Date: 20 July 2018

Your Ref:

Our Ref:

The Convener
Justice Sub-Committee on Policing
Scottish Parliament
Edinburgh
EH99 1SP

Nicola Burnett
Detective Superintendent
Organised Crime & Counter Terrorism
Specialist Crime Division
Scottish Crime Campus
Craignethan Drive
Gartcosh
G69 8AE

Nicola.Burnett@scotland.pnn.police.uk

Dear Convener

Further to the appearance of DCS Gerry McLean at the Justice Sub-Committee on Policing on Thursday 21 June 2018, I am writing to provide the additional information you requested via the Clerks in emails dated the 22 and 27 June 2018.

Business Case

A redacted copy of the Police Service of Scotland Business Case in support of Cyber Kiosks was provided to Committee prior to the last Evidence Session. To confirm this was authored by Mr Mike Dickson (CyberCrime) on 28 October 2016.

EqHRIA & DPIA

Attached separately are draft copies of Equality & Human Rights Impact Assessment (EqHRIA) and Data Protection Impact Assessment (DPIA). It has been highlighted to the Clerks that these documents are draft and will be finalised at the conclusion of stakeholder and external reference group engagement. Once finalised, these assessments can then be forwarded to the Committee. As with all assessments they will thereafter be subject to regular review.

External Reference Group

PSOS has now established a Reference Group to consult regarding the roll out of the Cyber Kiosks. The purpose of the Cyber Reference Group is to help inform the development, the directions and the implementation of policy supporting cyber kiosks.

The objectives of the group are to:-

- To be a point of reference for Police Scotland's development of policy and ethics to respond to the use of Digital Device Triage Systems (Cyber Mobile Kiosks).

- To provided challenge, test and scrutiny of the Police Scotland review process and of the outcomes to be delivered to ensure a value- based service is delivered.

- To highlight areas of compliance with relevant legislation that should be considered in any future model in accordance with human rights, data protection and security, privacy and employment law.

- To assist in the development of a Code of Ethics and associated behaviours.

The Group will comprise of representatives from Aamer Anwar & Co, Privacy International, Biometrics Advisory Group, Scottish Human Rights Commission and the Information Commissioners Office.

The inaugural meeting is due to take place on 26 July 2018. Further meetings have been scheduled for 13 August 2018.

Stakeholder Reference Group

PSOS has now established a Stakeholders' Group is to help inform the development, the direction and the implementation of policy.

The objectives of the group are:-

- To be a point of reference for Police Scotland's development of policy and ethics to respond to the use of Digital Device Triage Systems (Cyber Mobile Kiosks).

- To provided challenge, test and scrutiny of the Police Scotland review process and of the outcomes to be delivered.

- To highlight areas of compliance with relevant legislation that should be considered in any future model in accordance with human rights, data protection and employment law.

- To consider challenges for partner agencies and wider implications for the Criminal Justice System.

- To ensure enhanced delivery by considering suitable training and Continuing Professional Development for operational officers involved in the deployment of Digital Device Triage Systems (Cyber Mobile Kiosks).

- To assist in the development of a Code of Ethics and associated behaviours.

The group will comprise of representatives from the Scottish Police Authority (SPA), Crown Office & Procurator Fiscal Service (COPFS), Scottish Police Federation, Scottish Government Defence, Security & Cyber Resilience Division and HM Inspectorate of Constabulary for Scotland (HMICS).

The inaugural meeting took place on 27 June 2018. A further meeting has been scheduled for 27 July 2018.

Code of Practice & Time Line

PSOS Cybercrime Digital Forensics Team are in the process of developing the policy, practice, procedure and training to support roll out and operation of these devices. It is anticipated that this will culminate in the development of an overarching Code of Practice (CoP) which will be consulted on via the aforementioned groups. Once finalised, a copy of this can be made available to the committee.

It is anticipated that consultation via the aforementioned reference groups will run into September 2018. Once complete, the intention would be to commence an incremental roll out programme, commencing in Edinburgh, where each of the local policing areas would receive hardware (kiosks), training and support to the officers identified as suitable to operate the devices. We anticipate a phased 'go live' staring in September and concluding in December 2018.

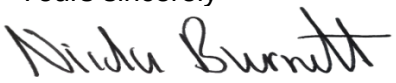
SPA Papers

In relation to the further information requested by the Sub- Committee in relation to papers that were provided by Police Scotland to the SPA Board to consider on costs. I can confirm a business case for cybercrime infrastructure (presented alongside the National Cybercrime Technical Strategy) was approved by the SPA Board in March 2015. This was prepared by (then) DSU Steven Wilson and (then) DI Brian Stuart. This included the provision of a range of cybercrime infrastructure, including cyber kiosks.

The introduction of an Investment Governance Framework to Police Scotland in 2017/18 meant that capital planning processes became more robust, and governance routes and funding approval became much clearer. As a result, a revised 2017/18 Capital Plan was approved by the SPA Board in September 2017. This included funding of £3.6m for cyber infrastructure. As a business case had already been approved by the SPA Board, the business case financial model was updated for changes in technology specification and pricing, whilst keeping in line with the strategic direction of the original business case. The infrastructure was purchased and delivered in full in 2017/18.

If I can be of any further assistance please do not hesitate to contact me.

Yours sincerely



Nicola Burnett
Detective Superintendent
Organised Crime and Counter Terrorism

SCOTTISH POLICE AUTHORITY

POLICE SCOTLAND
POILEAS ALBA

Division	SCD
File Path Record	

Police Scotland / SPA Equality and Human Rights Impact Assessment (EqHRIA)

This form is to be completed in accordance with the instructions as set out in the EqHRIA SOP and the EqHRIA Form Guidance.

Name of Policy / Practice (include version number)	Mobile Phone Kiosks – Purpose and Use
Owning Department	Cybercrime

1. Purpose and Intended Outcomes of the Policy / Practice - Consider why this policy / practice is being developed / reviewed and what it aims to achieve.

The Policy/ SOP aims to give police officers and police staff guidance on how to securely process data whilst using the mobile phone kiosks.
The Policy/SOP gives guidance on the use and governance of the mobile phone kiosks which will be installed within police premises.

2. Other Policies / Practices Related or Affected - Which other policies / practices, if any, may be related to or affected by the policy / practice under development / review?

The Policy/SOP also refers to the seizure of devices and production handling process.

3. Who is likely to be affected by the policy / practice? (Place 'X' in one or more boxes)											
No impact on people	☐	**Police Officers**	☒	**Special Constables / Cadets**	☒	**SPA / Police Staff**	☒	**Communities**	☒	**Partnerships**	☒

3.1 Screening for Relevance to Equality Duty – if the policy / practice is considered to have no potential for direct or indirect impact on people, an Equality Impact Assessment is not required. Provide information / evidence to support this decision below, then proceed to Section 5 of the form, otherwise complete all sections.

It has been decided not to complete an equality impact assessment because

4. Equality Impact Assessment - Consider which Protected Characteristics, if any, are likely to be affected and how.			
4.1 Protected Characteristics Groups	**4.2 Likely Impact** Positive, Negative or No Impact (Assessment of Low / Medium / High impact)	**4.3 Evidence Considered** (e.g. legislation / common law powers, community / staff profiles, statistics, research, consultation feedback) **Note any gaps in evidence and any plans to fill gaps.**	**4.4 Analysis of Evidence** (Summarise how the findings have informed the policy / practice – include justification of assessment of No Impact)
General / Relevance to All	Positive impact on officer, staff and those whose personal data is processed by PSoS.	Legislation – The Data Protection Act 1998 and The Human Rights Act 1998. The Data Protection Act 2018 alongwith guidance from the General Data Protection Regulations and Computer Misuse Act.	The SOP details in full, the sections within the legislation relating to the processing of personal data by informing officers and staff of their responsibilities, ensuring they know how they should handle personal data ensuring the public can have greater confidence in knowing their personal data is handled appropriately and retained securely by PSoS. All training provided in relation to an individual role will take account of any protected characteristics identified.
Age	No impact		
Disability	No impact		
Gender Reassignment	No impact		

Marriage and Civil Partnership	No impact		
Pregnancy and Maternity	No impact		
Race	No impact		
Religion or Belief	No impact		
Sex	No impact		
Sexual Orientation	No impact		

5. Human Rights Impact Assessment - Consider which rights / freedoms, if any, are likely to be protected or infringed?

5.1 Rights / Freedoms Relevant to Policing	**5.2 Assessment** Protects and / or Infringes or Not Applicable	**5.3 Analysis** What evidence is there as to how the process / practice protects or infringes Human Rights.	**5.4 Justification** – Summarise the following: • Legal Basis • Legitimate Aim • Necessity
Article 2 Right to Life	Protects	In the event of a Crime in Action or incident where there is an immediate threat to life the proposed Policy, Practise and Procedures associated with use of Cyber Kiosks will allow for the use of the technology in support of preventing loss of life.	The common law or warrant allows for PSOS officers and staff to seize items that may be relevant to the inquiry with the legitimacy of preventing the loss of life. Any use of the equipment will be Proportionate, Lawful, with appropriate authority, necessary and ethical.
Article 3 Prohibition of Torture	N/A		
Article 4 Prohibition of Slavery and Forced Labour	Protects	In the event of a report of Slavery or Forced Labour (Human Trafficking) being reported where there is an immediate threat to individuals the proposed Policy, Practise and Procedures associated with use of Cyber Kiosks will allow for the use of the technology in support of investigations.	The common law or warrant allows for PSOS officers and staff to seize items that may be relevant to the inquiry with the legitimacy of investigating incident involving slavery or Forced Labour. Any use of the equipment will be Proportionate, Lawful, with appropriate authority, necessary and ethical.

Article 5 Right to Liberty and Security	Protects	The practise will assist investigators in identifying relevant information either inculpatory of exculpatory to the enquiry.	This approach and deployment seeks to reduce the need for persons to be unnecessarily detained, whilst also protecting the wider security of the Public with early identification of offenders and their timeous presentation into the criminal justice process
Article 6 Right to a Fair Trial	Protects	The practise will assist investigators in identifying relevant information either inculpatory of exculpatory to the enquiry.	This approach and deployment seeks to reduce the need for persons to be unnecessarily detained, whilst also protecting the wider security of the Public with early identification of offenders and their timeous presentation into the criminal justice process
Article 7 No Punishment without Law	N/A		
Article 8 Right to Respect for Private and Family Life	Yes	Governed by legislation, Policy and SOP	Data obtained using current Police powers and legislation that are Proportionate, legal, accessible, necessary and ethical means to progress relevant investigation.
Article 9 Freedom of Thought, Conscience and Religion	N/A		
Article 10 Freedom of Expression	N/A		
Article 11 Freedom of Assembly and Association	N/A		
Article 14 Prohibition of Discrimination	N/A		
Protocol 1, Article 1 Protection of Property	Protect	Governed by legislation, Policy and SOP	Data obtained using current Police powers and legislation that are Proportionate, legal, accessible, necessary and ethical means to progress relevant investigation.

6. Decision - Decide how you will proceed in light of what your analysis shows (Place **'X'** in appropriate box)		
6.1	**Actual or potential unlawful discrimination and / or unlawful interference with human rights have been identified, which cannot be justified on legal / objective grounds. Stop and consider an alternative approach.**	☐
6.2	**Proceed despite a potential for discrimination and / or interference with human rights that cannot be avoided or mitigated but which can and have been justified on legal / objective grounds.**	☐
6.3	**Proceed with adjustments to remove or mitigate any identified potential for discrimination and / or interference in relation to our equality duty and / or human rights respectively.**	☐
6.4	**Proceed without adjustments as no potential for unlawful discrimination / adverse impact on equality duty or interference with human rights has been identified.**	☒

7. Monitoring and Review of Policy / Practice - State how you plan to monitor for impact post implementation and review policy / if required, and who will be responsible for this.

This Policy, Practise and Procedure detailed within the SOP will be reviewed annually or when there is a significant deviation or alteration to any elements of the SOP.

8. Mitigation Action Plan - State how any adverse / disproportionate impact identified has been or will be mitigated.

Issue / Risk Identified	Action Taken / to be Taken	Action Owner / Dept.	Completion Date	Progress Update

9. Management Log

9.1 EqHRIA Author Log

Name and Designation	Dugald Murray, Detective Sergeant	**Date** (DD/MM/YY)	10/05/2018
Comments	Completed initial form		
Name and Designation		**Date** (DD/MM/YY)	
Comments			
Name and Designation		**Date** (DD/MM/YY)	
Comments			

9.2 Quality Assurance Log

Name and Designation	Brian Stuart, Detective Chief Inspector	**Date**	11/05/2018	**Document Version**	0.2
Comments	Reviewed document with author and DI Cunningham and made necessary alterations.				

Name and Designation		**Date**		**Document Version**	
Comments					
Name and Designation		**Date**		**Document Version**	
Comments					

9.3 Divisional Commander / Head of Department Log

Name and Designation		**Date** (DD/MM/YY)	
Comments			
Name and Designation		**Date** (DD/MM/YY)	
Comments			
Name and Designation		**Date** (DD/MM/YY)	
Comments			

9.4 Publication of EqHRIA Results Log

Name and Designation		**Date Published**		**Location of Publication**	
Comments					
Name and Designation		**Date Published**		**Location of Publication**	
Comments					
Name and Designation		**Date Published**		**Location of Publication**	
Comments					

Data Protection Impact Assessment – Mobile Phone Kiosks

Law Enforcement Processing only

Control Sheet

Title	Mobile Phone Kiosks
Date Approved	
Version Number	0.1
Document Type	Data Protection Impact Assessment
Document Status	DRAFT
Author	DS Dugald Murray
Strategic Asset Owner	a) DCC Crime and Operational Support - Johnny Gwynne

Revision History

Version	Date	Summary of Changes
0.1	16/05/18	First draft

Consultation History

Version	Date	Name	Designation
			Information Asset Owner
			Project Board Chair
			etc

Part 1 - Determining whether the proposed processing of personal data for law enforcement purposes is likely to result in a high risk to the rights and freedoms of the data subject.		
Once completed, this part must be submitted to Information Management to validate the decision. (Refer to guidance note 1 for the definition of law enforcement purposes)		
Q1	Does this project involve the processing of personal data? (Refer to guidance **Note 1**)	Yes
Q2	Who is the Lead/Manager/Senior Responsible Owner for the project? (Provide name, designation and contact details)	Detective Chief Inspector Brian Stuart, Cybercrime telephone number 0131 335 6111
Q3	Provide a summary of the project.	The project concerns the introduction of 41 Cyber kiosks- As part of Police Scotland's commitment to its Policing 2026: Serving a Changing Scotland programme of work, the Service has made significant investment in cybercrime, and through a programme of modernisation is developing a model to meet current and future demands. The introduction of 41 Cyber kiosks will increase the cybercrime digital forensic capabilities for Police Scotland by offering a triage point in the examination process. Seized mobile devices will include those handed over voluntarily by victims and witnesses, as well as those obtained under the authority of a judicial warrant, statutory power or following a suspect's arrest. These Cyber kiosks provide specially trained officers (in the region of 410 officers) with the ability to triage lawfully seized devices, reducing the number which are required to be forensically examined, and reducing the inconvenience to a witness or victim of retaining a device which, on later examination, has no evidential value. No data is retained by the kiosk.
Q4	Detail the benefits of the project to Police Scotland.	Improved service to frontline officers resulting in offences being detected earlier thereby enabling more timely investigations. Triage will result in fewer devices being submitted to Cybercrime reducing backlogs. This is in line with the commitment to Policing 2026: Cyber kiosks represents a programme of modernisation which is developing a model to meet current and future demands.

		Promotes measures to prevent crime, harm and disorder quicker than the sytem that was in place prior to the Kiosks - whereby all devices were sent to Cybercrime - now only those assesed as relevant are progressed. It reduces a build up of devices pending examination as the specially trained officers will only be looking to assess specific information relative to offences under investigation. Cyber Crime in general - these crimes are a growing enabler to offending across Scotland. The majority of cyber-crimes reported related to sending messages that were grossly offensive or of indecent, obscene or menacing character via text message or on a social media platform. The Home Office Review of Cyber Crime (2013) stated that 'under-reporting of both cyber dependent and cyber enabled crimes is an issue amongst the general public and businesses', meaning that Police Scotland is more able to quantify the true scale of this issue and positively impact on criminality.
Q5	Detail the benefits of the project to any other relevant parties.	The kiosks have the potential to examine witness phones as well as suspect devices and thereby could offer the earlier return of devices to victims versus being put in the Cybercrime backlog to await examination. This allows an early decision to be made about the relevance of any device seized and delivers a more efficient process for frontline officers, the public, and the criminal-justice system. If no criminality is detected, the device can be returned with relative speed. In any case, no data will be retained by the kiosk. It is similar to the seizing of any other device except this initial view of data is made simple by the use of the technology and takes less time, which vastly frees up resources.
Q6	Define who has responsibilities for the data. (Provide name, designation and contact details) a) Strategic Asset Owner b) Tactical Asset Owner	a) DCC Crime and Operational Support - Johnny Gwynne b) DCS OCCTU -Gerry McLean
Q7	What personal data is to be processed? (Refer to guidance **Note 1**)	Personal and Sensitive Data.
Q8	What sensitive data if any, is to be processed? State the categories. (Refer to guidance **Note 1**)../../../../../../personal_data_east/Personal/1497510/Cybercrime Forensics 2012 to May 2018/Cyber Uplift PROJECTS Aug 2017/Kiosks/Data Protection Impact Assessment - Law Enforcement Processing - Guidance.doc - _Hlk513794443	In general terms any data that is held on a device - other than that which is cloud based or requires an internet connection - as such, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or TU membership; genetic data, or of biometric data, for the purpose of uniquely identifying an individual; data concerning health; data concerning an individual's sex life or sexual orientation. The data will be assessed but not extracted from the device.

Part 1 - continued		
Q9	What is the nature of the processing? (Refer to guidance **Note 2**)	Processing is using new technologies to Police Scotland and it is also a new kind of processing where no DPIA (or Privacy Impact Assessment has been carried out before.
Q10	Define the scope of the processing (Refer to guidance **Note 3**)	Introduction of a new IT software/hardware to process personal data for a law enforcement purpose – As advised above, it is the expansion of existing hardware/software to process personal data for a law enforcement purpose - mobile phone kiosks deployed within Police buildings to enable officers to triage mobile devices. The scope of processing, or what the processing covers includes a wide variety of personal data which is stored on the devices. This will take the form of text, images etc. The duration of processing will be limited to ascertaining the evidential value of the device and will target specific data in order to minimise unnecessary processing of data - this is not designed to be a method of "phishing".
Q11	Explain the context in which the processing will take place (Refer to guidance **Note 4**)	Triage of data from device to ascertain whether further enquiry or retention of the device is proportionate or necessary - or whether the device should be passed to Cybercrime - devices will not be triaged if there is vast data, indecent images, if the device is damaged or where a victim has disclosed that they have images/video of criminality. Only authorised officers will undertake the triage via the Kiosks, these officers will subject to audit and compliance checks to ensure adherance with prescribed guidelines. Processing will be undertaken in accordance with the Act and those concenred will be categorised as Victim, Witness, Suspect and Unknowm - all devices triaged will be
Q12	Describe the purpose of the processing (Refer to guidance **Note 5**)	Increased accessibility to officers to Mobile Device Kiosks will help establish if device contains data that is relevant and of evidential value. Legitimate interest- Policing purpose - Justice for individuals and prevention and detection of crime and prosecution of offenders Intended outcome for individuals- devices assessed quicker than sending all to Cybercrime as per previous procedure. Devices will be returned quicker to suspect/victim.

		Benefits- matters progressed to Cybercrime and inturn COPFS quicker. Only relevant devices being forwarded to Cybercrime. Freeing up of time in so far as only relevant devices will be passed for assesment. There has been documented public concern regarding the Kiosks. No data will be extracted at the Kiosks: date ranges can be used to assess specific information. This is not a Phishing excersise and all Kiosks activity will be logged and is fully auditable.
Q13	How many individuals will be affected by the processing, or what is the proportion of the relevant population affected?	The numbers will vary dependent on the number of investigations undertaken by Police Scotland and the number of devices seized during those enquiries. This is not quantifiable. For example, one device may have data concerning a number of individuals. Nonetheless, in a typical year we are likely to see approximately 10,000 mobile devices.
Q14	Is the personal/sensitive data already held by Police Scotland but it is now the intention to use it for another purpose? If so, provide full details of current purpose and new purpose.	No - data or the data held on devices to be triaged is not held by PS. Data will be assessed only and passed where necessary to Cybercrime. It will only be used as a triage tool to assist with processing relevant devices, and assessing more quickly those with evidential value.
Q15	Taking account of the types of personal/sensitive data to be processed, and the; • nature, • scope, • context and • purpose of the proposed processing, is the processing likely to result in a high risk to the rights and freedoms of the data subjects concerned? Provide the reason for your conclusion (Refer to guidance **Note 6**)	High Risk Processing We implement measures that adhere to an approved code of conduct / certification mechanism and we have additional policies and ensure that controls are in place to enforce them. The approved code of conduct is contained within the recently completed SOP. Further, we have an information security SOPs and take steps to make sure that this is implemented and undertake an analysis of the risks presented by our processing, and use this to assess the appropriate level of security we need to put in place: we understand the requirements of confidentiality, integrity and availability for the personal data we process and will audit users to ensure compliance.

Once this part (Part 1) has been completed, send it to the Information Assurance or ISO mailbox. IM will determine whether the processing is likely to be a high risk. A response will be sent to you within 5 working days.

The remainder of the Data Processing Impact Assessment (DPIA) should continue to be completed in the meantime.

Part 2 – Systematic Description of Processing		
In this section, describe the processing in detail.		
Q16	What will be the classification of the personal/sensitive data under the Government Classification Scheme? (GSC) Government Security Classification SOP	OFFICIAL-Sensitive
Q17	Exactly what personal data will be processed as part of the project? (Refer to guidance **Note 1**)	Potentially all types of sensitive data could you be processed as per question 8 answer: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or TU membership; genetic data, or of biometric data, for the purpose of uniquely identifying an individual; data concerning health; data concerning an individual's sex life or sexual orientation.
Q18	What, if any processing of sensitive data will be carried out and why? (Refer to guidance **Note 1**)	Sensitive data will be a potential by product of the triage process when the objective is to identify if the device contains data relevant to the enquiry - however this will be at a minimum, the Kiosk can assess data from a specified date range, for example, when a crime was perpetrated. We will have a valid lawful basis in order to process personal data from the devices, and we will have checked that the processing is necessary for the relevant purpose (law enforement), and are satisfied that there is no other reasonable way to achieve that purpose - processing is necessary for Police Scotland to perform a task in the interest of our official function - the task will have a clear basis in law - for example Police Fire Reform Act.
Q19	What is the source of the personal/sensitive data?	The source of the data will be held on the device triaged via the Cyber Kiosk - this will be contained in associated software programmes/apps on the device.
Q20	Will the personal/sensitive data be fully identifiable, pseudonymised or anonymised? (Refer to guidance **Note 7**)	No

Part 2 – continued		
Q21	Will another organisation be processing any of the personal/sensitive data either on behalf of Police Scotland or in conjunction with Police Scotland? e.g. contractors, external ICT support, partners? If so, provide details of: • the organisation • its Data Protection Officer and • the exact role of the other organisation in the processing of the data?	No
Q22	In relation to the proposed processing, what is the status of: a) Police Scotland b) the other organisation? (Refer to guidance **Note 8**)	Police Scotland (Chief Constable) will be the Controller
Q23	What training will be provided for individuals: • Within Police Scotland • Partners • Contractors/subcontractors	All users of the Mobile Phone Kiosk will required to certified and undergo training before using the equipment. The training will be delivered by trained trainers who are proficient in the use of the software. They will cascade this training to the 410 nominated officers in courses lasting two days. There will be no non-police access - all users will be suitably vetted and trained police officers. No partners or contractors will have access.
Q24	What Polices /SOPs /SyOps /Guidance, etc. will be in place prior to the commencement of processing?	Police Service of Scotland Mobile Phone Kiosks – Purpose and Use SOP DPIA, EqHRIA and SYOPS.
Q25	Data Flow analysis – (Refer to guidance **Note 9**)	

Part 3 – Assessment of Necessity and Proportionality

In this section, you are required to assess whether the processing is necessary and is not excessive.

	Requirement – The Data Protection Principles		Comments
Q26	**DPA 2018** **1st Principle** **Sections 35 & 42 Schedule 8**	**Lawful/Fair:** (Refer to guidance Note 10) • Is the processing based on consent and if so, why? • If the processing is necessary for the performance of a task? If so, provide details of the task.	The 1st principle - this data will be processed for law enforcement purposes and wiil be lawful and fair. Under Schedule 8, the processing of data meets a number of conditions - Administration of justice 2. This condition is met if the processing is necessary for the administration of justice. Protecting individual's vital interests 3. This condition is met if the processing is necessary to protect the vital interests of the data subject or of another individual. Safeguarding of children and of individuals at risk 4 (1) This condition is met if— (a) the processing is necessary for the purposes of— (i) protecting an individual from neglect or physical, mental or emotional harm, or (ii) protecting the physical, mental or emotional well-being of an individual. 42 Safeguards: sensitive processing (1) This section applies for the purposes of section 35(4) and (5) (which require a controller to have an appropriate policy document in place when carrying out sensitive processing in reliance on the consent of the data subject or, as the case, in reliance on a condition specified in Schedule 8).
		Sensitive Processing: (Refer to Note 1 and Note 10) • Does the processing involve processing of sensitive data?	Yes, this does involve processing sensitive data. During that triage examination collateral intrusion will occur and sensitive data may be accessed,

		• If so, state which categories are being processed? • Is the processing being based on consent? If so, why is consent appropriate in the circumstances? • If it is strictly necessary for LE purposes, state why and which condition in Schedule 8 is satisfied.	however existing practices and procedures are in place to manage this aspect. The examination would comply with SOP for Mobile Phone Kiosks and the standards set out during the certified kiosk training. Sensitive data would not be subject to any further or additional processing.
Q27	**DPA 2018** **2nd Principle** **Section 36**	**Specified/Explicit/Legitimate:** • State the specific purpose for which the personal/sensitive data will be processed. (Refer to guidance **Note 11**) • Is the data to be used for any other law enforcement purpose? If so what other law enforcement purpose? Is the data to be used for any non-law enforcement purpose? (Refer to guidance **Note 11**) If so: • What is that purpose? • Why do you believe that this purpose is not incompatible with the specific reason for which you gathered it?	The purpose for which personal data is collected on any occasion will be specified, explicit and legitimate, and personal data collected will not be processed in a manner that is incompatible with the purpose for which it is collected. However, data can be processed for any other law enforcement purpose PS (as the controller) is authorised by law to process the data for another purpose, and the processing is necessary and proportionate to that purpose. The purpose if to ascertain whether there is evidential value sufficient to prosecute or provide a report to COPFS.
Q28	**DPA 2018** **3rd Principle** **Section 37**	**Adequate/Relevant/Not excessive:** • What assessment has been made to ensure that the data being processed is adequate, relevant and not excessive in relation to what is necessary for the purpose for which they are processed?	We only process personal data we actually need for our specified purposes and we have sufficient personal data to properly fulfil those purposes. Given we only will triage there is no need to review the data we hold, nor do we require to delete data.
Q29	**DPA 2018** **4th Principle** **Section 38**	**Accurate/Kept up to date where necessary:**	
		• How will the accuracy of the data be checked?	The Mobile Device Kiosk will log that an examination has been undertaken but will not retain any personal data on the system. This audit log will be available to the system administrator for quality audits. We ensure the accuracy of any personal data we create and

			process, and we have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data.
		• What process will be in place to rectify/erase inaccurate data?	N\A
		• What process will be in place to keep it up to date (where necessary)?	N\A
		• How will you ensure that facts are distinguished from opinions? (see **Note 12**(1)) If this cannot be done, please explain why.	No personnel assessments will be undertaken - officers will assess what data is held relevant to the circumastances and and opinions will only be to the relevancy or that data.
		• How will you ensure that there will be a clear distinction between personal data relating to different categories of data subjects? If this cannot be done, please explain why. (see **Note 12**(2))	The Kiosk are able to make a clear distinction between personal data relating to different categories of data subject, such as: Suspects Witness Victim Unknown
		• How will you ensure that the requirements of Section 38(4) & (5) are met? (see **Note 12**(3))	Section 38(4) & (5) of the DPA requires that all reasonable steps must be taken to ensure that inaccurate, incomplete or out of date personal data is not transmitted or made available for any law enforcement purpose. Given that the Kiosk will only triage this will not have an impact on inaccurate or incomple/out of date data - it is a snapshot of what is held on the device.

Q30	**DPA 2018 5th Principle Section 39**	**Not kept longer than necessary:**	
		• How long will the personal data be retained?	No data will be held or extracted - this is a triage tool.
		• Is the personal data covered by the existing Police Scotland	No data will be held or extracted - this is a triage tool.

		Record Retention SOP? (Refer to guidance **Note 13**)	
		• The system must be able to have the data deleted. How will you ensure that the system will be able to delete the personal data when the retention period (defined as above) is met?	No data will be held or extracted - this is a triage tool.
		• Will the system require manual intervention or will deletion be automatic?	No data will be held or extracted - this is a triage tool.
		• If the data is required to be retained after the retention period, (e.g. for statistical purposes) how will it be anonymised?	No data will be held or extracted - this is a triage tool.
		• What processes will be in place to ensure the data is securely destroyed/deleted?	No data will be held or extracted - this is a triage tool.
Q31	**DPA 2018 6th Principle Section 40**	**Secure:** • How will the personal data be secured and kept safe? • What technical/operational security features and/or policies will be in place to protect the personal data?	No data will be held or extracted - this is a triage tool. Users can refer to Police Service of Scotland Mobile Phone Kiosks – Purpose and Use SOP which will provide guidance. No physical extraction will be possible for officers - Kiosks are only used to identify whether a device has evidential value and therafter (if so) it will be progressed by Cybercrime.

Part 4 – Measures Contributing to the Rights of the Data Subjects

In this section, assess how data subjects' rights will be protected.

Q32	**DPA 2018 Section 44**	**Information – Controller's general duties:** (Refer to guidance **Note 14**) • How will data subjects be made aware of what is happening to their data?	The Police Scotland website will provide an explanation informing the public how the kiosk will operate regarding the triage examination process.

		• Is it the intention to withhold any of the information listed under the exemptions? • If so, how do you propose to record your decisions?	
Q33	**DPA 2018 Section 45**	**Subject Access Requests:** (Refer to guidance **Note 15**) • How will you ensure that the information will be available to Information Management for the processing of subject access requests?	No data will be held or extracted - this is a triage tool.
Q34	**DPA 2018 Sections 46, 47 & 48**	**Right to Rectification:** (Refer to guidance **Note 16**) • What processes will be in place to manage requests for rectification? • What process will be in place to notify any recipients of the personal data that is/was inaccurate data? • What guidance will be in place to deal with the requirements under Section 48?	No data will be held or extracted - this is a triage tool.
Q35	**DPA 2018 Section 47 & 48**	**Right to erasure or restriction of processing** (Refer to guidance **Note 17**) • The system being designed must be able to allow erasure of data. What processes will be in place to manage requests for erasure? • What process will be in place to notify any recipients of the personal data that it has now been erased?	No data will be held or extracted - this is a triage tool.

Q36	**DPA 2018 Section 62**	**Logging:** (Refer to guidance **Note 18**) Confirm that the system you are proposing will meet the requirements of Section 62, and the requirement to be auditable, and how you will ensure this. Every effort must be made to ensure the logs record the identity of the following :	Cybercrime audit log of the Mobile Phone Kiosk are user defined and will record who are the users of the system and will dictate who can access data. Any anomalies can be recorded on the CMS system to reflect any discrepancies in the process. A regular audit will be collated displaying unique reference number for every triage.

		• the person who accessed the personal data and/or • the person who disclosed the data and/or • the recipients(s) of the data, however, if it is not possible, then the reason for this must be documented.	
Q37	**DPA 2018 Section 66**	**Security of processing:**	
		• Will the data be encrypted?	No data will be extracted - only visually assessed via the Kiosk.
		• Will the data be pseudonymised? If so how?	No
		• How will the data be protected against risk of loss, confidentiality, availability and integrity?	No data will be extracted.
		• Will back-ups be taken? If so, when/how often?	No
		• Will the security of the system be required to have any formal accreditation or independent certification (e.g. ISO27001)?	Each kiosk will have will have licenced dongles and password user access.
		• What processes will be in place to determine who will have access to the data/system?	Centrally administered: administration will create user accounts and passwords and Sy Ops Documentation. There will only be specified police officer users, appropriately vetted and trained. This will be centrally goverened by Cybercrime
		• What level of security clearance will be required to access the system/data?	MV

		• What data protection/security training will users of the data/system be required to have?	Successful completion of Certified training Course
		• How will access to the system be granted?	Administration will create user accounts and passwords and Sy Ops Documentation
		• What information asset register and/or risk register will the data be recorded on?	No data retained on System. Cybercrime CMS will record what actions have been taken.

		• Will you have a SyOps/Procedure manual/SOP, etc. to detail the above?	Yes
Q38	**Consultation**	**Consultation Requirements:** (Refer to guidance **Note 19**)../../../../../../personal_data_east/Personal/1497510/Cybercrime Forensics 2012 to May 2018/Cyber Uplift PROJECTS Aug 2017/Kiosks/Data Protection Impact Assessment - Law Enforcement Processing - Guidance.doc - _Hlk507408266	Scottish Government: Scottish Executive Cyber Resilience team and a representative from the ICO have been consulted at length as have HMIC, Police Federation, UNISON, SPA and COPFS and a demonstration of the Kiosk by senior management was delivered at Victoria Quay.
Q39	**DPA 2018 Sections 72 to 78**	**Data Transfers Outwith the UK:** (Refer to guidance **Note 20**) • Will the data be held or transferred to a third country (i.e. outwith the EU)? • If yes, for what purpose, and to where will it be held or transferred? • If yes, what processes will be place to ensure it is adequately protected? • Will the data be held or transferred to another country inside the EU? • If yes – for what purpose and to where will it be held or transferred?	No

Part 5 – Other privacy legislation and policies

In this section, assess the other rights that data subjects have. This helps balance the final risk assessment.

Q40	**RIPSA 2000/RIP(S)A 2000**	Does the project involve the use of powers within the RIPA 2000 or RIP(S) A 2000? If so, detail the relevant parts of the legislation.	No
Q41	**Human Rights Act 1998**	**Article 2: Right to Life**	No

		Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to life, subject to any limitations as may be defined in Article 2(2)? For the avoidance of any doubt, the limited circumstances are that in peacetime, a public authority may not cause death unless the death results from force used as follows: • Self-defence or defence of another person from unlawful violence; • Arresting of someone or the prevention of escape from lawful detention; and • A lawful act to quell a riot or insurrection.	
Q42		**Article 3: Prohibition of Torture** Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to be not subjected to torture or inhuman or degrading treatment? For the avoidance of doubt, this is an absolute right.	No

Part 5 – continued

Q43		**Article 4: Prohibition of Slavery or Forced Labour** Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to be not held in servitude or forced to perform compulsory labour? For the avoidance of doubt, this is an absolute right; the following are excluded from being defined as forced or compulsory labour: • Work done in ordinary course of a prison or community sentence;	No

		• Military service; • Community service in a public emergency; and normal civic obligations	
Q44		**Article 5: Right to Liberty and Security** Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to be not deprived of their liberty subject to certain limitations? For avoidance of doubt, the following limitations apply when a person is: • Held in lawful detention after conviction by a competent court; • Lawfully arrested or detained for non-compliance with a lawful court order or the fulfilment of any lawful obligation; • Lawfully arrested or detained to effect the appearance of the person before a competent legal authority; • Lawfully detained to prevent the spreading of infectious diseases; • Lawfully detained for personal safety (applies to persons of unsound mind, drug addicts etc.); and • Lawfully detained to prevent unlawful entry into the country or lawful deportation from the country.	No
Q45		**Article 6: Right to a Fair Trial** Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to have a public hearing within a reasonable time by an independent and impartial tribunal established by law? For the avoidance of doubt, the hearings included are both civil and criminal proceedings that are not	No

		specifically classified as hearings that must be heard 'in camera', i.e. closed to the public.	
Q46		**Article 7: Right to no Punishment without Law** Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to not be prosecuted for a crime that was not, at the alleged time of commission, constitute a criminal offence under national or international law? For the avoidance of doubt, this is an absolute right.	No
Q47		**Article 8: Right to Respect for Private and Family Life** Does the project involve new or existing data processing that adversely impacts an individual's right to respect for privacy in terms of their private and family life (subject to certain qualifications)? For the avoidance of doubt, the qualifications are: • Legal compliance; • National security; • Public safety; • National Economy; • Prevention of crime and disorder; • Protection of public health and morals; • Protection of rights and freedom of others.	Yes - As per any enquiry or investigation involving digital media there is an element of collateral intrusion. This will be managed using current and established Policy, Procedures and Practices.
Q48		**Article 9: Right to Freedom of Thought, Conscience and Religion** Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to freedom of thought, conscience and religion subject to certain qualifications? For the avoidance of doubt, the qualifications are: • Unless prescribed by law; • In interest of public safety;	No

		• Protection of public order, rights or morals; • Protection of rights and freedoms of others.	
Q49		**Article 10: Right to Free Expression** Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to hold opinions and express their views singly or in dialogue subject to certain qualifications? For the avoidance of doubt, the qualifications are set out in Article 9 above.	No
Q50		**Article 11:Right Freedom of Assembly and Association** Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to freedom of peaceful assembly and association with others subject to certain qualifications? For avoidance of doubt, the qualifications are set out in Article 9 above.	No
Q51		**Article 12: Right to Marry** Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to marry and found a family subject to certain restrictions? For the avoidance of doubt, the restrictions are regulated by law so long as they do not effectively take away the right , e.g. age restrictions apply	No
Q52		**Article 14: Right to Freedom from Discrimination** Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to be treated in a manner that does not discriminate the individual from others subject to certain restrictions?	No

		For the avoidance of doubt, this right is restricted to the conventions as set out in the European Convention of Human Rights 1950; the grounds for discrimination can be based on: • Sex • Race • Colour • Language • Religion • Political persuasion • Nationality or social origin • Birth • Other status	

Part 6 – Risks to the rights and freedoms of data subjects of the proposed processing

In this section, using the information you have gathered so far in the DPIA, complete a final risk assessment (Refer to guidance **Note 21**)

Risk(s) identified to the rights and freedoms of data subjects	**Likelihood and severity score**	**Mitigation(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Unlawful, access,modification or deletion of data		**- Certified Training** **- Mobile Phone Kiosk SOP** **- Audit Function** **-Central Governance** **- View Only (Unable to Extract data)** **- Compliance Check** **- Specified Users**	**Reduced**	

Once the DPIA has been completed in full, it must be referred to IM to check for completion. Please forward to the Information Assurance or ISO mailbox. Once approved, it will be returned signed by the DPO.

Part 7 – Approval

Data Protection Officer:
Signature:

Date:

Strategic Information Asset Owner:

Signature:

Date: