Security Classification:	OFFICIAL
Contents may be seen by:	
Author:	DS Jane McCourt
Organisation:	OCCTU
Telephone:	01236 818140
Date Created:	21st June 2019

Digital Triage Device (Cyber Kiosk) Stakeholder Group

MINUTE OF THE MEETING

DATE: 1100 Tuesday 11th June 2019

LOCATION: Nellis/Collins Room Scottish Crime Campus.

CHAIR: DSU Nicola Burnett

SECRETARIAT/ MINUTES: DS Jane McCourt

MEMBERS IN ATTENDANCE:

DSU Nicola Burnett	(NB) Police Scotland, Head of Cybercrime (Chair)
DCI Iain Craib	(IC) Police Scotland Cybercrime Capability Programme
DCI Stuart McAdam	(SM) Police Scotland Cybercrime
CI Claire Dobson	(CD) Police Scotland Information Management
DI Michael McCullagh	(MM) Police Scotland Cybercrime Capability Programme
Inspector Iain McPhail	(IM) HMICS
Inspector Heather Macdonald	(HM) Scottish Police Federation
DS Anna Ripley	(AS) Police Scotland Cybercrime Capability Programme
Julie MacLeod	(JM) Information Management
Joanne Holms	(JH) Police Scotland Corporate Communications
Andrew O'Neil	(AO) Police Scotland Corporate Communications
Craig Donnachie	(CD) SPA Forensics
Iain Logan	(IL) COPFS
DS Jane McCourt	Secretariat

1. INTRODUCTION AND WELCOME

The 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

Alice Stewart-	represented by CI Claire Dobson and Julie Macleod
Robert Hayes	SPA
Roslyn Rooney	Represented by Andrew O'Neil and Joanne Holms
Inspector Stephen Tidy	Represented by Inspector Iain McPhail

4. MINUTES

The Chair proposed the minutes of the last meeting of the Cyber Kiosk Stakeholders group for consideration and any amendment.

COPFS have provided minor adjustments to the previous minutes which have been amended accordingly.

The 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. TERMS OF REFERENCE

The Chair updated there has been no change to the roll out of Cyber Kiosks; The External Reference Group had suggested that the Terms of Reference should be extended to look at the wider digital forensic piece. The concern would be that to alter the focus of the Group could affect the momentum with relation to the implementation of Digital Triage Devices. There were no objections raised from the Group.

The Chair highlighted she wished to raise the letters from The Scottish Human Rights Commission and the Open Rights Group to Justice Sub Committee on Policing under AOCB

6.1 Summary of Position

A presentation was provided by IC

- Legal basis for use of Digital Triage Devices (Kiosks) ratified by COPFS and Senior Counsel Murdo MacLeod QC
- Ongoing engagement with Justice Sub Committee on Policing
- Document suite development continues, including enhanced consent information leaflet and frequently asked questions
- Police Scotland will seek to roll out Digital Triage Devices towards the end of the Summer

6.2 Justice Sub-Committee on Policing/ Legal Opinion

IC provided a presentation on the position of Police Scotland's engagement with Justice Sub Committee

On 8th April the Justice Sub Committee on Policing published an interim report on their evidence gathering to date on Police Scotland's proposed use of digital device triage systems (Cyber Kiosks).

"The Sub-Committee do not believe that the cyber kiosks should be deployed by Police Scotland until equalities and human rights and data protection impact assessments are agreed by key stakeholders."

"The Sub-Committee do not believe that the cyber kiosks should be deployed by Police Scotland until clarity on the legal framework is established."

Police Scotland now have unambiguous clarity from both COPFS and Independent Senior Counsel that the legal framework exists and there is a legal basis for use of the Kiosks by Police Scotland.

IC confirmed that independent legal counsel senior QC Murdo Macleod provided legal opinion, which was reinforced in terms of legal basis by the COPFS submission to Justice Sub-Committee on Policing.

DCC Kerr and ACC Johnson attended the Justice Sub-Committee on Policing on 9th May and highlighted going forward that police will introduce technology with ethical considerations and engagement. DCC Kerr was clear and unambiguous that he is satisfied with regards to legal opinion and as a result, roll out will be undertaken in summer 2019.

7. DOCUMENT SET

MM provided a presentation to the Group with respect to the document set.

- Data Protection Impact Assessment (DPIA)
- Equality and Human Rights Impact Assessment (EqHRIA)

MM stressed that the DPIA and EqHRIA are the cornerstones of what we want to do, which will be enhanced by securing the agreement of Stakeholders and Reference Group in support of the EqHRIA and DPIA. Furthermore a more detailed report will be submitted to Justice Sub Committee on Policing in answer to their report as it was considered there were inaccuracies in description of the kiosk and how it would be properly used.

A status report has been submitted to the offices of the DCC and ACC office which would immediately address all issues.

In terms of the timeline Professor Deacon highlighted at Justice Subcommittee during her attendance on 9th May that " *there has been not insignificant time and resource involved in the process which has generated and significant amount of correspondence".* The last letter was submitted on 4th June following the appearance of DCC Kerr and ACC Johnson, in which it highlighted that Police Scotland would adopt Ethics and Advisory Panels which would consider dilemmas, matters of ethics and challenges. The second part of the submission focuses on the matter of consent and the requirement to capture consent whilst addressing public and interested parties concern.

- Principles
- Toolkit

- Public Information Leaflet

Legal Opinion is clear and easy read and we would look to publish on Police Scotland website and incorporate in principles document where it will be translated into user friendly language.

HM asked has anyone provided a contrary legal opinion?

The Chair confirmed that no one to her knowledge has sought contrary legal advice, The Scottish Human Rights Commission has provided in broad terms the view that we cannot be compliant.

HM asked had they sought legal opinion

The Chair replied, not to her knowledge, and added the Open Rights Group, highlighted legal cases out with jurisdiction, we have not seen anything, however that is not to say that legal opinions are not being sought.

IL confirmed the only vehicle of legal challenge would be a challenge in court, COPFS have stated in letters to Justice Sub Committee, there are no appeals that COPFS are aware of pending. COPFS are not aware of any breach of data protection which would be a civil challenge.

MM presented to the Group with a document set update.

MM highlighted in respect to the DPAI and EqHRIA and Principles document there has been extensive engagement with Information Comissioners Office and COPFS. MM confirmed no significant challenges rose pending the implementation of suggested changes.

IL highlighted that he has commented on the Principles Document. IL stated that the EqHRIA and DPIA would be for others to comment. IL suggested there may be a danger in setting out a legal basis. This could be problematic as the law is defined and evolved from stated cases, the question would be would you wish to go into detail regarding counsel and stated cases, the principles are the principles. IL suggested to take from the letter submitted by COPFS, there is a legal basis for seizure and examination. If case law is described and what is said is not strictly correct, which may be the danger in describing it. It is understood counsel opinion in doing that. There is a risk that it is misunderstood or mis-represented. There is a legal basis, how operated less is more.

MM highlighted the challenge may come from Freedom of Information Requests and people asking what is the legal basis, which is why it was felt there was a need for this to be articulated in the opening piece of DPIA and EqHRIA, to fill the gap as best we could for member of the public.

The Chair highlighted there is an expectation to articulate what the legal basis, if Section 23 Misuse of Drugs Act 1971 that would be fine as the expectation is there, but for other circumstances there would be a requirement.

IL commented that he appreciates the reasons however; the phraseology is loaded in itself. From the perspective that thousands of cases, which have digital examination as evidence whether it be a Breach of the Peace or a murder case in the High Court. There is an absolute legal basis and being used appropriately. As prosecutors we are confident of relying on it and its admissibility we might want to review and position in a direct, positive manner.

The Chair stressed it was not only the public but staff and officers who require an understanding, knowledge and confidence that the legal basis has been properly articulated.

IL concurred it is maybe about articulation and factual correctness which could be worked though.

The Chair highlighted that legal basis may be produced as a piece of evidence

IL confirmed yes it could be challenged in court and the question regarding legal basis could be asked of the prosecution, if you quote law in this scenario, broad principles don't change case law does.

The Chair highlighted the requirement for future proofing

ACTION DI McCullagh to liaise with Iain Logan, COPFS to review language and phraseology contained in the principle document and to circulate to groups for comment and consultation.

MM highlighted that it would benefit consistency across the document set and stressed it will not change anything, we know what the legal basis is, but it is how it is articulated requires focus.

JM document pending legal basis worked through yesterday our thoughts on points raised by David Freeland.

Q8 Sensitive data

Following recent events in Australia, and debate in the UK when the Investigatory Powers Bill was going through Westminster, Police Scotland should at least consider the DPIA and other documents relating to digital triage should be more specific about the potential for inspection of legally privileged material, communications by or to an elected representative, confidential journalistic material and sources of journalistic information.

It may be sufficient to reference at appropriate points in the DPIA any existing guidelines or SOPs that cover coming into contact with these types of information. If such guidelines don't exist then they should be incorporated into officer training and the Principles document.
[1]

JM highlighted documented processes and what we do is in line with Standard Operating Procedures and included in the DPIA

Q11 Context

The third paragraph says that kiosk operators will be aware that their details and activity on the kiosk are stored and audited. It is not explicit how they will know that. References or links to a privacy notice and materials for trainers if part of the training could be cited as the supporting evidence.

This is also pertinent for the information relating to Q32.[2]

JM updated the Group that the processing of personal data focus on officers as data subjects, officers will be aware. JM advised a privacy notice required as it is covered in the training material and subject to all systems

The Chair queried is this something we could look to put on kiosk? The Chair confirmed that it is covered in training but would provide an assurance collation of management information

ACTION DCI McAdam to liaise with Cellebrite regarding initial users screen on opening digital triage device to remind officers their details may be stored and audited.

[1] Email from David Freeland Information Comissioners Office dated 7th June 2019
2 Email from David Freeland Information Comissioners Office dated 7th June 2019

JM agreed a technical option could be explored but reiterated it is highlighted in training.

Q26 Lawful basis

The schedule 8 conditions only need to be in the sensitive data section of this question. There's no need to duplicate in the first section.

There are a couple of typographical errors in the second from bottom paragraph on page 35.[3]

JM advised the Group that this has been taken on board and resolved

Q27 Specified/Explicit/Legitimate

Apologies for not mentioning this in feedback on v0.12 of the DPIA, but the secondary purposes quoted (missing persons, deaths without suspicious circumstances) would not be law enforcement purposes and thus are more likely to fall under the scope of the General Data Protection Regulation rather than Part 3 of the Data Protection Act 2018. You may want to confer with Information Management on how to deal with that.[4]

JM suggested that this appeared to be a misunderstanding, it has been suggested by David Freeland that missing person and non- suspicious deaths were not law enforcement process but there will still be an investigation to establish if a crime has been committed which has to be the primary focus.

ACTION Julie Macleod to liaise with David Freeland and answer points raised, thereafter share with the Group for audit purposes.

Q30 Kept no longer than necessary

The section on data retained after the retention period is answered as 'not applicable'. However, if personal data from the management information is going to be manipulated to provide some statistical information about kiosk use for public consumption, which is Police Scotland's intention, then the methodology for producing that anonymised information should be set out here.[5]

JM queried how long would audit data stay on the kiosk?

SM replied my assumption is once got information is collated from the kiosk, it is removed but I will confirm.

The Chair what is the expectation re management of information and data retention

JM confirms there is a policy with regards to data retention.

Q32 Information duty

There appears to be a misunderstanding as to what the information duty is. The duty is to inform the individual(s) concerned about how their personal data will be used by the police for the purpose of the triage at the very least. The intention to withhold this privacy information would occur in

[3] Email from David Freeland Information Comissioners Office dated 7th June 2019
[4] Email from David Freeland Information Comissioners Office dated 7th June 2019
[5] Email from David Freeland Information Comissioners Office dated 7th June 2019

circumstances where telling the person you were going to inspect their device for relevant information would prejudice the investigation. It may become possible to provide that information later, rather than prior to collection, such as when the person is charged, and this should be noted in the DPIA.[6]

JM highlighted it may be difficult to ascertain if this is the case and this may be a simplified position JM confirmed that the DPIA will always be a living document, as it stands the DPIA is almost at Version 1 and should be submitted to the Strategic Asset Owner ACC McLaren

The Chair asked the Group if they would wish to see the DPIA prior to submission to the Strategic Asset Owner.

HM confirmed yes particularly with respect to the information regarding officers

ACTION once amendments made to DPIA, it should be re-circulated for comment prior to submission to Strategic Asset Owner ACC McLaren

MM advised the toolkit has not been circulated simply due to engagement with division confirming, nothing in the original toolkit has been changed, just additions in the guidance.

MM updated on 29th May Cybercrime Capability programme held a public engagement event on Digital Device examination and Consent capture.

Attendance for the events included numerous organisations representing all protected characteristics and victims of crime including domestic abuse and rape. The event sought to engage the public regarding their understanding of device examination identify key concerns and discuss the challenges and potential solutions to consent capture.

The event was extremely beneficial to all involved with the Groups and Programme achieving a greater understanding of each other's perspectives and the complexities of Consent. Feedback on the event was positive and Programme will seek to continue this engagement in the products considered for public information and consent capture.

MM provided via presentation information relayed at the event for the attendees

Annual Policing Plan

Policing Priority:
Working with communities - Engaging with the public and communities to build resilience and prevent crime

Our objective:
- Improve the reach of our public and community engagement initiatives

Police Scotland will:
- Develop and enhance how we engage the public
- Communicate regarding their needs and local issues, including hard to reach and diverse communities

MM provided the Group with an update via presentation to the Group on

Standards of Service for Victims and Witnesses 2019-2020

Consent Capture Form and FAQs

[6] Email from David Freeland Information Comissioners Office dated 7th June 2019

The Impact of taking devices.

- *We will ensure you have fair and equal access to services throughout and are treated with dignity and respect at all times regardless of age, disability, gender identity, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex or sexual orientation.*

Examination Kiosk

.

We will discuss with you how you will be kept informed of progress in your case; we will also explain how we will deal with your case and what we may ask you to do to help us.
We will consider, with our partners, your particular needs, and thereafter try to ensure those needs are met.

Event Objectives

- Engage with the communities to provide reassurance and understanding regarding Police Scotland's approach to digital forensics.
- Ensure Police Scotland understands the needs and concerns of our communities regarding digital device examination and consent, addressing and mitigating these concerns where possible.

This is about you and who you represent. Your concerns define our requirements.
Help us design a considered, relevant and effective process

Examination of Digital Devices – Format

Group Discussions – Capture the Opinions / Impact / Improvement
Split agenda –

1- Digital Device Examination

2 – Consent

- Question and Answer format
  - Informal / Interactive / Open
  - Red Card
  - Scenarios
- Board -Concerns / Solutions
- Suggestion Box
- Flip Charts
- Discussion

How this is captured

Examination of Digital Devices

- When do Police examine digital devices?
- Who will examine a device and view the data?
- What information do Police look at on victim's device
- What happens with the data from a victim's device?
- Why do the police take this much data?
- Do Police share the victim's device data
- Why can't the Police just use the suspect's device to obtain the relevant data?
-

What other questions are the victims / witness likely to have?
What would work best for this type of public engagement / messaging?

Consent - Key Points

- Background – NPCC, England and Wales
- Applies to victims and witnesses.
- Why is Police Scotland doing this –This is not a material change it is doing what we do but better
- Doing the right thing for the victim where we can.
- How? -A Form?

WHAT DOES THAT FORM NEED?

MM highlighted what was learned from the engagement event is that consent need to be better informed

The Chair stressed that we already capture consent; we just want to do it better and demonstrate we have good communication with someone giving consent. We are not doing anything differently down south; however some of the language has been unfortunate
For example if you are rape victim but don't give phone you may not get justice the language This has led to an inference that digital stop searches being undertaken, we are not suddenly randomly stopping people in the street, something has had to have taken place, the device is a line of enquiry, which requires a conversation

The Chair stressed that this was the first engagement piece, which we need to keep going in terms of engagement. From the feedback, data was not an issue but people were concerned about getting their device back. It was stated by the attendees take everything off the phone, but give me the device as I am paying a contract. It really surprised me but data generation is different relationship with data.

IL stressed the safety of the individual is paramount for example in the case of domestic violence, to take the phone away endangers a victim's safety.

MM highlighted that feedback was collated and circulated to the attendees. The next event is scheduled for 5th July developed from feedback from the first event.

MM presented the feedback gained

Has today's event enhanced your knowledge and understanding of Police Scotland's examination of digital devices? *YES 12 / NO NIL*

Has today's event enhanced your knowledge of Cyber Kiosks, their intended use and processes involved? *YES 12 / NO NIL*

Has today's event enhanced your knowledge of Police Scotland's considerations when seeking consent for digital device examination? *YES 11 / NO 1*

Overall, do you feel the event has given you the opportunity to discuss your views and provide feedback? *YES 11 / NO NIL / SOMEWHAT 1*

IM asked the Chair if at the engagement meeting on 29th May was there geographical representation as someone who lives in Inverness may have different view from someone in the central belt. IM also asked has there been consideration of using "My View Counts?"

MM highlighted there were 45 National agencies invited, looked at venues, however there were logistical constraints

IM suggested that as part of the Annual Policing Plan, "My View Counts" may attract a lot of responses and further engagement.

MM reiterated the issue of consent is not for kiosks is not particular to kiosks but for the wider digital forensics piece.

The Chair added we inform national representatives there would be an expectation to disseminate and cascade throughout their organisation

JH advised if there is a need to pursue other lines of engagement. Corporate Communications can advise and support.

The Chair read a letter received from David Freeland, ICO and advised he had also shared with External Reference Group of which he is a member.

IL advises it is a matter for Government that needs clarity in the law in terms of data protection, not seizure or examination on the basis that we don't write law we are interpreting the law

JM advises similar to engagement it would require an overhaul of criminal justice system we have been told the lawful basis which is a wider conversation not for this forum

The Chair explained that the Justice Minister is giving evidence on Thursday which is the reason why letters are going out just now.

8. Processes

SM provided an update and presentation on the Electronic Referral Form and circulated the Gateway Review Flowchart.

SM confirmed that the gateway and supervisor provide a second layer of scrutiny to ensure examination is both necessary and proportionate. This was adapted from the feedback given by supervisors articulating requirement for more depth to demonstrate devices were justified and legally seized

Management information (MI) will be extracted from the Cybercrime Case Management System (CMS) on a monthly basis. The information will be drawn directly from the system automatically and thereafter formulated to provide an MI in an easy to read format and will report on:-

- **CRIME GROUP/TYPE**
- **REASON/ PURPOSE OF EXAMINATION**
- **REGION/ UNIT/DIVISION/ KIOSK**
- **STATUS OF OWNER**
- **DEVICE TYPE**
- **POWER OF SEIZURE**
- **DECLINED FORMS/ REASON**

Digital Triage Devices do not retain information extracted from devices, however statistical information is recorded to allow Cybercrime management to monitor demand and ensure equity of service throughout the country.
This data will be collected from Digital Triage Devices on a regular basis and Police Scotland intends to publish this information on the public website to increase public confidence in the use of Digital Triage Devices

SM provided via presentation an update on audit and assurance

- Regular reviews of the Crime Management Systems are carried out by Detective Inspectors and Digital Forensic Co-ordinators to provide quality assurance of the Electronic Referral Form and gateway process.
- 'Dip Sampling' checks are carried out on a monthly basis from the Management Information
- Management Information will be scrutinised to ensure appropriate use of kiosks and to

identify areas for development/ good practice
- Management Information from the kiosks will be reviewed regularly to ensure compliance of process and cross check with Crime Management, Management Information

SM confirmed a moodle package will provide for supervisors specific guidance and training

SM confirmed ICT has changed to it will be one form information does not need to be copied across

Rationale from kiosk user will be recorded therefore if submitted to a hub there will be background information. All gateway Detective Sergeants will be co-located to allow consistence process across the Organisation

SM stressed that the gateway form is automatically generated for supervisors. The Crime Groups are cognisant with Crime Recording Standards. Drop down boxes will give management information, and will collate information divisionally with respect to what kiosks are being used and how often.

SM advised risk factors allows gateway to prioritise self-populate e-mail to supervisors, which they will acknowledge ensuring devices provided on a voluntary basis are supported by written consent by owner.

CD highlighted that the Electronic Referral Form it is well structured and concise, which would meet the requirements of ISO17025 standard and request tenders and contracts and confirmed it would be fit for purpose

IM good to see level of scrutiny
Chair as area of business understanding what being asked of us start of improvement journey

9 Training/ Evaluation

IC provided an update via presentation of training he highlighted that Phase 2 of training was completed on 9th May 2019 with a total of 410 officers now trained in the use of Digital Triage Devices. This provides a cadre of 10 trained officers available for deployment for each Digital Triage Device, which will be monitored to ensure equity of service throughout the country.
As with Phase 1, an evaluation of Phase 2 training is scheduled for 27th June 2019 where organisational learning points will be identified and captured for future training. The subsequent evaluation gained 100 % response rate.

IC updated the Group with respect to Phase One Formal Debrief

Key Organisational Learning Recommendation (OLR 1)

A sustainable, dynamic and accessible training package and communication platform to be developed which caters for the needs of Cyber Kiosk Users at all stages to include pre read and user guidance material, current policy and procedure and examples of organisational learning.

IC updated that recommendation one was held in toolkit and readily available. The Chair added That once implemented there will be case studies built in.[7]

Key Organisational Learning Recommendation (OLR) 2:

Cyber Kiosk Training to be delivered by Cybercrime subject matter experts and to include training on policy, procedure and practical deployment of the Kiosk in line with each key role that will operate and interact with the Cyber Kiosk, i.e. Triage Officer, Supervisor, Cybercrime and

[7] Cyberkiosk Phase 1 Training Delivery Initial Debrief

Senior Investigating Officers[8]

IC confirmed the recommendation has been addressed with key roles and responsibilities being defined in the toolkit

Key Organisational Learning Recommendation (OLR) 3

Effective liaison and communication lines between Cybercrime and Local Policing to be established in order to support the initial operational deployment of Cyber Kiosks, on-going use and regular assessment and review of distribution and appropriateness of the same in line with operational demand[9]

IC confirmed ongoing support is provided via a group e-mail system, which provides a two- way system of communication with Cybercrime and peer group address. A hotline number to digital forensics staff has been provided and there is a step by step guide on the kiosk. There will be Liaison on quarterly basis with divisional spocs, regarding who is still trained, and to identify up any issues of training and resilience and inform CPD events, regional or local deployments.

Key Organisational Learning Recommendation (OLR) 4

Liaison between Cybercrime and COPFS to take place with regards to a standard statement template for Triage Officers which would highlight the search parameters requested in the ERF form and the search undertaken in the triage, which would reinforce that Triage Officers have only set the terms of search which were requested and authorised in the ERF process.

IC confirmed contained within the Toolkit is a draft pro forma statement which allows input parameters of search in statement[10]

10. Review of Action Log- to be updated

11. AOCB

The Chair afforded the opportunity to raise any areas of AOCB.

IL asked if timeframe for ICO investigation and confirmed the ICO had contacted COPFS regarding information on retention.

The Chair confirmed that this would likely be available in the near future.

No other areas of AOCB were raised by members.

12 DATE OF NEXT MEETING

The 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.

[8] Cyberkiosk Phase 1 Training Delivery Initial Debrief

[9] Cyberkiosk Phase 1 Training Delivery Initial Debrief

[10] Cyberkiosk Phase 1 Training Delivery Initial Debrief