Security Classification:	OFFICIAL
Contents may be seen by:	
Author:	DS Jane McCourt
Organisation:	OCCTU
Telephone:	01236 818140
Date Created:	31st October 2018

Digital Triage Device (Cyber Kiosk) Stakeholder Group

MINUTE OF THE MEETING

DATE: 1330 Hours Tuesday 30th October 2018

LOCATION: Nellis/Collins 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
Inspector Steven Tidy	(ST) HMICS
Inspector Heather Macdonald	(HM) Scottish Police Federation
Craig Donnachie	(CD) Forensic Services SPA
Robert Hayes	(RH) SPA
Andrew Richardson	(AR) COPFS
Peter Benson	(PB) Team Leader PSOS Cybercrime
Alice Stewart	(AS) Information Management
DS Jane McCourt	(JM) Secretariat

1. INTRODUCTION AND WELCOME

Chair opened the meeting and thanked members for their attendance to this meeting of the Cyber Kiosk Stakeholders Group.

2. VALUES STATEMENT

Chair *stated the values of police Scotland to members namely; 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 were submitted prior to the meeting by

Roslyn Rooney Police Scotland Corporate Communications

4. MINUTES

Chair proposed the minutes of the last meeting of the Cyber Kiosk Stakeholders group for consideration and any amendment. There were no amendments raised

Chair highlighted that in order to be transparent and open in our approach to the roll out of cyber kiosks and the consultation process that has been undertaken the minutes of the previous meeting of the External Reference and Stakeholder Groups have been published on the Police Scotland public facing internet site and the minutes of this meeting, including previous, shall be uploaded to the page unless there are any objections to their publication.

No objections were raised to the publication of the minutes of this group.

5. GROUP DISCUSSION

The Chair invited NB to provide an overview of the document sets, the work undertaken to date and observations raised by the External Reference Group at the meeting on 30th October 2018.

NB provided the Group with an overview regarding the proposed time-line, on 4th October a written submission was presented to the Justice Sub Committee on Policing which outlined the document set, being Toolkit, Public Information Leaflet, Principles of Use, EqHRIA (Equality and Human Rights Impact Assessments and DPIA (Data Protection Impact Assessment.) and confirmed these had been shared with the Group for consultation.

NB confirmed the letter contained information for the Committee with respect to Audit and Assurance, with an intimation to publish an agreed data set compliant with governance procedures. Taking on board advice from the Reference Group, management information would include

- Number of examinations undertaken during quarter broken down by location (North/East and West) and accused/victim/witness status
- Quarterly summary of audit regime and issues identified for action (by location; East, West & North)
- Quarterly summary of remedial action taken as consequence of audit regime, detailed in categories for example; equipment issues, data input or training,

NB confirmed an agreement has been established for PSOS Audit and Assurance Team to conduct compliance assessments including dip sampling and will monitor and review first line audit procedures implemented by Cybercrime ensuring compliance of use with toolkit and training.

NB highlighted engagement with Assurance and Governance confirming that there is a requirement for a robust audit process underpinned by the Principles of Use document. Cybercrime would ensure there was an effective audit procedure with regards to dip sampling and management information being collated with respect to kiosk users and non-use of kiosks.

Assurance and Governance would provide a second tier of assurance using collation of management information produced by Cybercrime.

If there were specific concerns raised a review could requested from HMICS.

The letter outlined the ambitions for accreditation not just for Cyber Kiosks but for the wider digital forensics piece. Police Scotland has produced a draft digital forensics strategy and whilst Police Scotland are not compelled by the Forensic Regulator for England and Wales to sign up to ISO17025 Accreditation, opinion was sought from Dr Gillian Tully, Forensic Science Regulator in order to understand potential benefits and challenges.

Police Scotland is seeking to employ a Data and Quality Assurance Manager to review the ISO17025 route or if an alternative route should be explored. The ambition is to be the best to support staff and the Organisation.

There will be ten officers trained per kiosk; there will be a rolling assessment in terms of capacity in each area. The training is due to be rolled out in November which will be assessed and evaluated before a proposed national roll out of training, which at the moment is scheduled for January to April 2019.

NB confirmed to the Group, with regards to the legal framework, ACC Johnson has written to Andrew Laing at COPFS, seeking clarification.

CD highlighted that ISO17025 does not fit most disciplines as a testing standard and there are difficulties with respect to wet forensics. CD advised the standard could be made compliant for digital forensics and advised it would be difficult to find more suitable accreditation.

NB confirmed that the External Reference Group understood the aspirations and were supportive of seeking accreditation.

GM advised that the standards sought by England and Wales are under the direction of NPCC and it would be difficult for Police Scotland not to seek the same level of standards.

CD has highlighted that third party review and accreditation provided value to the SPA, three sites have undergone UKAS assessment with Edinburgh still to be undertaken. The intense scrutiny highlighted that current processes are established and sufficient, which would not have been provided by internal audit.

CD further advised that finding managers conversant in ISO17025 rather than other regulatory frameworks may be difficult. Appendices have been built in to ensure future forensic compliance to Codes of Practice to address identified gaps.

Codes of Practice in England and Wales align to an agreed regulatory framework through UKAS. Whilst Police Scotland cannot be compelled it could be questioned why Police Scotland would not want to achieve the same standards. Codes of Practice require more work clarifying clauses in standards for Digital, DNA and Crime Scene Management best practice. SPA seeks to move forward with another level of assessment, leading to confidence and consistency in a court framework.

BS highlighted that I terms of Cyber Kiosks ISO17020 is removed from a lab environment and consequently ISO17025 has been identified as being more suitable.

GM highlighted there are wider considerations in relation to the legal basis for digital examination which is not constrained to kiosks but the wider digital forensics piece.

AR confirmed there are on-going discussions with respect to the issues raised by ACC Johnson's letter. The issues are not specific to Cyber Kiosks but that Kiosks have brought the issues into sharper focus. AR advised there is little case law in existence, one of which being HM Advocates V Rollo 1997 which is historic.

AR queried whether COPFS can address the issues raised or whether they were for the Force Solicitors seeking Crown Counsel Opinion may not guarantee an answer; it may be for an

Appeal Court or Legislation to address. Ramifications of Stop/Search were addressed through legislative change. The engagement with the Justice Committee could lead to legislative ramifications.

AR advised that the issues pertain to data retention and not kiosks. AR further advised that questions raised have led to new unchartered areas; which have not been aired in court. Defence agents have utilised traditional challenges regarding search warrants and tend to focus on Wet Forensics rather than Digital Forensics It is and area of great uncertainty the basic principles of distinction between what is specified in a search warrant, Statutory powers under the Criminal Procedure Act and whether device is being seized from a suspect, accused or where it is unknown whether a crime has been committed eg death investigation.

GM asked AR with respect to witnesses and victims is it still within police powers to carry out an examination.

AR advised when victims voluntarily provide phones with informed consent that is one thing but may be a matter for politicians if the police powers need to be altered where they don't.

GM recognised challenges are wider than kiosks and has updated the Group that a letter was submitted to Justice Committee today.

NB updated the Group that she and GM met with Diego Quiroz, Scottish Human Rights Commission, following his evidence session at Justice Committee. Mr Quiroz was provided with a demonstration of kiosk. There were subsequent discussions regarding the legal framework, Equality and Human Rights Impact Assessments and expectation of what should be considered for a wider discussion regarding case law and use of kiosk framework. His view has agitated a wider discussion regarding the legislative framework in both Scots and UK Law with regards to digital forensics

NB updated the Group, that limited case law does exist but applying the wider principles of Human Rights is challenging due to the historic nature of the case law, given that data held on a device has significantly evolved. There is a need for a wider national discussion, regarding what legislation need to look like.

NB further highlighted the document set was shared with the External Reference Group, the work undertaken by the Groups to review the documentation was acknowledged. In respect to the Public Information Leaflet, this was supported by the Group. There was a challenge regarding "what happens to the device", in answer assurance was given to the Group that there would be comprehensive signposting for the public to the Frequently Asked Questions with agility to maintain and evolve. With cognisance to the feedback from The Reference Group consideration will be given to taking the leaflet to an organisation to incorporate plain language.

GM highlighted that the Group had encouraged the inclusion of visual infographics and urged that a balance was found between being overly simplistic and overloading the public with information. The leaflet would be a helpful tool to signpost to the public facing website, providing more information to the public regarding both complaints and PIRC procedures. The Reference Group also suggested there should be a space on the leaflet to indicate someone will be in touch to enhance the customer experience by explaining timescales and organising follow up engagement. NB reinforced that the leaflet is not abdicating officer responsibility to tie in with members of the public; it will be a tool to assist the conversation and provide a point of contact.

GM suggested the most asked question would be "how long the police will have my phone "

AR highlighted public concern is not in relation to the phone but the data contained within the device.

GM stated there is a consideration to involve Victim Support if they have capacity in relation to capturing a victim's experience pre and post triage researching the benefits and differences to the victim experience.

GM queried in terms of policing powers, if a device is seized as a production can this be released back to the member of the public?

AR confirmed there is on-going national work with respect to productions, storage and the potential to use screenshots or labels in lieu for investigations in relation to less serious crimes.

GM posed the question if there is nothing evidential on the phone, could the phone be released?

AR asked why would the device be lodged as a production if it had no evidential value which in turn would preclude 90% of phones seized.

AS highlighted that phones are the main use of data signposting for people which may not be an issue if they have another device but may be an issue if they do not and do not have the financial means to purchase another.

BS highlighted 40,000 devices per year are submitted to Cybercrime leading to the storage of 10-15,000 devices. Subsequently there could be a £20m, saving to members of the public if you take into considerations the average price of device and associated contract. The current expectation would be to seek direction to release devices in relation to Serious and Organised Crime. In relation to less serious crime ongoing work is being undertaken by Angela Blair and Debbie Kelly to develop a process to release devices in lower level cases.

NB suggested Richard Whetton (Chair of the External Reference Group) may be able to take considerations to a wider arena, in terms of what the expectations would be in relation to collation of management information. The Reference Group has highlighted the EqHIRA and DPIA documents require further feedback but have concurred that the Toolkit is at an advanced stage. NB suggested further considerations should to be made with regards to whether it should be public facing document or not

GM updated the Group with respect to a complaint received by the Information Commissioners Office from Privacy International which has led to an investigation focusing on 3 forces in England. The report is due next year and whilst this does not impact on Police Scotland at present it, may become a focus in the future. Police Scotland will keep a watching brief

NB updated the Group that David Freeland and colleagues from the ICO have been invited to a meeting and demonstration of Cyber Kiosks on 6th December 2018 in Edinburgh.

6. DOCUMENT SET

MM outlined to the Group that several of the draft documents discussed and circulated prior to the meeting contained a summary of the legal framework and powers to seize and examine devices. He requested that these be considered by members and he be informed of any issues identified.

MM confirmed the document set had been circulated in terms of

- The Principles of Use Document, outlining standards with regards to digital forensics
- Toolkit
- Public Information Leaflet
- EqHRIA (Equality and Human Rights Impact Assessments

- DPIA (Data Protection Impact Assessment.)

MM confirmed these had been shared with the Group for consultation.

MM highlighted the capture of feedback suggested enhancement, with no specific issues in relation to kiosks identified.

MM confirmed the key themes related to alternatives to seizure and legal framework.

6.1 Public Leaflet

GM suggested the Toolkit has matured and confirmed there were no comments received from the Reference Group other than it should considered whether it will be an internal document or made public facing. The caveat being that to make public facing may have implications for other areas if it is to be open and transparent, internal details for example phone numbers and e-mails should be redacted. It would broadly be the same document with operational security arrangements applied. The potential to roll out training would be the next logical process.

6.2 Principle of Use

GM highlighted that the Reference Group have suggested an enhancement to Digital Forensics Principles with regards to human rights and privacy.

6.3 DPIA

GM highlighted that different categories of accused /suspect/witness/victim will be incorporated.

GM updated that the Reference Group has highlighted the inclusion of investigating officer/ user handling of notes, use of secure storage of devices scoring of residual risks rather than mitigated or accepted should be reflected.

MM queried if it was possible to articulate legal powers in respect to victim, witness, and suspect At present if a phone is seized to allow examination the phone would be lodged as a as a production, if the phone was to be returned post triage, what would the process or terminology be ?

6.3 Time line

NB updated that that The Justice Sub-committee on Policing was updated in writing on the 4th October regarding ambitions for roll out of training

NB provided an update to the Group regarding a proposed time line including consultation and engagement

The training roll out is scheduled for East 12-13th and 13-14th November. Over the two days, forty officers will be trained which equates to 10 per kiosk. The training has a significant divisional commitment in terms of abstraction.

NB confirmed she is content that in consultation with both Groups the documents are in an advanced stage and confirmed The Reference Group could see no reason to prevent training from progressing. The Reference Group expressed it would be an opportunity to engage officers and by evaluating their training experience and use of kiosks in the training environment could assist with the finalisation of the document set. It would provide an opportunity to measure the understanding of officers with respect to their obligations and responsibilities towards data protection and human rights.

Prior to “going live “the considerations highlighted with respect to the public leaflet will be accelerated and efforts to articulate the legal basis will be continued. The third piece being an assessment of kiosk locations how many were trained in each location to service these.

GM queried can a “go live” date be determined if there are not sufficiently trained officers, per kiosk location.

BS confirmed the licences allow access to any devices across network on user password; hence trained officers will not have to be location specific.

GM advised the Group that there has and will be comprehensive engagement with divisions when ready to “go live” this is planned for early mid-December although this remains under review.

NB reiterated that the outstanding concerns of the Justice Committee, Scottish Human Rights Commission and Information Commissioner’s with regards to the legal framework will have to be addressed.

HM queried how the officers who are to be trained were identified

BS explained Singe Points of Contact (SPOCs) were nominated at each division, identified suitable officers within their division

GM confirmed there have been no impediments for training and evaluation of training identified as yet

RH notes progress being made to ensure the document set is fit for purpose, but advises the key question is the legal framework of which the critical part being the letter to Crown Counsel, however advises the roll out of training should still continue

GM confirmed ACC Johnson as Senior Responsible Officer (SRO) and Chair of the Cyber Capability Programme will make any further determination on 9th November 2018

AR advises Police Scotland may get a reply but may not get an answer as there are so many scenarios it would be difficult to get a determination

RH replied until you get stated case as a result of court proceedings there may be no definitive answers.

AR stated that if the examination of devices is unlawful, it is a normal policing practice which is undertaken every day

GM agreed that it is an issue which is timely for review but the ramifications in terms of Criminal Justice to cease digital examinations are immense.

RH added Cyberkiosks are not the concern the issue is of seizure

GM advised case law relies on statutory power, common law and seizure under warrant, the device is submitted to Cybercrime for examination, it would be the investigating officer rather than the officer examining at Cybercrime who would seize the device. Police Scotland in the absence of challenge and in the furtherance of investigation and criminal justice has to hold this position at present.

GM stressed further to the importance to officer’s seizure powers that examination is necessary and proportionate and is recorded on the Examination Request Form

AR confirmed that this is good practice for any officer

GM advised the complaint made by Privacy International is not a consistent position with regards to powers to seize

AR reiterated that powers of seizure are fundamental police powers.

NB stressed during the extensive consultation period no one has provided any evidence to the contrary.

NB offered the Group the opportunity to observe training.

PB highlighted the majority of training set is focused on technical Cellebrite utilising the front end toolkit but also incorporating roles and responsibilities and empowering officers to scrutinise and challenge electronic request forms (ERF) if required.

GM added with respect to ERFs, the 410 trained officers will act as gatekeepers who will challenge submissions which are enhanced also by the supervisory check.

NB confirmed the ERF submissions for Kiosks build on existing processes, which are stringent and robust.

ST suggested in terms of the Public Leaflet, Citizen Advice and Mygov.scot can provide advice regarding language.

ST advised if third tier Government assessment is required, HMICS would look to bench mark against England and Wales as per the advice from the College of Policing.
HMICS asked to submit a response to Justice Committee which stated HMICS were encouraged by stakeholder engagement but it was too early to make any further observations.

GM stressed any undue delay between training and operational delivery will erode user confidence and could potentially damage collaboration with the Local Policing.

HM stressed the importance with having divisional engagement from the outset

AS advised the document set should be looked at from a compliance point of view.

7. AOCB

Chair afforded the opportunity to raise any areas of AOCB.

No other areas of AOCB were raised by members.

8. DATE OF NEXT MEETING

Chair thanked the members for their attendance and participation in the meeting and informed that suitable dates shall be circulated in due course and meeting date set.