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

Digital Triage Device (Cyber Kiosk) Reference Group

MINUTE OF THE MEETING

DATE: **Thursday 26th July 2018**

LOCATION: **Conference Room 2, Scottish Police College, Tulliallan**

CHAIR: **Richard Whetton (Head of Partnership and Collaboration, Police Scotland)**

SECRETARIAT/ MINUTES: **DS Jane McCourt**

MEMBERS IN ATTENDANCE:

Richard Whetton	Chair
DCS Gerry McLean	(GM) Police Scotland, Head of Organised Crime and Counter Terrorism Unit
DSU Nicola Burnett	(NB) Police Scotland, Head of Cybercrime
DCI Brian Stuart	(BS) Police Scotland, Cybercrime
CI Iain Moffat	(IM) Police Scotland, Strategy and Innovation
Michael Dickson	(MD) Police Scotland, Cybercrime Forensics Co-ordinator
Millie Wood	(MW) Privacy International (VTC)
Aamer Anwar	(AA) Aamer Anwar and Co
Dr Duncan Campbell	(DC) Advisor to Open Rights Group
Dr Megan O'Neill	(MO) Dundee University
Dr Liz Aston	(LA) Napier University
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 Reference Group. The Chair highlighted the Group provides the opportunity to work collaboratively, reflecting the values of Police Scotland of Integrity,

Fairness and Respect, allowing these values to be reflected in a number of workstreams whilst understanding scrutiny and increased transparency. The Group reflects the wider piece of work being undertaken by Police Scotland in terms of broader ethical advisory panels.

The Chair initiated round the room introductions.

2. VALUES STATEMENT

Integrity, Fairness and Respect are the values of Police Scotland. All decisions which we make must reflective our values and be able to withstand scrutiny when judged against them. Accordingly, our values will be the touchstones in all decisions we reach within this forum.

3. APOLOGIES

Apologies for absence were submitted by

- Victim Support
- Scottish Human Rights Commission

4. OVERVIEW OF DIGITAL TRIAGE DEVICES

GM provided the Group with an overview regarding the procurement of Digital Triage Devices, highlighting that the utilisation of Cyberkiosks provide an opportunity for service improvement within tight financial frameworks. He cited there is an opportunity to do things better, be more connected with detailed business plans.

GM informed the Group that there are currently five Cyber Hubs with connectivity and support provided to Local Policing partners. At present for an investigating officer it can be weeks before devices are examined which causes implications for investigations. In terms of the public, with thousands of devices being seized it is a slow turnaround which is compounded by the personal data contained within the devices.

GM highlighted Cyberkiosk technology is not new, being in existence for approximately ten years. All but four of the forces in England and Wales are currently using the technology.

GM 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 there are approximately 15,000 phones submitted for examination to Cyber Hubs at present. Triaging capability would cut the numbers to between 1000 and 1500 devices this in turn, leads to service improvement in regards to information being provided to the officers and the amount of devices being returned to owners. Information provided as a result of triage would allow investigating officers to confront suspects and provide an early determination for investigations

GM emphasised that Police Scotland has recognised public interest in relation to the control of the device, responsibility for data retention, privacy and the deletion of data.

GM informed the Group that 41 devices have been purchased after engagement with Local Policing Areas. Officers have undergone a two day training programme delivered by the manufacture Cellebrite which will allow them to cascade operational training to 410 front line officers.

GM stated that a commitment was given to the Justice Sub-Committee for Policing for the establishment of two groups; Stakeholder Group comprising of members from SPA, Inspectorate, COPFS, and staff associations looking at implementation within a legal framework. The second group being the Reference Group which would provide an opportunity

for wider consultation and engagement through an open and transparent lens. GM reiterated that Police Scotland would welcome contributions from position of listening.

GM highlighted that the establishment of the Reference Group would bring wider benefits to the arena of covert policing and the wider issues of data management and whilst it is important to protect tradecraft it is useful to examine ethical considerations.

MW asked are the devices still going to be Cellebrite as highlighted in a recent article in the Guardian regarding software and machine learning on top of extracted data.

GM confirmed the manufacturer of the devices is Cellebrite, and in the wider cyber capability Police Scotland are looking at the best use of technology; Cyber Kiosks would not be used for extracting data at this time.

MW asked for clarification regarding what the legal basis for seizure would be and if this would be under PACE

GM highlighted Police Scotland do not operate under PACE but instead seizure would be under the legal basis of Common Law, Statute such as Misuse of Drugs Act 1971 or Sherriff Search Warrant

MW asked if information would be logged for legal basis and how will statistical information be gathered in relation to victims/suspects

GM provided that statistical information would be useful, however, in terms of differentiating between witnesses and suspects, the police may also have Common law powers in relation to devices belonging to witnesses. The issue of what happens if a witness changes their mind and wants their device back; in the absence of an agreed position this is being considered by the Stakeholder Group. In terms of a form of words, COPFS position is that this is an operational matter for the police. Consideration is being given by the Stakeholder Group in relation to informed consent, obligation to public, powers to seize and powers to examine.

MW updated the Group that Privacy International and the Law Commission are consulting on search powers with regards to electronic devices, The Home Office have been slow to respond, MW highlighted there is a need for wider discussion police/law and wider society of what should be the correct lawful basis.

GM confirmed that in the operating environment in Scotland the position of COPFS would be if device is lawfully seized there are police powers to examine. Management information would be collated which is GDPR and data protection compliant by means of a case management system. This is an internal process which has been implemented which and is an on-line form submitted by the investigating officer. The form reflects pertinent information in relation to the electronic device. Before using a Cyber Kiosk, an examination form will be required to be completed. The cyber kiosk is the first stage of the examination process.

LA queried how cyber kiosk statistics, would be collected. LA cited stop search data was requested on how powers were being used. Independent oversight couldn't respond because of the way information was collected this led to each record being manually examined. This was previously ad hoc, there is now an ability to have data management analysed. The Group should consider what kind of data is being asked for in terms of what the information would be used for.

MO stated it would be useful to have statistics at point of departure and queried what happens to the device being used. How do kiosks link into stop search legislation? If device belonged to a witness, could it be considered a consensual search of someone's phone? Informed consent, what is the power for examination, do people know when they hand phone over they are consenting to examination of data on the phone.

GM stated the purpose of the Group is to discuss and consider these types of scenarios and how they may be reflected in the Standard Operating Procedures in relation to data protection and digital forensics

MO enquired if the Group could be provided with relevant SOPs

GM reiterated the Group are critical friends. The Operating Procedures in relation Cyber Kiosks are being re-drafted; presently it is a purpose and use guidance document for frontline officers. Codes of Practice are being explored but these would have to be endorsed by Scottish Government or Home office. The re-drafted document would be akin to Codes of Practice, the current operating principles do not reflect modern investigatory techniques and public interest. Operating principles will be transparent.

LA cited there are similarities to the Stop/Search journey and advised engagement with Supt Ian Thomson or Lynn Ross in relation to lessons learned.

New Action 001/18	DSU Burnett to engage with Stop/Search team regarding lessons learned	DSU Burnett

AA queried if Police Scotland are going to adopt a SOP and not Codes of Practice, how you hold police responsible, why not have Codes of Practice?

GM there will be engagement with the Stop/Search journey in respect of data/data retention and Codes of Practice, with recognition this is endorsed by a statutory instrument in the Criminal Justice Act 2016.

LA queried the figures of 10% of devices being submitted for examination are the figures based on the experience in England and Wales, locally is it the same process and how long does it take?

GM confirmed the figures come from anecdotal information from other forces and the trials which took place in Edinburgh and Stirling in 2016/17. 15,000 devices are submitted to the 5 hubs. Officers seize devices and submit using the electronic process in broad terms a report will be provided to the officer in 8-12 weeks.

LA enquired would the local process be the same as the Hub.

MD updated that for serious crime, phones submitted to the Hub can be examined within an hour, providing information pertinent to investigation which may either incriminate or exculpate.

GM confirmed that the kiosk does not extract data, the decision was taken not to export, but would quickly allow opportunity for officers to return or submit device for examination.

LA enquired whether there is a potential to lose information or find something that doesn't exist

GM confirmed there could be instances where other information unconnected to the investigation is recovered but this already happens in other areas of cyber and police investigations.

AA expressed that as a defence agent, the biggest concern for clients is when will their device be returned to them; an ability to address the backlog can be perceived as positive.

AA queried the training involved, the audit trail and data extraction, is there a guarantee that the information doesn't change is there a chance a case could collapse if you break the audit trail.

GM assured that in relation to serious crime, the device would be submitted straight to Cybercrime and further confirmed; officers who have undertaken the two day training course are also trained. They will train the 410 front line officers, who will examine the device using the test of relevancy, if there is material evidence the device will be submitted to Cybercrime as per normal procedures. By adhering to operating principles you will leave a trace but wouldn't materially change the device.

BS added 410 staff will be trained by accredited staff, who have already undertaken train the trainer by manufacturer Cellebrite as well as mandatory GDPR training.

AA queried if there is an audit trail if an officer is accused of untoward conduct.

MD confirmed the kiosk will only be accessed by the 410 staff; there is an admin and managerial function which will only be available to cybercrime staff. Dip samples will be carried out. The phone being triaged is a production and is cross referable to the case management system

BS confirmed relevant information will be available to Professional Standards, Information Management in relation to complaints against the police and external Information Commissioner if required

AA queried how officers are protected from allegations of data protection breaches

GM confirmed the check and balance would be, the investigating officer will not be carrying out the triage. The Investigating officer will start electronic process authorised by line management, dependant on the type of investigation, the officer will have to go to accredited/trained officer to triage. At the moment search parameters are not recorded on the kiosk, but are on the request form which would protect officers as the form would show the search parameters.

MD has confirmed there are on-going enquiries with the manufacturer to explore whether search parameters could be recorded on the kiosk.

DC highlighted that search terms are a key point and the heart of issues in relation to liberty and rights which is balanced with operational considerations. Officers must put in what has been searched for, bearing on proportionality, record what was handed over.

GM confirmed these points would be reflected in the case management form, if serious crime the device would be submitted to one of the five cyber hubs using an electronic request form in which parameters would be recorded. When Kiosk used it would also reflected in transaction code, providing an audit trail which would protect both officers and the integrity of the investigation.

DC highlighted a comparison with other forces where press reports indicate all data is collected.

GM cited other experiences in the UK. The devices have the ability to export but reiterated until there is an evidence base, Police Scotland would not be doing so. There are concerns about how data would be stored, data security and privacy. The 41 devices will be standalone, the kiosks could be networked to facilitate software upgrades but to network the devices, could lead to the perception of mass collection of data.

MO asked what would happen if witness from crime A became accused for crime B

GM stated there would be an obligation on officers to seek advice from COPFS on how to progress and dependant on the circumstances, the officer may have to apply for a warrant.

NB asked what is informed consent. For example in the circumstances of a victim of sexual crime, there needs to be a rider to the public providing a device in those circumstances, this would be incumbent on the police

BS stated the view from COPFS would be that the issue of lawful seizure would be tested in a court of law.

MO advised that informed consent, needs to be really clear in terms of data extracted and self-incrimination will be actioned, confirming there is there is an opportunity to establish robust informed consent.

NB advised that the issue of self-incrimination occurs just now, it would be wider set of officers before submission to digital forensics

AA advised that the issue cannot be left to court to decide there must be informed consent guidelines. Triage cannot be a fishing expedition. There would be public concern if there were no guidelines established.

LA asked if there is an option for victims or witnesses to set search parameters. How does this link in with other processes, for example a witness or victim could agree to give a particular photo.

DC advised in the cyber area, in terms of quality data there is a massive boundary between warrant and general research which could lead to a wide range of data, enabling general search of other crimes. There would have to be a 2 step process either a highly limited triage cyber or put to one side everything of someone's life

GM confirmed in terms of phones, having clear search parameters would minimise collateral intrusion. There is an opportunity to build assurance captured through transaction and electronic request form. There is a real opportunity regardless of status and in the absence of guidance, to do something similar for what we do for Schedule 7 Terrorism Act 2000, where a guidance leaflet was developed and includes information such as the role of PIRC and what is the legislative basis, providing the public with more information and guidance than what is available currently.

5. CYBER KIOSK DEMONSTRATION

MD provided a demonstration to the Group

6. GROUP DISCUSSION

6.1 TERMS OF REFERENCE

Chair – open to considering Chair of Group moving forward and suggests review of Terms of Reference

LA advised that will "meet no less than twice during the course of implementation" may not demonstrate on-going intent.

MO queried if the Reference Group will report into the SPA board and the Code of Ethics/Practice should look to broaden development of governance documents.

IM confirmed Police Scotland already have a Code of Ethics specific to governance, operations, rules and procedures.

New Action 001/18	Review of Terms of Reference	Members

6.2 OPERATING PRINCIPLES

AA advised Codes of Practice has to be in line with data protection for officers and members of the public, there has been a lot of sensationalism, hence, there must be a framework, aligned with a Code of Ethics which can hold Police Scotland to account if not adhered to. PSOS response to the media interest was poor which was picked up by various groups and politicians, there was not concerted approach to deal with this. There is now an opportunity to correct public perception.

LA suggests it is worth considering management data to be able to demonstrate what has been collected

GM confirms it would be best practice to have Codes of Practice but may not be in our gift but could be considered.

6.2 DATA PROTECTION IMPACT ASSESSMENT (DPIA)
6.3 EQUALITY AND HUMAN RIGHTS IMPACT ASSESSMENT (EqHIRA)

GM highlighted that data has to be GDPR compliant

DC highlighted at present DPAI and EqHIRA is a form filling exercise at this stage and advised create Codes of Practice and Operating Instructions and whilst they are adequate for time they will change, both documents should be living documents subject to annual review

7. REVIEW OF ACTION LOG

New Action 001/18	DSU Burnett to engage with Stop/Search team regarding lessons learned	DSU Burnett
New Action 002/18	Review of Terms of Reference	Members

8. AOCB

AA highlighted the demonstration was very helpful to confirm what a kiosk is. Going forward there is a lot to be done, however, it is a good start to have the Stakeholder and Reference Groups.

LA queried the relationship and governance between both groups, should SPA sit on both Groups, is there a potential to have someone with lived experiences on the Reference Group

GM confirmed group composition is open to consideration, Victim Support have been invited to participate in the Reference Group.

MO advised the Reference Group should remain independent and work with the Stakeholder Group. Any merge would be cumbersome, highlighted by important lessons learned from Stop and Search.

AA advised from his experience with CCU, groups have different interests and tend to be

dominated by Police Scotland. It is valuable having separate Groups.

GM asked the Group would there be value having SPA at the Reference Group?
Should there be someone from Reference Group at the Stakeholder Group?
What is the role of PSOS?

AA advised having someone from SPA at both Groups would be useful feeding backwards and forwards
DC asked have Cyberkiosks been deployed ?
GM confirmed procurement was published which led to increased media coverage. The establishment of both Stakeholder and Reference Groups is an assurance the Justice Committee. Roll out of the Kiosks will be after engagement and consultation with fluid timescales towards the end of the year

MO advises that from learning gained from Stop/Search until Codes of Practice are established; do not commence the training of front-line officers as this will have to re-done.

The Chair summarised that the next steps are revision of TOR and Draft Codes of Practice to be commented on by circulation.

8. CLOSE

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

9. DATE OF NEXT MEETING

1400 5th September, Scottish Crime Campus