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) Stakeholder Group

MINUTE OF THE MEETING

DATE:	**10.00 hrs Friday 27th July 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
Insp Heather Macdonald	(HM) Scottish Police Federation
Tom Nelson	(TN) Director of Forensic Services SPA
Robert Hayes	(RH) SPA
Iain Logan	(IL) COPFS
DS Jane McCourt	(JM) Secretariat

1. INTRODUCTION AND WELCOME

The Chair opened the meeting and thanked members for their attendance.

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

HMIC(S)
Unison
Unite
PSOS- Corporate Communications

4. EXTERNAL REFERENCE GROUP

The Chair provided the Group with an update regarding the inaugural meeting of the Cyber Reference Group which took place yesterday (26th July 2018) at the Scottish Police College, Tulliallan .The Chair highlighted the purpose of the Cyber Kiosk Reference Group is as much about the operational deployment of cyber kiosks, but focused more on issues of privacy and human rights.

The Chair highlighted the Stakeholder Group provides examination in relation to the use of kiosks within a statutory and policy framework.

The Chair highlighted that the Reference Group wish to remain independent of the Stakeholder Group The Chair summarised the feedback from the Reference Group regarding the need for a Codes of Practice, providing the caveat that Codes of Practice require endorsement from Scottish Government or Home Office, citing example of Stop and Search and Counter Terrorism legislation respectively.

The Chair highlighted that the Reference Group advised that Codes of Practice should be implemented from the wider perspective of how to hold Police Scotland accountable, but advised there was a note of caution expressed by HMIC(S) that there may be no legislative framework to establish Codes of Practice but that operational guidelines should reflect the threshold of Codes of Practice.

RH highlighted that the Scottish Police Authority recognises that there is intensive interest in regards of new investigative techniques for example facial recognition, which may become disclosable in a court of law or become known through the procurement process. RH stressed that the adoption of new techniques should be lawful, proportionate and justified. SPA endorsement would not stop attention, highlighting there is an opportunity to have a process in place.

BS asked if it would be advisable to invite Information Management to the Stakeholder Group.

New Action 004-2018	Information Management to be invited to next meeting- DS McCourt

TN asked the Chair if there are existing Codes of Practice in relation to cyber kiosks.

The Chair highlighted there are existing Standard Operating Procedures in respect of Digital Forensics and Record Retention which may not take cognisance of new technologies, these are paper based guidance documents, available to all officers on the force intranet.

TN highlighted that there may be an opportunity from a quality management perspective to devise Codes of Practice with Standard Operating Procedures, forming the basis which would provide validation of the process.

BS highlighted to the Group that presently there is a draft Purpose and Use document and frequently asked questions and answers are being developed.

TN stated there would be a need to examine what the purpose of Codes of practice would be

RH specified that high level Codes of Practice would require being part of a legislative framework and would be need to be a public facing document.

The Chair confirmed that presently there is an absence of public information regarding the retention and deletion of data. There is an inconsistent approach across the 39 forces that are utilising cyber kiosks. To address this Police Scotland have introduced an electronic case management system; this requires an electronic submission, which could be used to collate management information. The system is will be part of a suite of GDPR compliant systems used by Police Scotland. The wider Cyber Capability programme are recruiting a Quality Manager.

TN confirms the need for quality assurance, SPA Forensics went through a similar journey with fingerprints and the quality system utilised by SPA (Q pulse) provides electronic accountable audit records.

RH confirmed adopting the levels of SPA Quality for all forensics would provide a standard approach.

BS updated the Group that Cybercrime have liaised and met with SPA Forensics from the perspective of accreditation in a quality environment.

The Chair highlighted Richard Whetton, Head of Partnership and Collaboration chaired the Reference Group, he was asked due to his experience and involvement in Force Ethics Panels. The HMIC(S) review of undercover policing recommended a values statement in relation to covert policing. ACC Johnson is driving an ethical approached visibility to authority. Due to external scrutiny on authorities and public interest, the Organisation wants to provide public assurance that activity is authorised within an ethical and moral framework.

NB reiterated there is an increased requirement for engagement with the public and partners to speak about emerging technology

The Chair highlighted that the Reference Group framework relationship between the stakeholder and references Group in Terms of Reference of both groups. He highlighted the Reference Group are keen to work with the Scottish Police Authority.

RH advised by representing SPA in Stakeholder Group could provide a link in to the Reference Group. Issues or aspects which the Reference Group identify could be fed into SPA where appropriate.

The Chair queried if the Reference Group could be public facing or have any relationship with SPA public meetings.
RH queried if there is a mechanism for the Reference Group to communicate with the Stakeholder Group
NB advised the Terms of Reference for both groups should be revised with the aspiration being a more permanent structure

RH highlighted whereby the present position is an advisory capacity in relation cyber kiosks, if there are other areas which require this engagement and could become a rolling meeting.

The Chair confirmed the meeting structure could form a basis for cyber and digital progress

BS highlighted the Groups could form a wider Police Scotland mechanism for debate in relation to justice to be ahead of the crime narrative

TN highlighted the evolvement of DNA technology has benefitted from ethical considerations.

NB commented that lessons should be learned from the Stop/Search journey in relation to how we go forward, the need to document why we are doing what we are doing, the outcomes, and communication to the public. Communication with consultation and engagement should provide public assurance and protection of officers and police staff. Considerations from the Reference Group include allegations of misuse by officers, Codes of Practice, experiences from England and Wales and what challenges have been experienced.
Privacy international queried other technologies being considered, which may provide considerations for the wider Cybercrime Capability Programme, and what challenges may be faced in the future. The Reference Group recognised the need to consider new technologies but importantly it is imperative to focus on training and responsibilities in relation to the utilisation of equipment. The Reference Group highlighted the need for Management information highlighting the legal basis for seizure, whether statutory, warrant or common law and whether the device was provided or seized from a witness, suspect or accused. What management information does the kiosk hold and what information is expected for it to hold?

5. GROUP DISCUSSION AND REVIEW OF DOCUMENT SET

5.1 STANDARD OPERATING PROCEDURES /CODES OF PRACTICE
5.2 DATA PROTECTION IMPACT ASSESSMENT (DPIA)
5.3 EQUALITY AND HUMAN RIGHTS IMPACT ASSESSMENT (EqHRIA)

The Chair reiterated the need for communication with the public addressing the concerns regarding personal data should be addressed by publishing data seta and developing a communication strategy.

RH commented that HMIC(s) are a useful member of the Stakeholder Group from the perspective of review and inspection

BS underlined a proposed 6 month deployment review highlighting the business benefit for the public by using the case management system to provide management information.

Chair commented that data sets contained in the electronic submission to the crime management system should be more transparent

TN highlighted that statistical information regarding DNA is published on a monthly basis.

NB remarked that the Reference Group had queried whether the consensual examination of a mobile phone for example given by the victim of a sexual crime could be construed as a consensual stop search.

IL responded that there is no specific test for informed consent. Case law highlights that where an examination may be criticised when it is abundantly clear that a witness can refuse and they are not aware of everything that might happen to them as investigation takes place.
COPFS view is that this would only become an issue something else found which leads to a separate prosecution. There would be no basis for objection if the phone was taken lawfully and fairly. It may be construed unfair if they did not understand other information could come to light as the result of examination because officers did not explain the process properly.

The Chair highlighted there are four points to consider,

- Informed consent, do we have a legal basis in Common Law power to seize a device in furtherance of an investigation? What are the lessons learned from Stop Search.

- Data Sets and Management Information

- Guidance and Codes of Practice, Standard Operating Procedures or operating principles to ensure adherence to Codes of Practice providing accountability.

- Data protection, supervisory checks and protection for staff and officers, in terms of what happens if there is an allegation, could the kiosk demonstrate search parameters at the point of electronic submission. Cellebrite are being asked if search parameters could be factored into the kiosk minus personal data

IL reiterated there is a requirement to make clear to the public, what common law powers allow you to do

NB highlighted Cybercrime Capability Programme funds a Data Quality Assurance Manager which will allow major housekeeping, the job description is being drafted and processes are being mapped. Recruitment will ensure quality assurance across Cybercrime capability.

TN advised liaison with SPA Forensics Quality Assurance Manager could advise in relation to the audit function as SPA undertakes 1980-2000 audits per annum.

The Chair advises a link in with SPA Quality Manager would assist the process.

RH advised clear guidelines within the Terms of Reference for the Groups in relation to issues which will not be discussed within the Group, in respect of sensitive techniques.

The Chair confirmed protection of sensitive equities has to be a consideration.

NB highlighted there should be meaningful discussion in relation to draft EqHIRA and DPIA

TN advises effective audit documents are adopted, incorporating a testing mechanism with dip tests, which will protect officers/staff

BS confirmed that part of information management, similar to PNC enquiries, will record use on such date and reason for examination. He further highlighted the kiosks are standalone and not networked, there will be manual updates across the 41 locations and transaction information will upload to the information management system.

Chair stated that communication will be devised in terms of an information leaflet for the public, similar to the leaflet provided for Schedule 7 examinations under Terrorism Act, which will include QR codes, providing the public with information such as the role of PIRC and the legislative basis for seizure, how long examinations can take. This will be enhanced with publically available Frequently Asked Questions.

The Chair requests an action for the Reference Group to consider what issues the public would wish addressed in the information leaflet and Frequently Asked Questions

BS suggested signposting on the Police Scotland Website where there could be electronic copies of the information leaflet and a landing page for Frequently Asked Questions.

5. REVIEW OF ACTION LOG

New Action 004-2018	Information Management to be invited to next meeting- DS McCourt

The Chair requested the Group consider two issues

What should be contained in a Codes of Practice?
What should be incorporated in the Communication strategy?

New Action 005-2018	Consideration to be given to content of Codes of Practice and Communication Strategy- Members
New Action 006-2018	Document set to be shared with National Independent Strategic Advisory Group (NISAG) – DSU Burnett

6. AOCB

The Chair advised Cybercrime staff are prepared for a roll out of programmes before end of the financial year once the document set is agreed with the appropriate engagement and consultation.

RH advised the group, a high level Codes of Practice has to be developed, and training should be commenced at one location to provide proof of concept. There could be criticism if the kiosks go live too quickly, however, there will also be criticism if the process is too slow

BS remarked that once the document set is fit for purpose it will be a living document and reviewed regularly.

NB suggested at the next meetings of the Stakeholder and Reference Group an aspirational timeline could be discussed

TN advised a timeline should be established soon to ensure equipment is tested and training is continued

NB confirmed that training for front line officers has not been commenced.

TN commented that he is happy and keen to be part of conversation going in right direction and advised the cultural change may be challenging.

IL advised the Group that Codes of Practice in isolation without a legislative framework would mean a court would assume that they were to be used in the same way as statutory Codes of Practice, because there is no associated statute how will it be accountable?
If the Codes of Practice were published in the public domain, the role of a Defence Agent would be to put in front of officers and ask did you adhere to this, this would not be an issue if treated the same as Codes of Practice.

The Chair confirmed it would be an aim for the guidance to have the same threshold as statutory Codes of Practice.

RH advised the using the terminology Codes of Practice would be confusing as these would be statutory, if not statutory they guidance should be called something else

TN advised not taking down same route as Stop/Search as these are statutory Codes of Practice.

RH highlighted the issue is with the data held, the cyber kiosk is more of a process, but the concern is what happens to data

The Chair suggested guidance should be formed under something under GDPR rather than statutory considerations.

HM highlighted that Personal Digital Assistants (PDA) guidance document has already been developed and could be used as a reference for development of guidance given the other equipment utilised by front line officers.

NB suggested document set could be shared with the National Independent Strategic Advisory Group (NISAG) for further consultation and engagement.

10. CLOSE

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

11. Date of Next Meeting

10 am 12th September 2018- Scottish Crime Campus