Justice Sub-Committee on Policing

Police Scotland's proposed use of digital device triage systems (cyber-kiosks)

Supplementary written submission from Police Scotland

The **draft** Data Protection Impact Assessment (DPIA) and the **draft** Equality and Human Rights Impact Assessment (EqHRIA) were developed in conjunction with Force Information Assurance and the Safer Communities Equality and Diversity Advisor. The attached draft versions of these documents are those which were circulated to the established groups on 23 October 2018, namely:

Stakeholders Group
Crown Office & Procurator Fiscals Service
Her Majesty's Inspectorate of Constabulary in Scotland
Information Management
Scottish Police Authority
Scottish Police Authority Forensic Services
Scottish Police Federation
Staff Association

External Reference Group
Aamer Anwar
Academia
Information Commissioner's Office
National Independent Strategic Advisory Group
Open Rights Group
Privacy International
Scottish Human Rights Commission
Scottish Institute for Policing Research

The document sets were discussed at the respective meetings of both groups on 30 October 2018 as outlined in previous submission to the Justice Sub Committee. They were described at that time as being at an advanced stage and sufficiently progressed to support training. On 2 November 2018 the respective representatives from Scottish Human Rights Commission, Privacy International, Open Rights Group and the Information Commissioner's Office were contacted via email in which it was once again outlined, with specific reference to the EqHRIA and DPIA, that feedback and other considerations continue to be welcomed prior to any redrafting of the documents.

In conjunction with due considerations as regards the legal basis for use, this feedback if/when received, combined with the findings of the initial training, will form the basis of what is expected to be one of the final drafts of the documents sets.

Police Scotland
14 November 2018

Data Protection Impact Assessment – Cyber Kiosks

Law Enforcement Processing only

Control Sheet

Title	Cyber Kiosks
Date Approved	
Version Number	0.12
Document Type	Data Protection Impact Assessment
Document Status	DRAFT
Author	Cybercrime Forensic Coordinator Michael Dickson / DI Michael McCullagh, Cybercrime Capability Programme.
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
0.2	03/07/18	Process Map added
0.3	16/07/18	IA revisions added
0.4	24/07/18	Updated per IA queries
0.5	02/08/18	IA revisions added
0.6	29/08/18	Audit detail updated
0.7	29/08/18	IA revisions added
0.8	06/09/18	Updated per IA queries
0.9	13/09/18	IA revisions added
0.10	09/10/18	Updated following IA / Project Meeting
0.11	12/10/18	Final draft for consulation
0.12	12/10/18	Human Rights updated by Author

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' spread across Police Scotland Estate 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. A Cyber Kiosk is a computer terminal that can view data on a device in a targeted and focused way i.e. only looking at what is necessary. If unsure as to whether a device holds information relevant to an investigation it may undergo a triage process using a Cyber Kiosk. This process is only performed by trained staff, the purpose of which is to identify if the mobile phone or device contains any evidential data using, where appropriate, selected parameters, e.g. text messages. If no potential evidence is found it will be returned to the owner. The Kiosk only provides a viewing facility. It does not record any data from the mobile phone / device. 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 for mobile devices. Seized mobile devices will include those of victims, witnesses, suspects or accused

		persons including those obtained under common law powers, the authority of a judicial warrant or statutory power. All such devices are treated as productions by Police Scotland and are handled in accordance with the Productions SOP and subject to associated retention Policies. Cyber Kiosks are operated by specially trained officers (in the region of 410 officers c. 10 per kiosk machine for resilience) with the ability to triage lawfully seized devices, reducing the number which are required to be forensically examined within Cybercrime Hubs, and reducing the inconvenience to a witness, victims and suspects or accused persons of retaining a device which, on later examination, has no evidential value. It will only be used in cases where the evidential relevance of the device is unknown. If it is known that the device contains potential evidence that device will be submitted without triage within existing processes. No device data is retained by the kiosk machine. The equipment has the capacity to copy data however this facility is disabled and cannot be enabled by standard operators. It is possible that Police Scotland may review use of the extraction functions in future however there is no intention to do so at this time. Any change in the functionality of the device to be anything other than 'view only' will require a resubmission of an associated DPIA. The Kiosk has the capability to examine other items such as USBs or SD cards however the facility to examine anything other than a Mobile Phone or Tablet has been disabled. Any change in the functionality of the device to include other items will require a resubmission of an associated DPIA.
Q4	Detail the benefits of the project to Police Scotland.	Growth of cybercrime and the digital devices involved in or containing evidence relevant to police investigations has grown exponentially and continues to do so. Currently every device goes to a cybercrime hub for download to allow for both assessment of the information within and capture of evidence. In light of this Kiosks provide: Improved service to frontline officers in establishing the relevance of a device to an investigation and the identification of evidence resulting in more timely detections and

		investigations. Fewer devices being submitted to Cybercrime Hubs meaning only devices of evidential worth are submitted meaning swifter evidence identification and criminal justice process preventing and detecting crime, harm and disorder allowing hubs to focus and prioritise activity and evidence recovery. Resource saving as such a device being returned to the owner post triage means no copying of the data within a device as is currently required to facilitate an assessment of each device seized and therefore no data storage and transfer implications
Q5	Detail the benefits of the project to any other relevant parties.	The return of devices to owners where the triage has allowed an assessment that the device does not contain potential evidence. Such a device returned to the owner post triage means no copying of the data within a device as is currently required to facilitate an assessment of each device seized. Triage in a more focused manner than current processes allow, focused investigation in the relevant areas of the device for example text messages meaning less intrusion of privacy. Due to the reduced strain on hubs ,Criminal Justice partners receive a faster and improved quality of service with regard evidential requests.
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 Data including name, identification numbers, location data, online identifiers and factors specific to physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
Q8	What sensitive data if any, is to be processed? State the categories. (Refer to guidance **Note**	In general terms any data that is held on a device. Mobile data / internet connection will be disabled via SIM removal at point of seizure and confirmed as disconnected /

	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	removed by the operator to ensure only data on the device can be seen. There will be no access to the internet / cloud. The data may include anything which can be held on the device and may include, or from which the following may be inferred; 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 using new technologies to Police Scotland This process is an additional facility within the existing digital forensic examination process currently undertaken in and across Police Scotland.
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. The Kiosks design has been restricted to provide only a viewing facility. It cannot change, delete or otherwise manipulate or use the data within the device. Only the Police Scotland officers viewing the kiosk at the time can view the data. The manufacturer cannot access the kiosk or data. Once the triage is complete only management information such as operator, date, reference number, start time, end time, etc is retained, can be viewed and will be subject of audit and assurance processes. It allows triage in a more focused manner than current processes allow, focused investigation in the relevant areas of the device, for example text messages, means less intrusion of privacy. It will only be used in cases where the evidential relevance of the device is unknown. If

		it is known that the device contains potential evidence that device will be submitted without triage within existing processes. 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 / review of data. No device data will be kept or saved. The Kiosks do not have the ability to delete any data from the device.
Q11	Explain the context in which the processing will take place (Refer to guidance **Note 4**)	The devices will be situated within designated rooms within Police Scotland estate (police offices). Kiosks will only be used in cases where the evidential relevance of the device is unknown. If it is known that the device contains potential evidence that device will be submitted to the Cybercrime hub without triage, within existing processes. The Kiosks are password protected for use, only trained authorised officers will undertake the triage via the Kiosks, these officers will subject to audit and compliance checks to ensure adherence with prescribed guidelines. Only productions will be subject to triage. A production is an article, document or other thing which has been seized by the police as it is believed to potentially be relevant in some way to a police investigation or incident. The police are entitled at common law to seize anything it is believed to potentially be connected in some way to a police investigation or incident. This power of seizure applies to both common law and statutory offences even although the statute contravened makes no provision for seizure. All seizures must be for a policing purpose and includes devices seized during execution of a search warrant or under legislative provision. These powers form the legislative framework under which digital devices are seized and by default the data within and any subsequent examination. Devices should be sent directly to the Cybercrime Unit, without kiosk examination, when: • The device does not work and is thought to be critical to the enquiry

		• The password for the device cannot be overcome (after consultation with cybercrime) • The case involves child abuse images or other disturbing material • The investigation relates to a potential Professional Standards Department or Anti-Corruption Unit enquiry including Police Scotland, COPFS, SPS etc. • The data is known to be on the device (e.g. a witness can speak to recording something on the device) • The data extraction is extremely large and cannot be managed on a kiosk Examination must be; Necessary – This means that the action taken is necessary to achieve the objective of the digital investigation of that device. If an action is not necessary the intrusion can therefore not be justified and the action should not be taken. Proportionate – This means that the officer has considered the intrusion that their activity will involve and with due regard to the implications in terms of respect for private and family life. The officer must be content that any / further interrogation of data is proportionate under the circumstance / needs of the investigation. Relevant – This means that the data which the officer seeks to review is only the data relevant or potentially relevant to the investigation. If the data held is not potentially relevant it should not be reviewed. Legitimate Aim - Acting with a legitimate aim, for a policing purpose with the associated reasonable belief as outlined are the grounds on which the power of seizure described above is based. It is only with this legitimate aim that an officer should seize and subsequently review a device.
Q12	Describe the purpose of the processing (Refer to guidance **Note 5**)	All seizure and Triage using Kiosks will be strictly only for a policing purpose, in accordance with training and the associated 'Principles of Use'. Kiosks will only be used in cases where the evidential relevance of the device is unknown. If it is known that the device contains potential evidence that device will be submitted to the

		cybercrime hub without triage, within currently existing processes. It is anticipated the roll out of this facility will greatly reduce the unnecessary retention and copy of devices within Police Scotland Cyberhubs and reduce submission to hubs overall by between 80 and 90%. Benefit to Police Growth of cybercrime and the digital devices involved in or containing evidence relevant to police investigations has grown exponentially and continues to do so. Currently every device goes to a cybercrime hub to allow for both assessment of the information within and capture of evidence. In light of this, Kiosks provide: Improved service to frontline officers in establishing the relevance of a device to an investigation and the identification of evidence resulting in more timely detections and investigations. Fewer devices being submitted to Cybercrime Hubs meaning only devises of evidential worth are submitted meaning swifter evidence identification and criminal justice process preventing and detecting crime, harm and disorder allowing hubs to focus and prioritise activity and evidence recovery. Resource saving as such a device being returned to the owner post triage means no copying of the data within a device as is currently required to facilitate an assessment of each device seize and therefore no data storage and transfer implications Benefit to others The return of devices to owners where the triage has allowed an assessment that the device does not contain potential evidence. Such a device returned to the owner post triage means no copying of the data within a device as is currently required to facilitate an assessment of each device seized.

		Triage in a more focused manner than current processes allow, focused investigation in the relevant areas of the device for example text messages, meaning less intrusion of privacy. Due to the reduced strain on hubs, Criminal Justice partners receive a faster and improved quality of service with regard evidential requests.
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 otherwise quantifiable. For example, one device may have data concerning a number of individuals. As digital devices in particular mobile phones are used across all demographics of the population there will be no disproportionate impact on any particular community. Nonetheless, in a typical year we are likely to see approximately 10,000 mobile devices subject to Triage
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 – The data is not already held by Police Scotland.
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	High Risk Processing. The prevalence of Mobile phone / device use within the communities we police means processing will be on a large scale given the number of devise in use by the public. The capacity of devices is such that they can hold significant amounts of data. The Kiosk Capability will be nationally available to Officers. Whilst the devices examined are lawfully obtained and processed, the potential for a large number of individuals to have their data accessed either directly or indirectly (for example as a consequence of their data being held on the device of another person which is obtained and triaged using a kiosk machine) is significant. Whilst an examination will only be undertaken in association with the investigation of

	guidance **Note 6**)	an incident/crime/event, for a policing purpose and within existing legal frameworks it is possible that much of the data on a device may not be relevant to the investigation, but may be assessed during triage and if irrelevant will be disregarded. Kiosk processing allows for mitigation of collateral intrusion by selecting only the areas of interest where these are known for example 'text messages'. There is no combining of datasets. Given the scale of device ownership, vulnerable data subjects will be within the demographic of population affected. The legislative framework, training and requirement of a 'policing purpose' protect those vulnerabilities.

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**)	In general terms any data that is held on a device. Mobile data / internet connection will be disabled via SIM removal at point of seizure and confirmed as disconnected / removed by the operator to ensure only data on the device can be seen. There will be no access to the internet / cloud. The data may include anything which can be held on the device and may include, or from which the following may be inferred; 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.
Q18	What, if any processing of sensitive data will be carried out and why? (Refer to guidance **Note 1**)	Processing will potentially include all sensitive data; In general terms any data that is held on a device. Mobile data / internet connection will be disabled via SIM removal at point of seizure and confirmed as disconnected / removed by the operator to ensure only data on the device can be seen. There will be no access to the internet / cloud. The data may include anything which can be held on the device and may include, or from which the following may be inferred; 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. . Process types will potentially include – Retrieving / Consulting Using – as Evidence or intelligence Disclosing or otherwise making available - for example by including identified relevant evidential data as evidence thereafter submitted to Crown as part of a case, or using that data during an interview of a suspect. Sensitive data will be a potential by-product of the triage process when the objective is to identify if the device contains any data relevant to the enquiry (some of which may be sensitive data). Kiosks have the functionality to assess data in a manner that minimises intrusion for example from a specified date range, when a crime was perpetrated or data type for example text messages. During the triage process, any data or sensitive data which is not relevant to the case

		under investigation will be disregarded.
Q19	What is the source of the personal/sensitive data?	The source of the data will be the device to be triaged via the Cyber Kiosk - this will be recorded 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**)	Identifiable – Personal / Sensitive data will be fully identifiable Pseudonymised – No - There will be no adaptation, alteration, reorganisation, deletion or destruction of data Anonymised - No - There will be no adaptation, alteration, reorganisation, deletion or destruction of data

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	No. No other organisation (including the manufacturer) will process in any way / view any of the data or devices subject to triage.

	• the exact role of the other organisation in the processing of the data?	
Q22	In relation to the proposed processing, what is the status of: a) Police Scotland b) the other organisation? (Refer to guidance **Note 8**)	A) - Police Scotland (Chief Constable) will be the Controller B) – Not applicable – No other organisation involved in processing.
Q23	What training will be provided for individuals: • Within Police Scotland • Partners • Contractors/subcontractors	All users of the Mobile Phone Kiosk will required to be 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 (PSoS), Cybercrime Kiosk Toolkit, PSoS – Digital Forensics, Principles of Use DPIA, EqHRIA Cellebrite – Kiosk User Manual.
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.	No - not consent based.- Whilst there will be occasions when a witness / member of the public provides their device to assist in a police investigation the taking possession of the device by the police is by means of seizure. There may be consent on behalf of the devise owner at that time however by virtue of the fact that device is seized and may not be returned to them if it is requested, consent is not required to access the data. The processing is strictly necessary and is for the purpose of identifying potential evidence to facilitate the subsequent (unrelated to kiosk) capture of that evidence within a Cybercrime forensic hub. The kiosk provides a means of viewing device content in a controlled auditable manner (as opposed to manual device examination). Given the data is digital and stored in the device, access and the processing involved is the only means by which the data can be viewed. There is no other way to access the data other than using the device within which it is held to do so. The kiosk review functionality is bespoke in terms of its potential to focus in areas in which relevant data may be stored for example text messages or within a date range which allows reduced impact in terms of amount of data viewed, and therefore reduced infringement regards rights and freedoms. The processing is necessary under the Police Fire & Reform (Scotland) Act 2012 – Section (20) Constables: general duties-

			(1)It is the duty of a constable— (a)to prevent and detect crime, (b)to maintain order, (c)to protect life and property, (d)to take such lawful measures, and make such reports to the appropriate prosecutor, as may be needed to bring offenders with all due speed to justice, Section (32) Policing principles: The policing principles are- (a)that the main purpose of policing is to improve the safety and well-being of persons, localities and communities in Scotland, and (b)that the Police Service, working in collaboration with others where appropriate, should seek to achieve that main purpose by policing in a way which— (i)is accessible to, and engaged with, local communities, and (ii)promotes measures to prevent crime, harm and disorder. Under the Act, the 1st principle and requirement that data will be processed for law enforcement purposes and will be lawful and fair. The legal framework for seizure, identification of and use of evidence within digital devices is established within common law, statute or by virtue of a warrant. This use of kiosk does not change this legal framework in any way. Under Schedule 8, the processing of data meets a number of conditions in particular;

			1(a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, namely the powers of a police constable in the execution of their duty. 1(b) is necessary for reasons of substantial public interest, namely the public interest regard the prevention, detection of crime and the bringing of offenders to justice. 2 Administration of justice, for example the capture of relevant evidence 3 Protecting individual's vital interests such as right to life, prohibition of torture, prohibition of slavery and forced labour, right to liberty and security and fair trial. 4 Safeguarding of children and of individuals at risk, in particular communications data used in furtherance of criminal conduct such as child sexual exploitation or human trafficking.
		Sensitive Processing: (Refer to **Note 1** and **Note 10**) • Does the processing involve processing of sensitive data? • 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.	Yes. Processing involves the processing of sensitive data and potentially all forms of sensitive data including 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. No Processing is not consent based.

			Under Schedule 8, the processing of data meets a number of conditions in particular; 1(a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, namely the powers of a police constable in the execution of their duty. 1(b) is necessary for reasons of substantial public interest, namely the public interest regard the prevention, detection of crime and the bringing of offenders to justice. 2 Administration of justice, for example the capture of relevant evidence 3 Protecting individual's vital interests such as right to life, prohibition of torture, prohibition of slavery and forced labour, right to liberty and security and fair trial. 4 Safeguarding of children and of individuals at risk, in particular communications data used in furtherance of criminal conduct such as child sexual exploitation or human trafficking.
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	Cyber Kiosk triage is for the prevention, investigation, or detection of crime or the prosecution of offenders. The processing of data will only be for LE purposes. The purpose of processing is to ascertain whether there is evidential data of value sufficient to prosecute or provide ultimately (via Cybercrime Hub) a report to COPFS for that purpose. Triage of devices will be necessary and proportionate

		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?	and relevant and will only serve a policing purpose. A secondary LE purpose may involve the use of Kiosk to review data within a device where there is a concern for life such as high risk missing persons the result of which may not result in viewed data being used as evidence in any criminal process. Triage will not process this for non LE purposes.
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?	Police Scotland will only triage devices (and thereby process the data thereon) that are seized lawfully and where it is necessary for the investigation of a crime/incident. The 'Digital Forensic Principle of Use' guides officers in relation to what is adequate, relevant and not excessive and outline the following; Officer's balance of investigative needs versus the public expectation of privacy must be met by doing what is lawful, ethical and in good faith and no more than is necessary and proportionate to achieve the lawful objective sought. Fairness, integrity and respect of property and right to privacy outlined within Article 8 (ECHR) above are the key principles which guide all officers in the execution of duty. These principles are requirements for the use of Police Scotland technical ability including the examination of devices. It is the responsibility of all officers and staff at all stages of the investigative and examination process associated with digital device examination to ensure that they were possible review only what is relevant to the investigation and consider, comply and act in accordance with the law and these principles all at times. Police Scotland will only process personal data for the specified purposes. However the triage process may involve the processing of non-relevant data in order to

			disregard it, even with the application of training and use of search parameters on certain devices. Evidence of suspected criminality unrelated to the scope of the investigation will not be deliberately sought out. However if such information is found, officers must consider this in conjunctions with the obligations imposed by their duty.
Q29	**DPA 2018 4th Principle Section 38**	**Accurate/Kept up to date where necessary:**	
		• How will the accuracy of the data be checked?	During triage no accuracy issues will be applicable in relation to device data - it is only an assessment of the device data. The Kiosk software provides a viewing facility with regard the data held on that device. It is not within the software's capability to alter or delete the data in any way therefore there is no potential compromise to accuracy. There are validation processes undertaken by the kiosk manufacturers to ensure the accuracy of their devices. Management Information (MI), Kiosk Use - The Kiosk will log that an examination has been undertaken and what the results were (positive/negative, passed to Cybercrime and times and dates etc.) This audit log will be available to the system administrator (Cybercrime) for quality audits and to ensure all devices are being processed in accordance with agreed processes and that it is being assessed and triaged appropriately, including the accuracy of what is being recorded in that MI log. Police Scotland will rectify inaccurate data when it becomes apparent, or, if an individual Kiosk Operator requests it. If personal data of an operator is identified as inaccurate as a matter of fact, or incomplete, Police Scotland will seek to amend this by rectifying or

			completing the data. This will be logged The use of the system will be audited. Kiosks produce logs which show the times of extractions, the ID of the person doing the extraction, when the extraction occurred, the name of the device being extracted and the case reference number from our Case Management system. These logs are stored on the kiosk itself and are not accessible by operators. Cybercrime staff will periodically visit the kiosks to provide updates, etc. At this time, using enhanced credentials, they will log into the kiosk and recover these logs. The logs will be aggregated at Newbridge and viewed on a Central Management System. They will be used for training and business purposes, but also for audit purposes. A dip sample (volume to be confirmed once level of use of the kiosks is better understood) will be taken of examinations from the logs. This will be compared against the case management system to ensure that the examination was authorised, that it was proportionate to the case and that the device was provided legally. If the examination fails on any of these points then the appropriate action will be taken, whether that is by remedial training or by disciplinary process.
		• What process will be in place to rectify/erase inaccurate data?	During triage no accuracy issues will be applicable in relation to device data - it is only an assessment of the device data. The Kiosk software provides a viewing facility with regard the data held on that device. It is not within the software's capability to alter or delete the data in any way therefore there is no potential compromise to accuracy. Were an issue is identified with regard user data which is input by cybercrime unit or kiosk operator Police

			Scotland will rectify inaccurate data when it becomes apparent, or, if an individual Kiosk Operator requests it. If personal data of an operator is identified as inaccurate as a matter of fact, or incomplete, Police Scotland will seek to amend this by rectifying or completing the data. This will be logged.
		• What process will be in place to keep it up to date (where necessary)?	During triage no accuracy issues will be applicable in relation to device data - it is only an assessment of the device data. The Kiosk software provides a viewing facility with regard the data held on that device. It is not within the software's capability to alter or delete the data in any way therefore there is no potential compromise to accuracy. The only data kept up to date is the MI data produced as outlined above. This is an automated facility of the kiosk.
		• How will you ensure that facts are distinguished from opinions? (see **Note 12**(1)) If this cannot be done, please explain why.	Officers will only assess data in terms of its evidential relevance. The only opinion will be as to whether the data is considered evidential and will be the decision of the officers reviewing. The facts pertinent to that data are a matter for the court.
		• 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))	Prior to carrying out the assessment, a record of what is to be done is recorded by the Kiosk software. For each device that is to be assessed, the operator must fill in a field to define the category of data subject. The Kiosks are able to make a clear distinction between personal data held on devices lawfully obtained from 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, incomplete or out of date data - it is a snapshot of what is held on the device. The assessment of quality, accuracy completeness or date is not relevant in this circumstance. There is no data transmission.
Q30	**DPA 2018 5th Principle Section 39**	**Not kept longer than necessary:**	
		• How long will the personal data be retained?	No data will be saved from mobile devices as a result of their examination - this is a triage tool. The audit data, i.e. the record of what device was assessed, when, why and by whom etc. will be retained in line with all Audit and Assurance records and the Record Retention SOP; Transaction Validations – 2 years Full Audit Paperwork - Current year + 3 Final Audit report – 6 years Internal audits of service systems may be retained for a shorter period.

			The audit data does contain personal data that will identify the person conducting the examination, as well as the name of the reporting officer and the case reference number. The audit data is inaccessible to Kiosk operators due to permissions on their accounts preventing them from having access to it. This data will be extracted by Cybercrime staff using encrypted devices, raised from the Kiosk, and taken back to Cybercrime for processing on a standalone central management system for assessing training needs, Kiosk use, operator issues, etc. Once transferred to this system the data will be removed from the encrypted USB device. Once removed the data will be deleted form the kiosk and thereafter only held centrally The cloned SIMS do not hold any personal data whatsoever. They only hold two numbers - the original SIM's ICCID and its IMSI. This is to convince the handset that it has its original SIM card still within it to allow it to be used without connecting to a network. The data on a cloned SIM is completely (and automatically) overwritten on every use.
		• Is the personal data covered by the existing Police Scotland Record Retention SOP? (Refer to guidance **Note 13**)	No data will be held or extracted - this is a triage tool. The audit data will be retained in line with the Record Retention SOP.
		• 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. Audit data logged on each Kiosk will be extracted by Cybercrime staff onto encrypted USB pen drives and transported to Cybercrime where they will be collated onto a standalone system which will process this data to determine patterns of use and identify training needs etc. In doing this, the audit logs will be securely

			deleted from the individual Kiosks.
		• Will the system require manual intervention or will deletion be automatic?	No data will be held or extracted - this is a triage tool. The audit data will be retained in line with the record and manually deleted.
		• If the data is required to be retained after the retention period, (e.g. for statistical purposes) how will it be anonymised?	Not applicable
		• 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. Audit data will be electronically deleted centrally at Cybercrime.
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 saved from mobile devices as a result of their examination - this is a triage tool. We will not retain or hold any device data on the Kiosk and therefore this is no security implication. Kiosk are situated in rooms in police Scotland estate. Only investigating officers and kiosk operators will be present during a device triage. Any Data taken in the form of contemporaneous notes will be lodged as a production for evidential purposes and therefore subject to record retention policy. Kiosks are standalone systems that are not connected to any network. Data cannot be egressed from them due to restrictions placed on the controlling software. Kiosk operation is password protected with each operator having an individual log on. Triage will be guided by 'Digital Forensic Examination Principles of Use' and the processes outlined in Guidance 'Toolkit'. 'Cloned' SIM cards used to access some mobile devices are only written with the IMSI and ICCID

			relating to the original SIM found within the device. No other data is written to them. They are wiped prior to every use. While data is being assessed by trained officers it will be visible on screen. Officers will be instructed to 'lock' the Kiosk at any time that they are called away from an examination to prevent unauthorised access to the Kiosk and to the data extracted from the current mobile device. Audit data logged on each Kiosk will be extracted by Cybercrime staff onto encrypted USB pen drives and transported to Cybercrime where they will be collated onto a standalone system which will process this data to determine patterns of use and identify training needs etc. In doing this, the audit logs will be securely deleted from the individual Kiosks.

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	A public information document has been drafted and will be made available to all persons from whom a digital device is seized. This will provide information on

		happening to their data? • Is it the intention to withhold any of the information listed under the exemptions? • If so, how do you propose to record your decisions?	the Kiosk and general digital device forensics. This advice will be published on the force internet and intranet. No data will be saved from mobile devices as a result of their examination - this is a triage tool. We will not retain or hold any device data on the Kiosk and therefore there is no security implication. Any Data taken in the form of contemporaneous notes will be lodged as a production for evidential purposes and therefore subject to record retention policy. Current year + 6 years from the date made known to the police or the date in which the matter was reported to the relevant prosecuting authority for standard cases (resolved and unresolved). Yearly reassessment thereafter Current year + 12 years from the date made known to the police or the date in which the matter was reported to the relevant prosecuting authority for serious resolved cases. Yearly reassessment thereafter. Not disposed of for serious unresolved cases. Intention to withhold – Because no device data is held or retained on the device this is not applicable Recording of decisions - Records Management retain all FOI and the associated management thereof. Management information data is produced by the kiosk and will be managed as outlined at question 29. It is the intention that this will be published.

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 saved / stored from mobile devices as a result of their examination - this is a triage/ viewing tool. As explained above, the Mobile Device Kiosk will log that an examination has been undertaken and what the results were (positive/negative, passed to Cybercrime and times and dates etc.) This audit log will be available to the system administrator (Cybercrime) for quality audits and to ensure all devices are being processed in accordance with agreed processes and that it is being assessed and triaged appropriately including the accuracy of what is being recorded in the log. Any data taken in the form of contemporaneous notes will be lodged as a production, for evidential purposes and therefore subject to record retention policy Audit data logged on each Kiosk will be extracted by Cybercrime staff onto encrypted USB pen drives and transported to Cybercrime where they will be collated onto a standalone system which will process this data to determine patterns of use and identify training needs etc. In doing this, the audit logs will be securely deleted from the individual Kiosks. This audit / management information will be held in accordance with record retention policy and available to information management when required If a request for information is received Cybercrime can provide for any relevant data that may be held in relation to audit. The GDPR and the Data Protection Act 2018

			strengthen the rights of individuals, as data subjects, in relation to the personal data that Police Scotland holds about them. If an individual wishes to exercise this right, Article 15 of the General Data Protection Regulation and section 45 of the Data Protection Act 2018 provide a right of access to the information Police Scotland holds about them. Individuals can submit a subject access request by emailing: dataprotectionsubjectaccess@scotland.pnn.police.uk Cybercrime will work with Information Management, who process such requests as a statutory obligation, and respond accordingly subject to certain restrictions. For example, restricting individuals rights may be necessary to protect the rights and freedoms of third parties or to avoid prejudicing the prevention and detection of criminal offences. Police Scotland publishes a Privacy Notice on its website that outlines why we process data and our legal basis for doing so for Law Enforcement Purposes. The enhanced rights of individuals are included in this Privacy Notice and further advice and guidance for the public on how to exercise these rights is also available on the Force website or by contacting 101
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	No data will be saved / stored from mobile devices as a result of their examination - this is a triage/ viewing tool. The only circumstance in which data may be taken is in the form of contemporaneous notes. Any data taken

		inaccurate data? • What guidance will be in place to deal with the requirements under Section 48?	in the form of contemporaneous notes will be lodged as a production, for evidential purposes and therefore subject to record retention policy. The GDPR and the Data Protection Act 2018 strengthen the rights of individuals, as data subjects, in relation to the personal data that Police Scotland holds about them. Concerning this right, Cybercrime will work with Information Management, who process such requests as a statutory obligation, and respond accordingly. The above right is subject to exemptions that we may apply, for example if data is being processed for law enforcement purposes or under a legal obligation. Police Scotland publishes a Privacy Notice on its website that outlines why we process data and our legal basis for doing so for Law Enforcement Purposes. The enhanced rights of individuals are included in this Privacy Notice and further advice and guidance for the public on how to exercise these rights is also available on the Force website or by contacting 101
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?	Not Applicable - No data will be saved / stored from mobile devices as a result of their examination - this is a triage/ viewing tool. The only circumstance in which data may be taken is in the form of contemporaneous notes. Any data taken in the form of contemporaneous notes will be lodged as a production, for evidential purposes and therefore subject to record retention policy.

			The erasure of this data is as per existing process in relation to productions and associated retention periods / policy. The GDPR and the Data Protection Act 2018 strengthen the rights of individuals, as data subjects, in relation to the personal data that Police Scotland holds about them. Concerning this right, Cybercrime will work with Information Management, who process such requests as a statutory obligation, and respond accordingly. The above right is subject to exemptions that we may apply, for example if data is being processed for law enforcement purposes or under a legal obligation. Police Scotland publishes a Privacy Notice on its website that outlines why we process data and our legal basis for doing so for Law Enforcement Purposes. The enhanced rights of individuals are included in this Privacy Notice and further advice and guidance for the public on how to exercise these rights is also available on the Force website or by contacting 101

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 have a logging function to track the details so that a record (or log) is created each time a person undertakes the triage of a device. The logs will make it possible to establish the justification for, and date and time of the triage. Cybercrime audit log of the Mobile Phone Kiosk will record who the users of the system are and will Mobile

		• 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.	Device Kiosk will log that an examination has been undertaken and what the results were (positive/negative, passed to Cybercrime and times and dates etc.) This audit log will be available to the system administrator (Cybercrime) for quality audits and to ensure all devices are being processed in accordance with agreed processes and that it is being assessed and triaged appropriately including the accuracy of what is being recorded in the log. Justification for kiosk use will be outlined within the ERF. Any anomalies can be recorded on the Case Management system (ERF) to reflect any discrepancies in the process. A regular audit will be collated displaying unique reference number for every triage. The logs will make it possible to establish the justification for, and date and time of the triage. It will be possible to see who has undertaken the triage, what the search criteria was and whether the device contained evidential value and passed to Cybercrime or no evidential value and returned to the owner for example. The person who accessed the personal data is therefore identified No data can be directly disclosed from the examination as no data can be retained. The only circumstance in which data may be taken is in the form of contemporaneous notes. Any data taken in the form of contemporaneous notes will be lodged as a production, for evidential purposes and therefore identifiable and subject to record retention policy.

			Other than lodged notes, no data can be received as no data can be retained Force Audit and Assurance have been engaged and are devising process for Bi Annual Audit of Kiosk Use
Q37	**DPA 2018 Section 66**	**Security of processing:**	
		• Will the data be encrypted?	Any data extracted for display on the kiosk will not be encrypted.
		• Will the data be pseudonymised? If so how?	Any data extracted for display on the kiosk will not be pseudonymised.
		• How will the data be protected against risk of loss, confidentiality, availability and integrity?	Any data extracted for display on the kiosk will be securely wiped from the kiosk when the examination is complete.
		• Will back-ups be taken? If so, when/how often?	As data extracted for display on the kiosk is securely wiped after examination, and as no data egress is possible from the kiosk it follows that no backup from the device is possible
		• Will the security of the system be required to have any formal accreditation or independent certification (e.g. ISO27001)?	No formal system security will be required. The system is however protected by being retained within a Police Station and available for use only by trained Police Officers who access the Kiosk via a unique user name and password. The Kiosks are not networked and are standalone.
		• What processes will be in place to determine who will have access to the data/system?	All access will be via individual passkey. Persons having access to the system will comprise nominated, trained and certificated police officers who will be granted 'operator' access to the kiosk systems, and all Cybercrime staff who will have 'admin' access to the kiosk systems. There will be a further 'management' account which will oversee both accounts and which will only be available to Cybercrime management.

			To allow for resilience in the event of a local kiosk being faulty, all users of the system will have the right to access any kiosk throughout the force area. Cybercrime will retain the right to add and delete user access to the kiosks.
		• What level of security clearance will be required to access the system/data?	Management Vetting

		• What data protection/security training will users of the data/system be required to have?	Successful completion of Certified training Course, which includes Data Protection. Three training modules are currently available on Moodle and are mandatory for officers and staff, the modules are: • Module 1 – General Awareness • Module 2 – Behaviour and Security • Module 3 – Consent
		• How will access to the system be granted?	Cybercrime Administration will create user accounts and passwords conforming to SyOps Documentation
		• What information asset register and/or risk register will the data be recorded on?	Corporate Information Asset Register. Cybercrime Case Manangement System will record what actions have been taken.
		• Will you have a SyOps/Procedure manual/SOP, etc. to detail the above?	Yes - Cybercrime Kiosk Toolkit, Digital Forensic examination , Principles of Use'
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, the ICO, Scottish Human Rights Commission and Privacy International have been consulted as have HMIC, Police Federation, UNISON, SPA and COPFS and a demonstration of the Kiosk by senior management was delivered at Victoria Quay. COPFS, ICO, and the Scottish Exec were represented at Victoria Quay on 24th May 2018 .

			Justice sub Committee have been involved and the opinion and views of members included in development of this and associated documents sets. In particular Justice Sub Committee of 13th September 2018 where Data Protection and Human Rights were discussed. The final draft of this document will be circulated to the above partners via the Stakeholder and External Reference groups established in by Police Scotland in relation to Kiosks.
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** 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.	No
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; • Military service; • Community service in a public emergency; and normal civic obligations	No
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;	No - The practice will assist investigators in identifying relevant information either inculpatory or exculpatory to the enquiry. Kiosk use seeks to reduce the need for persons to be unnecessarily detained, as an assessment of digital evidence within a relevant device is assessed locally via kiosk and therefore much quicker than within existing hub processes. Kiosk use protects the wider security of the public with early identification of offenders and their timeous presentation into the criminal justice process. If the legal framework as outlined was compromised Article 5 would be engaged as to continue to use

		• 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.	evidence obtained as a result of Triage from devices deemed as unlawfully seized or examined, would result in the unlawful arrest detention, and conviction of individuals in breach of Article 5 Police Scotland has no reason to believe that the legal framework allowing us to lawfully seize and examine mobile devices is compromised and has submitted evidence obtained from devices and secured numerous convictions in recent years.
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 specifically classified as hearings that must be heard 'in camera', i.e. closed to the public.	Yes – The Impact is not in direct relation to the use of this facility as the impact associated exists within the current seizure and associated digital forensic processes employed by Police Scotland. The introduction of triage to that process does not change this. Article 6 is engaged with regard to the legality of the possession, retention and review of a device by Police Scotland which is subsequently triaged as part of the proposed implementation of Kiosk use. The taking possession therefore must be for a policing purpose and connected to a police investigation. Seizure is the means by which an officer will take possession of a device connected to an investigation. The police are entitled at common law to seize anything it is believed to potentially be connected in some way to a police investigation or incident. This power of seizure applies to both common law and statutory offences even although the statute contravened makes no provision for seizure. All seizures must be for a policing purpose and includes devices seized during execution of a search

			warrant or under legislative provision. These powers form the legislative framework under which we must consider seizure of digital devices and by default the data within and any subsequent examination. An individual's right to a fair trial could therefore potentially be compromised by the unlawful seizure and subsequent recovery and review of a device and its data. Each officer has the responsibility to ensure their actions in that regard are lawful thereby protecting these rights Police Scotland has no reason to believe that the legal framework allowing us to lawfully seize and examine mobile devices is compromised and has submitted evidence obtained from devices and secured numerous convictions in recent years.
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:	Yes - As per any enquiry or investigation involving digital data there is an element of intrusion and collateral intrusion. The impact of the introduction of this facility is a reduction in the copy, storage, and retention of data associated with devices by virtue of potentially removing the device from cybercrime hub processes were no evidence is found. The facility will also reduce the number of officers reviewing device

		• 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.	data with those trained in kiosk use being used for devise triage across multiple investigations as opposed to individual investigating officers. There is no change in terms of the impact to Article 8 rights as the review of data required in kiosk triage is currently undertaken but via a full download process at cybercrime hubs. The 'Digital Forensic Examination, Principles of Use' outline the following principles which must be adhered to. There is no change in terms of the impact to article 8 rights. To conduct diligent enquiry and maximize our capability to detect crime, the balance of investigative needs versus the public expectation of privacy must be met by doing what is lawful, ethical and in good faith and no more than is necessary and proportionate to achieve the lawful objective sought. Fairness, integrity and respect of property and right to privacy outlined within Article 8 ECHR are the key principles which guide all officers in the execution of duty. These principles are requirements for the use of Police Scotland technical ability including the examination of devices. It is the responsibility of all officers and staff at all stages of the investigative and examination process associated with digital device examination to ensure that they review were possible only what is relevant to the investigation and consider, comply and act in accordance with the law and these principles all at times. Necessity – This means that the action taken is necessary to achieve the objective of the digital investigation of that device. If an action is not necessary the intrusion can therefore not be justified and the action should not be taken. Proportionate – This means that the officer has

			considered the intrusion that their activity will involve and with due regard to the implications in terms of respect for private and family life. The officer must be content that any / further interrogation of data is proportionate under the circumstance / needs of the investigation. Relevant – This means that the data which the officer seeks to review is only the data relevant or potentially relevant to the investigation. If the data held is not potentially relevant it should not be reviewed.
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; • Protection of public order, rights or morals; • Protection of rights and freedoms of others.	No
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.	Yes – The Impact is not in direct relation to the use of this facility as the impact associated exists within the current digital forensic processes employed by Police Scotland. The introduction of triage to that process does not change this. The impact of digital forensic examination whether by Kiosk Triage or otherwise impacts upon Article 10 not by virtue of the data review but in relation to the denial

			of access to a device which is a means by which individuals exercise their right to expression via the various platforms, applications and communication opportunities the device provides. As such the denial of an individual's access to their devise must be with due regard to the necessity and proportionality of the circumstances of the investigation. Necessity – This means that the action taken is necessary to achieve the lawful objective of the digital investigation of that device. If an action is not necessary the impact can therefore not be justified and the action should not be taken. Proportionate – This means that the officer has considered the impact that their activity will have and with due regard to the implications in terms of right to free expression. The officer must be content that any denial of this right in seizure of a device is proportionate under the circumstances / needs of the investigation.
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	No

		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	
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? 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	No

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	**Low (2)** **High (4)** **Score: 8**	**- Existing Legal Framework** **-Certified Training** **- Mobile Phone Kiosk SOP** **- Audit Function** **-Central Governance** **- View Only (Unable to egress data)** **- Compliance Check** **- Specified Users**	**Reduced**	**YES** **Mitigations placed kiosk capability and the mitigations outlined in this risk will greatly reduce the possibility of destroying or mishandling personal information.**
Article 8 - Right to Respect for Private and Family Life	**Very high (5)** **Medium (3)** **Score: 15**	**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, Practices, Training and Guidance.** **At the point were it is established there is evidential value the triage will cease and the device will**	**Accepted**	**YES** **The impact is justified, compliant and proportionate within the bounds of police investigations. All trained kiosk users are bound by Guidance, 'Principles of Use' and the Data Protection Act.**

		be sent to Cybercrime.		
Article 5 - Right to Liberty and Security	Very low(1) Very High (5) Score : 5	There is currently no threat of engaging this right re Kisok Use as the legal framework for the seizure and review of devices exists	Eliminated	YES If this changes this would significantly impact this right and require full review and change of process and police actions
Expectations and Concerns of the General Public	May Happen (3) Medium (3) Score: 9	Consultation with Scottish Government: Scottish Executive Cyber Resilience team and a representative from the ICO and SHRC 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.	Reduced	YES All possible steps have been taken to consider the opinions and observations of a variety of stakeholders with a view to demonstrating the capabilities of the kiosks and to give transparency and justification to the policies, procedures and practises in their use.
Article 6 - Right to a fair trial	Very low(1) Very High (5)	There is currently no threat of engaging this right re Kisok Use as the legal framework for	Eliminated	YES If this changes this would significantly impact this right and require full review

	Score : 5	**the seizure and review of devices exists.**		**and change of process and police actions**
Article 10 – Right to freedom of expression	**High (4)** **Low (1)** **SCORE : 4**	**The impact of digital forensic examination whether by Kiosk Triage or otherwise impacts upon Article 10 not by virtue of the data review but in relation to the denial of access to a device which is a means by which individuals exercise their right to expression via the various platforms, applications and communication opportunities the device provides. As such the denial of an individual's access to their devise must be with due regard to the necessity and proportionality of the circumstances of the investigation.**	**Reduced**	**Yes** **Providing the legal frameworks exists – The right is not removed entirely merely in relation to the opportunities within that devise provide the individual as described which can be achieved via other devices or means.**

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:

SCOTTISH POLICE AUTHORITY

POLICE SCOTLAND
POILEAS ALBA

Division	SCD	**Department**	Cybercrime
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 Device Cyber Kiosks
Owning Department	SCD, OCCTU, 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.

Purpose:
The objective of the project is to allow Police Scotland to preview mobile device productions in a focused, more precise and less intrusive manner than currently available and to establish if those devices contain potential evidence before their submission to Cybercrime Hubs.

A cyber kiosk is a computer terminal that can view data on a device in a targeted and focused way i.e. only looking at what is necessary. If unsure as to whether a device holds information relevant to an investigation it may undergo a triage process using a 'Cyber Kiosk'. This process is only performed by trained staff, the purpose of which is to identify if the mobile phone or device contains any evidential data using, where appropriate, selected parameters, e.g. text messages or a specific date range. If no potential evidence is found it may be returned to the owner. The current Kiosk configuration only provides a viewing facility. It does not record any data from the mobile phone / device.

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 for mobile devices.

Seized mobile devices will include those of victims, witnesses, suspects or accused persons including those obtained under common law powers, the authority of a judicial warrant or statutory power. All such devices are treated as productions by Police Scotland and are handled in accordance with the Productions SOP and subject to associated retention policies.

Cyber kiosks are operated by specially trained officers (in the region of 410 officers' c. 10 per kiosk machine for resilience) with the ability to triage lawfully seized devices.

No device data is retained by the kiosk machine. The equipment has the capacity to copy data however this facility is disabled and cannot be enable by standard operators. It is possible that Police Scotland may review use of the extraction functions in future however there is no intention to do so at this time. Any change in the functionality of the device to be anything other than view only will require a resubmission of an associated DPIA and EqHRIA.

The Kiosk has the capability to examine other items such as USBs or SD cards however the facility to examine anything other than a Mobile Phone or Tablet has been disabled. Any change in the functionality of the device to include other items will require a resubmission of an associated DPIA and EqHRIA as appropriate.

Associated guidance has been developed to give police officers and police staff guidance on the use of mobile phone kiosks.

Intended outcomes:

- The potential return of devices to owners where the triage has allowed an assessment that the device does not contain evidence.
- Improved service to frontline officers in establishing the relevance of a device to an investigation and the identification of evidence resulting in more timely detections and investigations.
- Fewer devices being submitted to Digital Forensics Hubs meaning only devices of evidential worth are submitted meaning swifter evidence identification and criminal justice process preventing and detecting crime, harm and disorder allowing hubs to focus and prioritise activity and evidence recovery.
- Resource saving, as where no evidence is identified, there is no copying of the data held on a device to facilitate an assessment of each device seized and therefore no data storage and transfer implications.
- Triage in a more focused manner than current processes allow, focused investigation in the relevant areas of the device for example' text messages meaning less intrusion of privacy.
- Due to the reduced strain on hubs, Criminal Justice partners receive a faster and improved quality of service with regard evidential requests.
- Fewer submissions to Digital Forensics Hubs will reduce backlogs and provide an improved turnaround time for submissions. It will also allow Cybercrime staff to focus their time and forensic tools on more high priority complex examinations that require a higher skill set.

NOTE – Whilst kiosk triage includes the implementation of new technology for Police Scotland for use outside Digital Forensics hubs the kiosk facility provides a function already carried out by police Scotland in terms of digital download and review of mobile devices currently performed within those Digital Forensics Hubs. This is not a new capability for the force. It is an additional process within existing digital forensic structure to eliminate devices of no evidential value from police investigations. The Kiosk is essentially a simplified version of the technology used within hubs, with appropriately limited capabilities, which achieves the outcomes outlined above.

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?

- Digitally Stored Evidence PSoS SOP
- Productions PSoS SOP
- Information Security Policy
- Interpreting and Translating SOP

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 – NOT APPLICABLE

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.	The only protected characteristic where impact may occur are age, race and disability in relation to Kiosk users.	**Consultation** has included the following -Scottish Government: Scottish Executive Cyber Resilience team, the ICO, Privacy International have been consulted as have HMICS, Scottish Police Federation, UNISON, SPA, Scottish Human Rights Commission and COPFS. .

			Scottish Government, Justice Sub Committee have been involved and the opinion and views of members and above partners included in development of this document. It has been made clear during this engagement that the concerns considered in relation to Cyber Kiosks are not in relation to the principle kiosk capability and use itself but rather more general with regard police access to, review and management of the digital data held within Mobile devices. These wider concerns are reflected and considered within this assessment. Training New training of Police officers in Kiosk Use and train the trainer training has been considered in terms of implications with regard the upskilling of staff and impact in terms, conditions or work pattern. There is no identified impact in this regard.
Age	Low Impact	Potential that this practise impacts upon individuals of a particular age range.	There is a potential that this practise impacts more upon individuals of a particular age range due to the generational use, understanding and prevalence of digital devices and associated communications being more prevalent within those of working age as opposed to the elderly or very young with a peak internet usage at 99% of people in the age range from 16 to 34. Compared to over 75s being at 44% (Office of National Statistics, Internet users UK, 2018). This impact upon these demographics of the population is likely further enhanced by overlap with the age range during which individuals are most likely to come into contact with Police during Police incidents and investigations. Whilst the impact is recognised this is accepted as out with any control and subject to change and

			influenced by digital culture, economics or media and other factors out with police control.
Disability	Low Impact	Potential user accessibility issues to operate equipment effectively due to an existing disability relating to eye impairments or dyslexia.	The fonts and icons are fixed on the kiosks by the manufacturer and cannot be adapted or modified. Local solutions will need to be considered dependent on the individual's requirements and would be assessed on a case by case basis. Existing support for users of police Systems will be available to anyone who requires access to the kiosks and may mitigate any potential issues relating to viewing data and operating the kiosk.
Gender Reassignment	No impact	No Evidence available to suggest any impact due to membership of this protected group	
Marriage and Civil Partnership	No impact	No Evidence available to suggest any impact due to membership of this protected group	
Pregnancy and Maternity	No impact	No Evidence available to suggest any impact due to membership of this protected group	
Race	Low impact	Potential that digital data may be in the form of a language other than the users first language / a language in which the user has no or limited ability to translate.	Where triage of a device identifies use of a foreign language, officers whose first language is English may need to refer to the Interpreting and Translating SOP.
Religion or Belief	No impact	No Evidence available to suggest any impact due to membership of this protected group	
Sex	No impact	No Evidence available to suggest any impact due to membership of this protected group	
Sexual Orientation	No impact	No Evidence available to suggest any impact due to membership of this protected group	

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 an incident where there is a threat to life the proposed use of Cyber Kiosks could allow for the use of the technology in support of preventing loss of life via the ability to review device data.	Triage of devices will be necessary, proportionate and relevant and will only be conducted to serve a policing purpose. **The legal framework for Kiosk Use -** The police are entitled at common law to seize anything it is reasonably believed to potentially be connected in some way to a police investigation or incident. This power of seizure applies to both common law and statutory offences even although the statute contravened makes no provision for seizure. All seizures must be for a policing purpose and includes devices seized during execution of a search warrant or under legislative provision. With regard to 'Policing Purpose', the general duties of a constable outlined in the Police Fire reform (Scotland) act 2012 are; (a) to prevent and detect crime, (b) to maintain order, (c) to protect life and property, (d) to take such lawful measures, and make such reports to the appropriate prosecutor, as may be needed to bring offenders with all due speed to justice, These powers form the legislative framework under which we must consider seizure of digital devices and by default the data within and any subsequent examination. It is in the execution of these duties that we undertake all digital forensic examinations.

			Examination must be / have; Necessary – This means that the action taken is necessary to achieve the objective of the digital investigation of that device. If an action is not necessary the intrusion can therefore not be justified and the action should not be taken. Proportionate – This means that the officer has considered the intrusion that their activity will involve and with due regard to the implications in terms of respect for private and family life. The officer must be content that any / further interrogation of data is proportionate under the circumstance / needs of the investigation. Relevant – This means that the data which the officer seeks to review is only the data relevant or potentially relevant to the investigation. If the data held is not potentially relevant it should not be reviewed. Legitimate Aim - Acting with a legitimate aim, for a policing purpose with the associated reasonable belief as outlined are the grounds on which the power of seizure described above is based. It is only with this legitimate aim that an officer should seize and subsequently review a device.
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 guidance associated with use of Cyber Kiosks will allow for the use of the technology in support of investigations.	Legal Framework - As outlined above
Article 5 Right to Liberty and Security	Protects	The practise will assist investigators in identifying relevant information either inculpatory or exculpatory to the enquiry.	Legal Framework - As above

		Kiosk use seeks to reduce the need for persons to be unnecessarily detained, as an assessment of digital evidence within a relevant device is assessed locally via kiosk and therefore much quicker than within existing hub processes. Kiosk use protects the wider security of the public with early identification of offenders and their timeous presentation into the criminal justice process However if the legal framework as outlined was compromised Article 5 would be engaged as to continue to use evidence obtained as a result of Triage from devices deemed as unlawfully seized or examined, could result in the unlawful arrest detention, and conviction of individuals in breach of Article 5	Police Scotland has no reason to believe that the legal framework allowing lawfully seizure and examination of mobile devices is compromised and has submitted evidence obtained from devices and assisted in securing multiple thousands of convictions in recent years.
Article 6 Right to a Fair Trial	Protects	Article 6 is engaged with regard to the legality of the possession, retention and review of a device by Police Scotland which may subsequently be triaged as part of the proposed implementation of Kiosks. The taking possession of devices by Police therefore must be for a policing purpose and connected to a police investigation. Seizure is the means by which an officer will take possession of a device connected to an investigation. An individual's right to a fair trial could therefore potentially be compromised by the unlawful seizure and subsequent recovery and review of a device and its data. Each officer has the responsibility to ensure their actions in that regard are lawful thereby protecting these rights. The practise will assist investigators in identifying relevant information either inculpatory or exculpatory to the enquiry. The associated guidance contains information regarding seizure and handling of devices	Legal Framework - As above The police are entitled at common law to seize anything it is reasonably believed to potentially be connected in some way to a police investigation or incident. This power of seizure applies to both common law and statutory offences even although the statute contravened makes no provision for seizure. All seizures must be for a policing purpose and includes devices seized during execution of a search warrant or under legislative provision. These powers form the legislative framework under which we must consider seizure of digital devices and by default the data within and any subsequent examination. The process outlined within the Toolkit and training regard disabling the ability of devices to connect to a

		for evidential purposes.	network protects against any potential for interception of data. Therefore the only data reviewed will be that which was on the device at the time of seizure. Police Scotland has no reason to believe that the legal framework allowing us to lawfully seize and examine mobile devices is compromised and has submitted evidence obtained from devices and assisted in securing multiple thousands of convictions in recent years.
Article 7 No Punishment without Law	N/A		
Article 8 Right to Respect for Private and Family Life	Protects/infringes	As per any enquiry or investigation involving digital data there is an element of intrusion and collateral intrusion. The impact of the introduction of this facility is a reduction in the copy, storage, and retention of data associated with devices by virtue of potentially removing the device from Digital Forensics hub processes were no evidence is found. The facility will also reduce the number of officers reviewing device data with those trained in kiosk use being used for device triage across multiple investigations as opposed to individual investigating officers. There is no change in terms of the impact to Article 8 rights as the review of data required in kiosk triage is currently undertaken but via a full download process at Digital Forensics hubs. The process of examining devices using the Kiosk does not retain data on the Kiosk itself. The data extracted from the mobile device is securely wiped from the internal storage on the Kiosk once the operator has finished the examination.	Legal Framework - As above The 'Digital Forensic Examination, Principles of Use' have been written to outline the following principles which must be adhered to in the use of kiosk devices and general digital forensic investigations. To conduct diligent enquiry and maximize our capability to detect crime, the balance of investigative needs versus the public expectation of privacy must be met by doing what is lawful, ethical and in good faith and no more than is necessary and proportionate to achieve the lawful objective sought. Fairness, integrity and respect of property and right to privacy outlined within Article 8 are the key principles which guide all officers in the execution of duty. These principles are requirements for the use of Police Scotland technical ability including the examination of devices. It is the responsibility of all officers and staff at all stages of the investigative and examination process associated with digital

		The only data retained on the Kiosk as a consequence of the examination is the logging information retained for the purposes of auditing and assurance. Kiosks can only be used to examine lawfully seized devices. No other devices should be examined on them. To enforce this, regular dip samples from the system logs will be taken for Quality Assurance purposes. This article can be perceived as being infringed by individuals whose data is being viewed by Police however this action is permitted under the legal framework outlined, enabling Police investigation.	device examination to ensure that they review were possible only what is relevant to the investigation and consider, comply and act in accordance with the law, well established practise and process in relation to the legal framework and these principles all at times. Necessity – This means that the action taken is necessary to achieve the objective of the digital investigation of that device. If an action is not necessary the intrusion can therefore not be justified and the action should not be taken. Proportionate – This means that the officer has considered the intrusion that their activity will involve and with due regard to the implications in terms of respect for private and family life. The officer must be content that any / further interrogation of data is proportionate under the circumstance / needs of the investigation. Relevant – This means that the data which the officer seeks to review is only the data relevant or potentially relevant to the investigation. If the data held is not potentially relevant it should not be reviewed. Legitimate Aim - Acting with a legitimate aim, for a policing purpose with the associated reasonable belief as outlined are the grounds on which the power of seizure described above is based. It is only with this legitimate aim that an officer should seize and subsequently review a device.
Article 9 Freedom of Thought, Conscience and Religion	N/A		

Article 10 Freedom of Expression	Infringes	The Impact is not in direct relation to the use of this facility as the impact associated exists within the current digital forensic processes employed by Police Scotland in particular seizure of devices. The introduction of triage to that process does not change this. The impact of digital forensic examination whether by Kiosk Triage or otherwise impacts upon Article 10 not by virtue of the data review but in relation to the denial of access to a device which is a means by which individuals exercise their right to expression via the various platforms, applications and communication opportunities the device provides. As such the denial of an individual's access to their device must be with due regard to the necessity and proportionality of the circumstances of the investigation.	Legal Framework – As Above Necessity – This means that the action taken is necessary to achieve the lawful objective of the digital investigation of that device. If an action is not necessary the impact can therefore not be justified and the action should not be taken. Proportionate – This means that the officer has considered the impact that their activity will have and with due regard to the implications in terms of right to free expression. The officer must be content that any denial of this right in seizure of a device is proportionate under the circumstances / needs of the investigation. Legitimate Aim - Acting with a legitimate aim, for a policing purpose with the associated reasonable belief as outlined are the grounds on which the power of seizure described above is based. It is only with this legitimate aim that an officer should seize and subsequently review a device.
Article 11 Freedom of Assembly and Association	N/A		
Article 14 Prohibition of Discrimination	N/A		
Protocol 1, Article 1 Protection of Property	Infringes	The Kiosk Toolkit and Principles of Use contain information regarding seizure and handling of devices. This article might be perceived as infringed by the individual as they are deprived of their private property by Police. This is covered by appropriate legislation enabling investigation of crime.	Legal Framework regarding seizure as above.

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.

Owning department will monitor changes in legislation/circumstances which may affect the Kiosk making amendments as appropriate, assessing how these changes may impact on the protected groups and Human Rights. In addition, they will be responsible for the cyclical review of Kiosk use, associated documents and EqHRIA.

Management Information (MI), Kiosk Use - The Kiosk will log that an examination has been undertaken and what the results were (positive/negative, passed to Cybercrime and times and dates etc.) This audit log will be available to the system administrator (Cybercrime) for quality audits and to ensure all devices are being processed in accordance with agreed processes and that it is being assessed and triaged appropriately, including the accuracy of what is being recorded in that MI log.

Kiosks produce logs which show the times of extractions, the ID of the person doing the extraction, when the extraction occurred, the name of the device being extracted and the case reference number from our Case Management system. These logs are stored on the kiosk itself and are not accessible by operators.

Cybercrime staff will periodically visit the kiosks to provide updates, etc. At this time, using enhanced credentials, they will log into the kiosk and recover these logs. The logs will be aggregated at Newbridge Police Office and aggregated on a central repository on the Cybercrime network which is secured.

They will be used for training, business and audit purposes. A dip sample (volume to be confirmed once level of use of the kiosks is better understood) will be taken of examinations from the logs. This will be compared against the case management system to ensure that the examination was authorised, that it

was proportionate to the case and that the device was seized legally and handled in accordance with productions processes. If the examination fails on any of these points then the appropriate action will be taken, whether that is by remedial training or by disciplinary process.

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
Proper and lawful use of the Kiosk	Training and guidance including the following documents have been consulted on with partners including, Human Rights Commission, Privacy International, SPA, Police Federation, Unions, Scottish Government, HMICS, COPFS, Information Management. The Principles of Use, Toolkit and two day training course, DPIA, EqHRIA, Quality assurance measures and full auditable and accountable process ,from seizure to Case Management System (ERF) Submission, triage and beyond to Digital Forensics Hub examination ensure compliance with law and responsibilities	DCI Cybercrime Operations	Estimate by November 2018	Documents and training still under development. Final Consultation and Sign off required and anticipated following circulation for feedback at meeting of 30 October.
Officer's awareness and clear parameters of their responsibilities re data interrogation with regard to ECHR and necessity, proportionality and relevance.	Develop a 'Principles of Use' document articulating this guidance, roles , responsibilities and ensure awareness of kiosk operators via training and communications strategy re principles of use. Ensure these parameters are reflected and outlined in all guidance.	DCI Cybercrime Operations	Estimate by November 2018	11/10/18 Under development. Due ratification pre training

Existence of legal framework under which triage and forensic examination is undertaken	PSoS are content that legal framework currently exists and is supported by current Court cases and trials in which such evidence is accepted. Several stated cases support this framework. A letter has been sent to crown requesting COPFS confirmation of this position. Activity being developed to consider further the existing legal framework recognising change in device capability and content over time. HRC believe a warrant may be required to access a mobile phone. Their legal team are considering this and will share feedback with PSoS due W/C 15 October.	DCI Cybercrime Operations	Estimate by November 2018	11/10/18 – Draft letter to Crown with DCS McLean for ratification.
Appropriate forum for the enhancement of ECHR knowledge / responsibilities of Kiosk operators.	Roles and Responsibility of operators in terms of Principles of Use, DPIA and EQHRIA have all been incorporated into the 2 day Kiosk operator training course.	DCI Cybercrime Operations	Estimate by November 2018	11/10/18 Under development by Cyber Training Team. Force training aware, sighted on proposal and content that no formal involvement is required from them.
Appropriate audit and assurance of Kiosk use to ensure compliance with ECHR, process , oversight and means to address issues.	Kiosks produce Management Information Data providing oversight of use by an operator. A plan will be drafted which will outline what is being monitored including frequency and purpose of kiosk use, dip sampling process , learning and remedial action taken, This data will be subject to regular review and dip sampling and will be published.	DCI Cybercrime Operations	Estimated March 2019 following roll out	Under development by Cybercrime training team.
Failure to appropriately or adequately circulate / propagate communications in relation to clear parameters of	Communication Strategy developed to mitigate this risk to consider intranet publications, Guidance Circulations. There is also established liaison with operators via divisional and Cybercrime SPOCs (emails / contacts list and FAQs etc)	DCI Cybercrime Operations	Estimated November 2018 to February 2019	Communications Strategy being drafted for sign off on 29/10/18

Kiosk operator responsibilities re data interrogation with regard to ECHR, necessity and proportionality				
Failure to ensure appropriate collation of issues identified and process for referral of any potential compromise to ECHR obligations.	A local SPOC has been identified for each Kiosk. This SPOC will hold responsibility for the collation of all issues including those under this risk and will collate and articulate such issues to Cybercrime. A process has been developed via another SPOC at Cybercrime in relation to this. Kiosk Operators are aware of this via training / guidance. A list of SPOCs is included in Guidance. A list of all SPOCs and Operators will be held at Cybercrime. Operators will also be Identifiable via SCOPE as having completed Kiosk Training This feed of issues will be monitored by Cybercrime staff and issues addressed via the communications mediums available via SPOCs and Operators. Associated Kiosk Document s, EqHRIA , DPIA, Toolkit etc can and will be changed if required.	DCI Cybercrime Operations	October 2018	Complete – Process map within the Toolkit
8- Sufficient public awareness regard lawful device seizure, rights and associated police process and implications.	A ‘public leaflet’ will be developed and consulted on via the partners listed above. The intention is that these will be made available to frontline staff to provide the public on each occasion a device is seized.	DCI Cybercrime Operations	Estimate by November 2018	Under development
Officers have the appropriate vetting for Kiosk use.	All police officers undergo Recruitment Vetting (RV) as part of the role. Force Vetting Unit have been consulted and confirm that RV vetting provides sufficient protection in relation to the proposed kiosk functionality.	DCI Cybercrime Operations	October 2018	Complete

	RV is the minimum level required for all applicants to join SPA/Police Scotland irrespective of their role. Successfully attaining RV clearance allows access to police systems, assets, premises and classified information up to CONFIDENTIAL or OFFICIAL-SENSITIVE with occasional access to SECRET.			

9. Management Log

9.1 EqHRIA Author Log

Name and Designation	Michael McCullagh, T/Detective Inspector	**Date** (DD/MM/YY)	18/10/2018
Comments	Draft EqHRIA has been completed in consultation with Nasreen Mohammed, Force E&D Adviser, SCD Safer Communities following engagement with the Scottish Human Rights Commission and their valuable input regards the various aspects of Human Rights engaged by this practise and wider the investigation of digital data.		
Name and Designation		**Date** (DD/MM/YY)	
Comments			
Name and Designation		**Date** (DD/MM/YY)	
Comments			

9.2 Quality Assurance Log

Name and Designation	DCI Brian Stewart	**Date**	20/10/18	**Document Version**	V0.3
Comments	Fully reviewed document and suggested changes to wording and spelling. Consideration to be made around some of the areas that are listed as N/A for comment to be drawn up if appropriate.				
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					