Agenda Item(s) subject to closed minute or reason for closure of minute	**Counter Terrorism** – This item is subject of exemption under Section 35(1) (a) & (b) of the Freedom of Information (Scotland) Act 2002.

Security Classification:	**RESTRICTED**
Contents may be seen by:	
Author:	DS Jane McCourt
Organisation:	OCCTU
Telephone:	01236 818140
Date Created:	27 June 2018

Digital Triage Device (Cyber Kiosk) Stakeholder Group

MINUTE OF THE MEETING

DATE: **Wednesday 27th June 2018**

LOCATION: **Nellis Room, Scottish Crime Campus.**

CHAIR: **DCS Gerry McLean**

SECRETARIAT/ MINUTES: **DS Jane McCourt**

MEMBERS IN ATTENDANCE:

DCS Gerry McLean	Police Scotland *Chair*
DSU Nicola Burnett	(NB) Police Scotland, Head of Cybercrime
DCI Brian Stuart	(BS) Police Scotland, Cybercrime
DI Michael McCullagh	(MM) Police Scotland, Cybercrime Capability Programme
Roslyn Rooney	(RR) Police Scotland Corporate Communications
Stephen Tidy	(ST) HMICS
Iain Logan	(IL) COPFS
Neil Stewart	(NS) Unite
DS Jane McCourt	(JM) Secretariat

1. INTRODUCTION AND WELCOME

The Chair opened the meeting and thanked members for their attendance at the inaugural meeting of the Cyber Kiosk Stakeholder Group and highlighted the Group provided a forum to raise issues and identify risks to ensure they are brought to the fore and dealt with collaboratively. The Chair initiated round the room introductions.

.

2. APOLOGIES

Apologies for absence were submitted by

SPA
SPA Forensics
Scottish Police Federation
Unison

3. OVERVIEW OF DIGITAL TRIAGE DEVICES

The Chair provided the Group with an overview regarding the implementation of Digital Triage Devices.

The Chair updated the Group regarding his recent attendance at the Justice Sub- Committee on Policing and the attendance of DSU Burnett previously. The Chair emphasised that engagement with the Justice Sub-Committee highlighted there is a requirement for transparency and clarity around the use of the devices and the requirement for an indicative time line for implementation.

The Chair updated the Group with regards to the establishment of a Reference group comprised of critical friends who will advise on ethics and policy. The Chair confirmed that listening and consulting with key partners and advisors would allow Police Scotland the opportunity to become a leading force and in the forefront by developing policy and guidance with respect of Cyber Kiosks.

The Chair highlighted by having the guidance and support of the Reference Groups which has representation from such agencies as The Open Rights Group, Privacy International along with representatives from Academia, allows scrutiny not just through a policing lens. The establishment of the Stakeholder Group augments this support. Legislative and disclosure obligations can be considered in an ethical manner, by considering feedback from both Stakeholder and Reference Groups.

Cyber Kiosks are utilised by all but four forces in England for the last ten years, the approach in respect of Codes of Practice, management of information and privacy has been inconsistent but provides a starting point.

The Chair reiterated that cyber kiosks and cyber data management will be subject to mandatory GDPR compliance in accordance with force procedures.

The Chair highlighted, officers have undergone a two day training programme delivered by the manufacture Cellebrite this will allow them to cascade operational training to 410 front line officers Implementation is scheduled after consultation circa October/ November 2018.

The Chair stressed dependant on the development of Codes of Practice which will be underpinned by communication internally and to partners would lead to benefits this will create positive implications for data security and privacy. Critical voices from key partners in criminal justice and partners such as Unite and The Scottish Police Federation will allow an opportunity for Police Scotland to concentrate on key strands and practices whilst considering the impact on staff and officers.

The Chair highlighted there are clear benefits collated from anecdotal evidence which was collected during trials of the devices in 2016. A bid was made for capital monies following the trials in 2016, however, this was unsuccessful. Trials demonstrated that Cybercrime receive in the region of 15,000 phones for examination at present. Triaging capability would cut the numbers to between 1000 and 1500 devices which in turn, leads to service improvement in

regards to information being provided to the officers and the amount of devices being returned to owners
The use of triage allows Cyber staff to build capability and capacity under the transformational piece building a level of expertise in a professional visible manner.

5. TERMS OF REFERENCE

The Terms of Reference were circulated to the Group.

The Chair pointed out Point 2.6 to be amended to read Codes of Practice.

New Action 001-2018	Terms of Reference to be amended- DS McCourt

6. STANDARD OPERATING PROCEDURE

BS highlighted that Police Scotland are in better place than colleagues in England and Wales. Due to a lack of policy and procedure, there are issues with the management of data for the police. The triage facility provided by Cyber Kiosks decreases data retention and increases public confidence in a measured way.

BS updated the Group; record retention is in line with force policy regarding data
(As per Record Retention Standard Operating Procedures), records are retained for:
6+1 (1 year for review)
12+1 for serious crime

Data retention is established within force structures. It would not be a decision for Cyber or OOCTU to change force policy but to deal with records in accordance with Force Procedures.

A new case management system was established in Cyber Forensics two years ago and has the ability to archive information which is mapped by a unique reference number to Cybercrime Crime Management System, information is locked down after six years at which time it is considered for review.

Forces in England and Wales have experienced failures in system management process by having no crime management system or examination request form.

There has been a Purpose and Use document drafted in conjunction with Force Policy, however, feedback from the policy unit advised the document was not a Standard Operating Procedure but a Code of Practice.

BS updated the Group that a further two key documents have been drafted including Data Protection Impact Assessment (DPIA) and Equality and Human Rights Impact Assessment (EqHIRA) (which were circulated to the Group for their information). These documents have been submitted to the Information Management Office which could be considered innovative in respect of documents sets creation.

The Chair stressed the documents should be subject to peer review, by being open to joint contribution and treated as evolving, living documents.

BS updated the group in two years time connectivity to a new infrastructure ISO 17025 may allow accreditation to adapt.

The Chair stressed Codes of Practice should be publically available to address public concern regarding the management of their data.

The Codes of Practice should answer public concern by establishing the legal basis for seizure of a mobile phone whilst highlighting investigating officer's responsibilities in respect of revelation and disclosure.

The Cyber Kiosk will not permit exporting of information until there is a supporting evidence base for export.

The Chair asked IL for clarification in terms of disclosure and revelation regarding which information at the time of seizure is not known to have bearing on an investigation, what should be retained in case it is exculpatory and how should that be managed.

IL advises information should be linked back to legislative obligation- revelation principles are open to interpretation; In terms of what is going to be seized or retained, initial consideration should be given to what items are going to be seized. IL advised these principles should be kept general as could be used as an objection at a later stage. From a criminal perspective what would prevent prosecuting case, for example, data protection, GDPR, different legal obligations which would not prevent prosecution but may lead to grounds for civil claims.

IL advised a back to basics approach under the Criminal Justice Licensing Act; police have to reveal everything relevant, whilst not using revelation as a means to "data dump "onto COPFS

BS highlighted that forensic examination of computers allows specific search parameters whilst exculpatory evidence would not be captured by Cybercrime, devices would be retained should they be required in terms of exculpatory evidence for the defence of an accused.

The Chair stressed Police Scotland should be exploring new ways of working which would limit a "dump of data" taking cognisance of the capability and capacity for investigating officers to examine which is extremely challenging for officers.

BS emphasised that the Police Scotland should be looking at ways to return devices to members of the public, which is where triage devices would be beneficial and confirmed this would be a new way of working for an investigating officers and COPFS.

NS asked the Group at what point could a mobile phone be seized?

BS explained seizure of mobile phones would occur under Common Law in serious crime investigations, under statute and under warrant.

The Chair stated where a device was triaged and found to be of evidential value, devices would be submitted to Cybercrime in accordance with current practice. The device would be retained for COPFS/defence in the event new evidence comes to light. Devices which had been triaged and found to have no evidential value would be returned to owners.

BS reiterated that once the device had been triaged, the information from the device would be deleted from the system

NS asked would this be the same for victim's phones

Chair confirmed that would be the case but that the police could improve means of providing information which would be addressed by the development of Codes of Practice

ST enquired if College of Policing were exploring Codes of Practice.

BS confirmed a National Validation package for digital forensics sits within different arenas

with no common practice across forces in England and Wales and further stated at this time Police Scotland has no statutory obligations, but it is the correct course of action to have accreditation

The Chair explained to the Group that Cybercrime had explored policy and operational use throughout the UK and Police Scotland have the opportunity be in a leading position by implementing a Codes of Practice.

ST asked the Chair if ICO invited to be part of the Stakeholder Group

Chair confirmed Scottish Government and ICO were invited but both parties declined as they wished to retain independence

BS updated the Group that David Freeland from ICO engaged with the Information Manager and looked at policy with a view to shaping forward thinking. In terms of what does data retention should look like?

NB stressed that the issue of informed consent has to be clear, as potentially examination of a mobile phone could potentially uncover another crime, for example an indecent image of a child.

The Group discussed a form of words for investigators. The Chair reiterated personal devices are diaries documenting people's lives and contain sensitive matters; as a result people are concerned about image sharing/ internet connection.

BS highlighted collateral intrusion is also a concern in regards of third party information on mobile phones.

IL confirmed to the group that if a phone is seized in furtherance of an investigation but additional criminality is uncovered during the examination of the device could lead to an objection from a defence, if it is found that seizure and examination is unfair. The test will be for Case Law to provide the test of fairness.

IL confirmed there would be a reluctance from COPFS to issue a form of words as this would be determined on an individual case basis.

Case Law provides general principles; it should be made clear to individuals in certain cases they do not have to comply, if not made clear the evidence may be found to be unfair. It should also be recorded clearly that they voluntarily provided the phone

IL is seeking views from others in COPFS in relation to a situation where a person gives their phone voluntarily. They must truly understand what is involved. A police officer cannot ignore evidence of a crime but cognisance should be taken that it may be challenged by the defence at a later stage of proceedings. Police Scotland must adhere to principles and have clear expectations of when people can refuse to provide their mobile phone.

BS advised if phones are sitting inactive for a period of time they may not work causing the best evidence to be the information on the system as opposed to capturing at source.

The Chair queried risk, obligation and cost of storage of retaining data

BS advised the cost of storage is minimal, more importantly there needs to be a reason for keeping data, there are technologies which exist to manage how information is retained or deleted, for example, the NUIX toolset which is GDPR compliant.

NS enquired whether, there a risk to staff and would there be a potential for staff to be prosecuted under data protection offences for holding data not for a policing purpose and are they at risk of committing an offence.

Chair highlighted that systems are GDPR compliant, with end to end processes which ensure data protection compliance. The offence would be committed if staff shared or used information held not for a policing purpose

ST enquired if there is an audit process in place

BS confirmed the kiosk would retain minimal information. On a quarterly basis trained accredited staff would download an audit function which is aggregated into the crime management system held by the Cybercrime. The information but would be made available to Professional Standards and Information Management if required.

The Chair confirmed when not in use the kiosk would be switched off and unplugged, no internet facility would be enabled, the function to export would be switched off.

BS confirmed the 410 officers trained would only carry out the initial examination and first line management would be required for authorisation on the completion of a request form. Documented process would confirm who authorised the triage. If the device is to be submitted to Cyber Support Services following triage, this would be in line with standard practice; the phone would be packaged, sealed and documented before being analysed fully, results would be given to investigating officer for court purposes. Consequently triage would result in 10 % of devices submitted being subject to production procedures.

7 Codes of Practice

ST would encourage Codes of Practice with a view for building in review from HMICS

RR advised the group, Frequently Asked Questions which are categorised into privacy, data retention. Particular groups could go to FAQs and information they would require. RR advised this would be a progressive living document.

The Chair highlighted FAQs could be tabled to the Cyber Reference Group. Key considerations could be in line with the work which was done in relation to Schedule 7 Terrorism Act 2000 by adopting good practice such as an information leaflet and QR codes
; Leaflet, QR codes, policy

New Action 002-2018	An information leaflet pertaining to Schedule 7 to be shared with the Group- DS McCourt

8. Review of Actions

Actions

New Action 001-2018	Terms of Reference to be amended- DS McCourt

New Action 002-2018	An Information leaflet pertaining to Schedule 7 to be shared with the Group- DS McCourt

New Action 003-2018	DS McCourt to invite representation from Victim Support to Cyber Reference Group

9. AOCB

NB advised asking Victim Support to the Cyber Reference Group

New Action 003-2018	DS McCourt to invite representation from Victim Support to Cyber Reference Group

10. CLOSE

The Chair thanked Members for their attendance and contribution to the meeting.

11. Date of Next Meeting

27th July 2018- Scottish Crime Campus