Reference:
Cyber Kiosk Operator:
Date and Time of Kiosk Examination:
Location of Kiosk Examination:
Device(s) examined and result(s):
Summary of evidential material observed (if Any):
Any Additional Information of note:

The results of the Cyber Kiosk triage should be shared with COPFS as this may influence the requirement for a full examination.

Depending on the circumstances of the case, results may be returned to the OIC for review to identify material of evidential significance or an evidential joint report may be prepared straight away

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Cyber Kiosk Management Information

Public Document

July 2023

Contents

Cyber Kiosks – Overview

Also known as a ‘Digital Triage Device’, a Cyber Kiosk is a desktop computer specifically designed to view data stored on a digital device in a targeted and focused way. Cyber Kiosks are operated by Kiosk Operators who are responsible for carrying out the 'triaging' of devices. Kiosk Operators can set parameters e.g. restricting searches to a date/time range, searching only text messages/photographs. If, after examination, no evidence is found, the device may be returned to the owner. There are 41 Cyber Kiosks located in Police Scotland buildings across Scotland.

Cyber Kiosk Public Commitment

Police Scotland has made a public commitment to publish data relating to the use of Cyber Kiosks. This data is referred to as Management Information (MI) and is taken on a monthly basis from the Cybercrime Case Management System (CMS); a system used by Police Scotland to record all requests for digital device examination, document the required approval process and to record the number and type of devices examined. This information is recorded on an Examination Request Form (ERF). The Cybercrime Case Management System (CMS) records information entered by the Investigating Officer at the time of initial submission. Management Information from the CMS is accurate at the time of retrieval however may not reflect any operational developments or administrative amendments which occur following submission, for example the status of a Subject changing as an enquiry develops.

Cyber Kiosk Management Information

Police Scotland undertake to each calendar month collate and present in a clear and precise manner the number of Kiosk examinations which have taken place. As an ERF can contain more than one device for examination, the number of devices examined will be presented rather than the number of ERFs. Information from the Cybercrime Case Management System (CMS) will be collated at the start of the calendar month and is accurate as of the specific time and date of retrieval.
In addition to the overall numbers, the following will also be reported on:

- Status of Owner – whether the device owner is a Complainer, Deceased, Missing Person, Not Officially Accused, Officially Accused or a Witness.
- Power of Seizure – the authority under which Police have taken possession of the device; Common Law, under Warrant, Statutory or Voluntary (consent).
- Reason for Device Examination – criminal investigation, death enquiry, instructed by Procurator Fiscal, missing person or National Security.
- Declined Forms – the number of examination requests declined by either Supervisory officer or the Cybercrime Gateway. Forms can be declined for many reasons, including the test of necessity and proportionality not having been met, but more commonly this is for administrative reasons such as the form containing insufficient detail or being incorrectly completed. In many cases amendments will be made and the form re-submitted.
- Completed Examinations – the number of Cyber Kiosk ERFs and devices completed, broken down by each Division.
- Crime Group & Crime Type – Crime Group is the overarching crime category and the Crime Types are sub-categories of the Group. For example, ‘Crimes of Dishonesty’ is a Crime Group with the sub-categories – the Crime Types – including Theft, Fraud and Housebreaking.

In February 2022 Police Scotland introduced a revised Communications' Accessibility Strategy to comply with the Public Sector Bodies (Website and Mobile Applications) (No. 2) Accessibility Regulations 2018. This new strategy required a holistic review be undertaken of the information published by Police Scotland in relation to Cyber Kiosk to ensure that this was explained in context throughout the document and in an easy to understand format which was accessible to all.

In order to comply with the required changes in document accessibility, there are a number of minor changes which have been made to the layout and format of this document, and the granularity of information has been revised to make this as easy to interpret as possible and avoid unnecessarily complex charts and tables. The key changes from previous data are as follows:

1. The previously published flowchart depicting the ERF submission process has been removed as this was not compatible with accessibility software

2. The previously published "Table 1 Status of Owner / Power of Seizure" has now been split into four sub tables 1A – 1D in order to display this information in a more accessible format. This breaks down the number of devices seized using Common Law powers, warrant, statutory powers and voluntarily (with the consent of the owner) into separate tables, however the underlying information remains the same.

3. The previously published "Table 2 Status of Owner / Reason for Device Examination" has been narrowed in scope to "Reason for Device Examination" as the Status of Owner information was duplication of information shown in table 1.

4. The previously published tables 3, 4 and 5 – "Cyber Kiosk Examination Kiosk Declined / Completed East/North/West" have been revised and now present the number of ERFs and Devices declined in all Divisions on one page (table 3), and the number of ERFs and Devices completed in all Division on one page (table 4).

5. The previously published table 6 "Crime Group & Crime Type" have been separated into two separate tables – Crime Group (table 5) and Crime Type (table 6) in order to present this information in a more accessible format.

The information contained within this document remains consistent with commitments made regarding accountability and transparency concerning the use of Cyber Kiosks within Scotland.

For ease of reference, the Management Information has been laid out in tables, grouped as follows:
Table 1A Status of Owner / Power of Seizure – Devices seized using Common Law Powers
Table 1B Status of Owner / Power of Seizure – Devices seized under warrant
Table 1C Status of Owner / Power of Seizure – Devices seized using statutory powers
Table 1D Status of Owner / Power of Seizure – Devices seized voluntarily (with consent of the owner)
Table 2 – Reason for Device Examination
Table 3 – Cyber Kiosk Examination Requests – Declined
Table 4 – Cyber Kiosk Examination Requests – Completed
Table 5 – Cyber Kiosk Examination Requests – Crime Group

All information was extracted from the Cybercrime Case Management Systems (CMS) on 1st August 2023 and may be subject to change due to operational or investigative developments.

Table 1 – Status of Owner / Power of Seizure – July 2023

Table 1A – Devices seized using Common Law powers

Status Of Owner	ERFs	Devices
Complainers	5	6
Deceased Persons	39	49
Missing Persons	2	3
Not Officially Accused Persons	58	77
Officially Accused Persons	36	51
Witnesses	2	3
Persons Unknown	15	22

Information presented in the above table:

5 ERFs (6 devices) were completed where devices belonged to complainers and were seized using common law powers.

39 ERFs (49 devices) were completed where devices belonged to deceased persons and were seized using common law powers.

2 ERFs (3 devices) were completed where devices belonged to missing persons and were seized using common law powers.

58 ERFs (77 devices) were completed where devices belonged to not officially accused persons and were seized using common law powers.

36 ERFs (51 devices) were completed where devices belonged to officially accused persons and were seized using common law powers.

2 ERFs (3 devices) were completed where devices belonged to witnesses and were seized using common law powers.

15 ERFs (22 devices) were completed where devices belonged to persons unknown and were seized using common law powers.

Table 1B – Devices seized under warrant

Status Of Owner	ERFs	Devices
Complainers	-	-
Deceased Persons	1	1
Missing Persons	-	-
Not Officially Accused Persons	25	54
Officially Accused Persons	20	54
Witnesses	-	-
Persons Unknown	11	24

Information presented in the above table:

No ERFs were completed where devices belonged to complainers and were seized under warrant.

1 ERF (1 device) was completed where devices belonged to deceased persons and were seized under warrant.

No ERFs were completed where devices belonged to missing persons and were seized under warrant.

25 ERFs (54 devices) were completed where devices belonged to not officially accused persons and were seized under warrant.

20 ERFs (54 devices) were completed where devices belonged to officially accused persons and were seized under warrant.

No ERFs were completed where devices belonged to witnesses and were seized under warrant.

11 ERFs (24 devices) were completed where devices belonged to persons unknown and were seized under warrant.

Table 1C – Devices seized using statutory powers

Status Of Owner	ERFs	Devices
Complainers	-	-
Deceased Persons	-	-
Missing Persons	-	-
Not Officially Accused Persons	13	20
Officially Accused Persons	13	20
Witnesses	-	-
Persons Unknown	5	8

No ERFs were completed where devices belonged to complainers and were seized using statutory powers.

No ERFs were completed where devices belonged to deceased persons and were seized using statutory powers.

No ERFs were completed where devices belonged to missing persons and were seized using statutory powers.

13 ERFs (20 devices) were completed where devices belonged to not officially accused persons and were seized using statutory powers.

13 ERFs (20 devices) were completed where devices belonged to officially accused persons and were seized using statutory powers.

No ERFs were completed where devices belonged to witnesses and were seized using statutory powers.

5 ERFs (8 devices) were completed where devices belonged to persons unknown and were seized using statutory powers.

Table 1D – Devices seized voluntarily (with consent of owner)

Status Of Owner	ERFs	Devices
Complainers	2	3
Deceased Persons	1	1
Missing Persons	-	-
Not Officially Accused Persons	-	-
Officially Accused Persons	-	-
Witnesses	4	4
Persons Unknown	1	1

Information presented in the above table:

2 ERFs (3 devices) were completed where devices belonged to complainers and were seized with the express consent of the owner.

1 ERF (1 device) was completed where devices belonged to deceased persons and were seized with the express consent of the owner.

No ERFs were completed where devices belonged to missing persons and were seized with the express consent of the owner.

No ERFs were completed where devices belonged to not officially accused persons and were seized with the express consent of the owner.

No ERFs were completed where devices belonged to officially accused persons and were seized with the express consent of the owner.

4 ERFs (4 devices) were completed where devices belonged to witnesses and were seized with the express consent of the owner.

1 ERF (1 device) was completed where devices belonged to persons unknown and were seized with the express consent of the owner.

Table 2 - Reason for Device Examination – July 2023

Reason For Examination	ERFs	Devices
In Relation To A Criminal Investigation	134	238
In Relation To A Death Enquiry	44	60
In Accordance With An Instruction From The Procurator Fiscal	45	98
In Relation To A Missing Person Enquiry	2	3
For The Purposes Of Protecting National Security	-	-
For Purposes Which Were Not Detailed By The Investigating Officer.	-	-

Information presented in the above table:

134 ERFs (238 devices) were completed in relation to a criminal investigation.

44 ERFs (60 devices) were completed in relation to a death enquiry.

45 ERFs (98 devices) were completed in accordance with an instruction from the Procurator Fiscal.

2 ERFs (3 devices) were completed in relation to a missing person enquiry.

No ERFs were completed for the purposes of protecting National security.

No ERFs were completed for purposes which were not detailed by the Investigating Officer.

Table 3 - Cyber Kiosk Examination Requests – Declined – July 2023

Division	ERFs Declined	Devices Declined
A Division	15	28
D Division	7	10
N Division	13	28
C Division	5	13
E Division	10	15
J Division	12	22
P Division	8	12
G Division	19	30
K Division	7	12
L Division	10	15
Q Division	13	19
U Division	5	6
V Division	4	5
Specialist Crime Division	3	5

Information presented in the above table:

15 Cyber Kiosk ERFs (28 devices) were declined by either the authorising supervisor or the Cybercrime Gateway in A Division.

7 Cyber Kiosk ERFs (10 devices) were declined by either the authorising supervisor or the Cybercrime Gateway in D Division.

13 Cyber Kiosk ERFs (28 devices) were declined by either the authorising supervisor or the Cybercrime Gateway in N Division.

5 Cyber Kiosk ERFs (13 devices) were declined by either the authorising supervisor or the Cybercrime Gateway in C Division.

10 Cyber Kiosk ERFs (15 devices) were declined by either the authorising supervisor or the Cybercrime Gateway in E Division.

12 Cyber Kiosk ERFs (22 devices) were declined by either the authorising supervisor or the Cybercrime Gateway in J Division.

8 Cyber Kiosk ERFs (12 devices) were declined by either the authorising supervisor or the Cybercrime Gateway in P Division.

19 Cyber Kiosk ERFs (30 devices) were declined by either the authorising supervisor or the Cybercrime Gateway in G Division.

7 Cyber Kiosk ERFs (12 devices) were declined by either the authorising supervisor or the Cybercrime Gateway in K Division.

10 Cyber Kiosk ERFs (15 devices) were declined by either the authorising supervisor or the Cybercrime Gateway in L Division.

13 Cyber Kiosk ERFs (19 devices) were declined by either the authorising supervisor or the Cybercrime Gateway in Q Division.

5 Cyber Kiosk ERFs (6 devices) were declined by either the authorising supervisor or the Cybercrime Gateway in U Division.

4 Cyber Kiosk ERFs (5 devices) were declined by either the authorising supervisor or the Cybercrime Gateway in V Division.

3 Cyber Kiosk ERFs (5 devices) were declined by either the authorising supervisor or the Cybercrime Gateway in Specialist Crime Division.

Table 4 – Cyber Kiosk Examination Requests – Completed – July 2023

Division	ERFs Completed	Devices Completed
A Division	40	61
D Division	16	22
N Division	11	20
C Division	7	22
E Division	25	47
J Division	13	25
P Division	13	24
G Division	29	42
K Division	12	18
L Division	9	13
Q Division	19	49
U Division	9	12
V Division	13	25
Specialist Crime Division	11	25

Information presented in the above table:

40 Cyber Kiosk ERFs (61 devices) were completed in A Division.

16 Cyber Kiosk ERFs (22 devices) were completed in D Division.

11 Cyber Kiosk ERFs (20 devices) were completed in N Division.

7 Cyber Kiosk ERFs (22 devices) were completed in C Division.

25 Cyber Kiosk ERFs (47 devices) were completed in E Division.

13 Cyber Kiosk ERFs (25 devices) were completed in J Division.

13 Cyber Kiosk ERFs (24 devices) were completed in P Division.

29 Cyber Kiosk ERFs (42 devices) were completed in G Division.

12 Cyber Kiosk ERFs (18 devices) were completed in K Division.

9 Cyber Kiosk ERFs (13 devices) were completed in L Division.

19 Cyber Kiosk ERFs (49 devices) were completed in Q Division.

9 Cyber Kiosk ERFs (12 devices) were completed in U Division.

13 Cyber Kiosk ERFs (25 devices) were completed in V Division.

11 Cyber Kiosk ERFs (25 devices) were completed in Specialist Crime Division.

Table 5 - Cyber Kiosk Examinations – Crime Group – July 2023

Crime Group	ERFs Completed	Devices Completed
Group 1: Non Sexual Crimes Of Violence	29	51
Group 2: Sexual Crimes	35	38
Group 3: Crimes Of Dishonesty	9	18
Group 4: Fire-Raising, Malicious Mischief Etc.	2	4
Group 5: Other (Pro-Activity) Crimes	87	211
Group 6: Miscellaneous Offences	22	22
Group 7: Offences Relating To Motor Vehicles	3	4
Group 8: Areas Outwith The Control Strategy	40	53

Information presented in the above table:

29 Cyber Kiosk ERFs (relating to 51 devices) were completed concerning Group 1: Non Sexual Crimes Of Violence investigations.

35 Cyber Kiosk ERFs (relating to 38 devices) were completed concerning Group 2: Sexual Crimes investigations.

9 Cyber Kiosk ERFs (relating to 18 devices) were completed concerning Group 3: Crimes Of Dishonesty investigations.

2 Cyber Kiosk ERFs (relating to 4 devices) were completed concerning Group 4: Fire-Raising, Malicious Mischief Etc. investigations.

87 Cyber Kiosk ERFs (relating to 211 devices) were completed concerning Group 5: Other (Pro-Activity) Crimes investigations.

22 Cyber Kiosk ERFs (relating to 22 devices) were completed concerning Group 6: Miscellaneous Offences investigations.

3 Cyber Kiosk ERFs (relating to 4 devices) were completed concerning Group 7: Offences Relating To Motor Vehicles investigations.

40 Cyber Kiosk ERFs (relating to 53 devices) were completed concerning Group 8: Areas Outwith The Control Strategy investigations.

Table 6 - Cyber Kiosk Examinations – Crime Type – July 2023

Crime Type	ERFs Completed	Devices Completed
Murder	4	10
Attempted Murder	10	17
Culpable Homicide	-	-
Serious Assault	4	10
Robbery	6	8
Threats And Extortion	2	3
Miscellaneous	4	5
Rape	15	17
Attempted Rape	-	-
Sexual Assault	9	10
Public Indecency	1	1
Voyeurism	2	2
Brothel Keeping / Prostitution	-	-
Indecent Images Of Children (IIOC)	-	-
Extreme Pornography	-	-
Grooming Of Children	-	-
Sextortion	1	1
Communication Offences	7	7
Housebreaking / Opening Lockfast Places	2	4
Theft	3	3
Fraud	4	11
Fireraising	2	4
Vandalism	-	-
Computer Misuse Act	-	-
Culpable And Reckless Conduct	-	-
Human Trafficking	3	7
Offensive Weapons	-	-

Crime Type	ERFs Completed	Devices Completed
Drug Supply	70	173
Serious & Organised Crime	12	28
Bail / Licence / Sopo Offences	10	10
Assault	1	1
Breach Of The Peace	1	1
Threatening & Abusive Behaviour	7	7
Stalking	3	3
Hate Crime	-	-
Wildlife Offences	-	-
Fatal RTC	1	2
Road Traffic	2	2
National Security	-	-
Missing Persons	2	3
Death - Unexplained	6	8
Death - Suspected Drugs	33	43
Fatal Accident	-	-
Anti-Corruption	-	-

Information presented in the above table:

4 Cyber Kiosk ERFs (10 devices) were completed concerning Murder investigations.

10 Cyber Kiosk ERFs (17 devices) were completed concerning Attempted Murder investigations.

No Cyber Kiosk ERFs were completed concerning Culpable Homicide investigations.

4 Cyber Kiosk ERFs (10 devices) were completed concerning Serious Assault investigations.

6 Cyber Kiosk ERFs (8 devices) were completed concerning Robbery investigations.

2 Cyber Kiosk ERFs (3 devices) were completed concerning Threats and Extortion investigations.

4 Cyber Kiosk ERFs (5 devices) were completed concerning Miscellaneous investigations.

15 Cyber Kiosk ERFs (17 devices) were completed concerning Rape investigations.

No Cyber Kiosk ERFs were completed concerning Attempted Rape investigations.

9 Cyber Kiosk ERFs (10 devices) were completed concerning Sexual assault investigations.

1 Cyber Kiosk ERF (1 device) was completed concerning a Public Indecency investigation.

2 Cyber Kiosk ERFs (2 devices) were completed concerning Voyeurism investigations.

No Cyber Kiosk ERFs were completed concerning Brothel Keeping / Prostitution investigations.

No Cyber Kiosk ERFs were completed concerning Indecent Images of Children (IIOC) investigations.

No Cyber Kiosk ERFs were completed concerning Extreme Pornography investigations.

No Cyber Kiosk ERFs were completed concerning Grooming of Children investigations.

1 Cyber Kiosk ERF (1 device) was completed concerning a Sextortion investigation.

7 Cyber Kiosk ERFs (7 devices) were completed concerning Communication Offences investigations.

2 Cyber Kiosk ERFs (4 devices) were completed concerning Housebreaking / Opening Lockfast Places investigations.

3 Cyber Kiosk ERFs (3 devices) were completed concerning Theft investigations.

4 Cyber Kiosk ERFs (11 devices) were completed concerning Fraud investigations.

2 Cyber Kiosk ERFs (4 devices) were completed concerning Fire-raising investigations.

No Cyber Kiosk ERFs were completed concerning Vandalism investigations.

No Cyber Kiosk ERFs were completed concerning Computer Misuse Act investigations.

No Cyber Kiosk ERFs were completed concerning Culpable and reckless conduct investigations.

3 Cyber Kiosk ERFs (7 devices) were completed concerning Human Trafficking investigations.

No Cyber Kiosk ERFs were completed concerning Offensive Weapons investigations.

70 Cyber Kiosk ERFs (173 devices) were completed concerning Drug Supply investigations.

12 Cyber Kiosk ERFs (28 devices) were completed concerning Serious & Organised Crime investigations.

10 Cyber Kiosk ERFs (10 devices) were completed concerning Bail / Licence / SOPO Offences investigations.

1 Cyber Kiosk ERF (1 device) was completed concerning a Assault investigation.

1 Cyber Kiosk ERF (1 device) was completed concerning a Breach of the Peace investigation.

7 Cyber Kiosk ERFs (7 devices) were completed concerning Threatening & Abusive Behaviour investigations.

3 Cyber Kiosk ERFs (3 devices) were completed concerning Stalking investigations.

No Cyber Kiosk ERFs were completed concerning Hate Crime investigations.

No Cyber Kiosk ERFs were completed concerning Wildlife offences investigations.

1 Cyber Kiosk ERF (2 devices) was completed concerning a Fatal RTC investigation.

2 Cyber Kiosk ERFs (2 devices) were completed concerning Road Traffic investigations.

No Cyber Kiosk ERFs were completed concerning National Security investigations.

2 Cyber Kiosk ERFs (3 devices) were completed concerning Missing Persons investigations.

6 Cyber Kiosk ERFs (8 devices) were completed concerning Death - Unexplained investigations.

33 Cyber Kiosk ERFs (43 devices) were completed concerning Death - Suspected Drugs investigations.

No Cyber Kiosk ERFs were completed concerning Fatal Accident investigations.

No Cyber Kiosk ERFs were completed concerning Anti-Corruption investigations.

Police Scotland remain committed to ensuring that Cyber Kiosks are used legally and proportionately to support victims and witnesses of crime and to bring offenders to justice. All examination requests are subject to a robust two-stage assessment and approval process, with an initial assessment made by an officer of at least the rank of Sergeant and the second by specialist officers and staff within the Cybercrime business area. Each assessment considers the legality, necessity, proportionality and justification of the examination request, and examination cannot proceed until the request has been approved at both stages.

The integration of Cyber Kiosks into Police Scotland presented unique opportunities to engage with stakeholders in critical partner agencies including the Crown Office and Procurator Fiscals Service (COPFS), Scottish Institute for Police Research (SIPR), Privacy International, Scottish Human Rights, Information Commissioners Office (ICO) and victim and witness advocacy groups and organisations who represent some of the most vulnerable members of our communities.

The creation of the Cyber Kiosk Stakeholders Group and the Cyber Kiosk External Reference Group allowed Police Scotland to gain a comprehensive understanding of the key concerns which existed in relation to the use of Cyber Kiosks and to develop revised processes in partnership with members. The lessons learned during public engagement events enhanced a number of existing processes, including how and when informed consent for digital examination is requested and recorded from victims and witnesses of crime, and detailed information regarding this is now published on the Police Scotland website.

Police Scotland will continue to publish this information on a monthly basis.