Data Protection Impact Assessment – Cyber Kiosks

Law Enforcement Processing only

Control Sheet

Title	**Cyber Kiosks**
Date Approved	11/11/2019
Version Number	1.3
Document Type	Data Protection Impact Assessment
Document Status	APPROVED
Author	SCD, OCCTU, Cybercrime Capability Programme.
Strategic Asset Owner	ACC Organised Crime, Counter Terrorism and Intelligence

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
0.13	20/12/18	Updates following consulation with ICO
0.14	24/05/19	Updates following Senior Council Opinion
0.15	15/08/19	Update following Consultation with ICO
0.16	22/10/19	Update following PSOS Legal Services Opinion
0.17	08/11/19	Update to Risks and Q2, 11, 26, 40
1.0	10/11/19	Approved by Information Assurance

1.1 1.2 1.3	14/11/19 18/11/19 06/01/20	Updated following feedback from Legal Services Correction of typographical error Amendments at the request of Strategic Asset Owner to Q2; Q6, Q11, Q17, Q26 and Q40

Consultation History

Version	Date	Name	Designation
See Q38			

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)	ACC Angela McLaren - ACC Organised Crime, Counter Terrorism and Intelligence
Q3	Provide a summary of the project.	The project concerns the introduction of 41 Digital Triage Devices (DTD) - '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. The only devices that may be subject of Triage using a kiosk is a mobile phone or tablet. 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. The areas of the device which will be examined during the kiosk process will be guided by the device owner and the investigation. The search for evidential material can be filtered, directing the triage to specific areas such as Text messages, Call Data, Chat (Whats app / Snap chat), Multimedia (Audio, Video, Photographs), Internet history, Email, etc. This also includes the ability to limit the search using a date range or keyword search criteria. If no potential evidence is found the device can 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 / Submitted mobile devices will include those of victims, witnesses, suspects or accused persons including those obtained voluntarily, under common law powers, the authority of a judicial warrant or statutory power including search. 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 or voluntarily submitted devices, for a policing purpose, reducing the number which are required to be forensically examined within Digital Forensic (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 a new associated DPIA / EqHRIA.

		Sufficient personal details to identify the Police Officer or member of Police Staff conducting the triage will be recorded by the Cyber Kiosk. The operator will be aware that their details are stored and all their activity on the Kiosk is auditable. Contemporaneous notes may be taken by officers. A contemporaneous note refers to notations made (pen and paper / Police Scotland official notebook) by the reviewer / enquiry officer for use in association with the investigation in question for example if during triage of a suspects phone, evidence is recovered that officer wishes to quote to the suspect verbatim during interview. Guidance in relation to such notes is made within the associated toolkit requiring officers to lodge any notes taken on paper making them subject to production processes (Audit) retention policy, locatable and secure. If noted within an officer's notebook this would be again subject to the protections, audits function and retention periods associated to note books. 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 a new associated DPIA/ EqHRIA
Q4	Detail the benefits of the project to Police Scotland.	Most people now own and use a digital device, in most cases a mobile phone with many using significant amounts of data and multiple applications. This provides modern policing with a challenge; to balance its duty to protect the public whilst respecting the rights of citizens in an increasingly digital environment. An increasing amount of crime is now committed either in the virtual world or has a significant digital footprint. Even those crimes committed in the physical world increasingly have some form of digital evidence. As a result, the ability to harness relevant data within devices has become an essential part of judicial process and the administration of justice. In order to ensure Police Scotland protects the communities of Scotland and keeps people safe, it requires to continually enhance its capability to keep up with the changes in everyday technology and devices, which continue to grow, not only in number but also in capability and complexity. In light of this Kiosks provide:

		Improved service to frontline officers in establishing the relevance of a device to an investigation and the existence of evidential content which may expedite investigations and detections. Only devices of evidential worth are submitted to Digital Forensic Hubs, thus allowing swifter evidence identification and criminal justice process. This permits increased prevention and detection of crime, reduction in harm and disorder and allows hubs to focus on high priority activity and evidence recovery. Resource saving and reduced data processing; 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. Allowing Digital Forensic Hub staff to focus their time and forensic tools on more high priority complex examinations requiring their higher skill set. The taking of contemporaneous notes. A contemporaneous note refers to notations made (pen and paper / Police Scotland official notebook) by the reviewer / enquiry officer for use in association with the investigation in question for example if during triage of a suspects phone, evidence is recovered that officer wishes to quote to the suspect verbatim during interview, a benefit being the early identification of evidence. Guidance in relation to such notes is made within the associated toolkit requiring officers to lodge any notes taken on paper making them subject to production processes (Audit) retention policy, locatable and secure. If noted within an officers notebook this would be again subject to the protections, audits function and retention periods associated to note books
Q5	Detail the benefits of the project to any other relevant parties.	The return of devices to owners where the triage showed that the device does not contain 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.

		Focused Triage, allowing investigators to target specific, relevant areas of the device, for example, text messages, photographs etc., thus minimising intrusion into personal data. 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) ACC Organised Crime, Counter Terrorism and Intelligence – Angela McLaren b) D/Chief Supt OCCTU – Phil Chapman
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. Contemporaneous notes may be taken by officers. A contemporaneous note refers to notations made (pen and paper / Police Scotland official notebook) by the reviewer / enquiry officer for use in association with the investigation in question for example if during triage of a suspects phone, evidence is recovered that officer wishes to quote to the suspect verbatim during interview. Guidance in relation to such notes is made within the associated toolkit requiring officers to lodge any notes taken on paper making them subject to production processes (Audit) retention policy, locatable and secure. If noted within an officers notebook this would be again subject to the protections, audits function and retention periods associated to note books Sufficient personal details to identify the Police Officer or member of Police Staff conducting the triage will be recorded by the Cyber Kiosk. The operator will be aware that their details are stored and all their activity on the Kiosk is auditable.

Q8	What sensitive data if any, is to be processed? State the categories. (Refer to guidance **Note 1**)https://spi.spnet.local/policescotland/guidance/Force Forms/Police-Scotland/Data Protection Impact Assessment - Law Enforcement Processing - Guidance.doc - _Hlk513794443	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 data which, 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 permanently extracted from the device. There is also the potential that Legally Privileged, Journalistic material or communications by or to an elected representative may be inadvertently stumbled upon. The procedure is no different than that which exists in guidance for such intrusion in other aspects of policing. The material will be disregarded, will not be viewed further and will not be recorded or otherwise retained. Full details of responsibility and actions are outlined within the 'Covert Surveillance and Property Interference Code of Practice'.

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. The devices are not currently networked and cannot transfer data or be remotely accessed by any means. 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. Contemporaneous notes may be taken by officers. A contemporaneous note refers to notations made (pen and paper / Police Scotland official notebook) by the reviewer / enquiry officer for use in association with the investigation in question for example if during triage of a suspects phone, evidence is recovered that officer wishes to quote to the suspect verbatim during interview. Guidance in relation to such notes is made within the associated toolkit requiring officers to lodge any notes taken on paper making them subject to production processes (Audit) retention policy, locatable and secure. If noted within an officers notebook this would be again subject to the protections, audits function and retention periods associated to note books Sufficient personal details to identify the Police Officer or member of Police Staff conducting the triage will be recorded by the Cyber Kiosk. The operator will be aware that their details are stored and all their activity on the Kiosk is auditable.

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 be subject to audit and compliance checks to ensure adherence with prescribed guidelines. Sufficient personal details to identify the Police Officer or member of Police Staff conducting the triage will be recorded by the Cyber Kiosk. The operator will be aware that their details are stored and all their activity on the Kiosk is auditable. Officers are made fully aware of this during Module 1 of Training which covers Human Rights and Data Protection compliance including clear intention and requirement to audit use of the Kiosk. 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 be potentially relevant in some way to a police investigation or incident. Contemporaneous notes may be taken by officers. A contemporaneous note refers to notations made (pen and paper / Police Scotland official notebook) by the reviewer / enquiry officer for use in association with the investigation in question for example if during triage of a suspects phone, evidence is recovered that officer wishes to quote to the suspect verbatim during interview. Guidance in relation to such notes is made within the associated toolkit requiring officers to lodge any notes taken on paper making them subject to production processes (Audit) retention policy, locatable and secure. If noted within an officers notebook this would be again subject to the protections, audits function and retention periods associated to note books.

Authority for Seizure, Examination and Data Processing

1 Introduction

1.1 Police Scotland proceeds on the premise that there must be a proper basis in law for the actions of its officers and staff. In proceeding upon that basic premise and with regard to the examination of digital devices Police Scotland's action accord with the law as it is understood to be.

1.2 Senior Counsel, Murdo MacLeod's Opinion was sought in relation to legal basis for use of Digital Triage Devices (Cyber Kiosks). He concluded that *'there is lawful basis for the use of cyber kiosks'.*

1.3 It should be noted that powers outlined below apply only to the contents of a device, commonly referred to as 'stored data' and not 'online data' accessed via that device.

2. Seizure and Examination - Common Law Powers

2.1 The common law of Scotland operates no differently in relation to the seizure of a digital device by a police officer in the course of an investigation to any other item which is reasonably suspected to be evidence in a police investigation or incident.

2.2 The same applies when it comes to examination of the 'contents' of any such device. A digital device can be regarded as being the electronic equivalent of a briefcase or filing cabinet, where the device is often protected by some sort of barrier or lock which requires a PIN or password to access its 'contents'.

2.3 Therefore, if a police officer in the execution of a lawful power seizes a digital device, the law allows for the examination of that device for information held within.

2.4 The extent of the current common law power of seizure in Scotland (including subsequent powers of examination) will be guided by what is said by the Scottish courts in instances where challenges have been mounted to the use of such powers

Police Scotland will be guided by judicial precedent but recognises that each judgement will be 'fact specific' and that caution requires to be exercised in the broader application of general principles from such judgements. Any decision regarding admissibility is determined by the Courts, with the common law having a degree of adaptability which guides law enforcement as to what is permitted and deemed lawful.

2.5 Where evidence has been recovered as a result of actions for which there is legal authority, then that evidence will be admissible subject to any other legal rules which may apply.

3. Seizure and Examination - Statutory Powers - Accused / Suspects / Temporarily Detained Persons (Powers of Search)

3.1 A search will be lawful where there is a statutory power, a warrant conferring such a power or a power at common law. Section 47 and 48 the Criminal Justice (Scotland) Act 2016 permits a police constable to search any arrested person or seize any item in their possession whether or not they have been charged with an offence.

3.2 A list of statutory powers of search of the person includes, but are not limited to;

- Section 47 Criminal Justice Scotland Act 2016 – Search on arrest and charge
- Section 48 Criminal Justice Scotland Act 2016 – Search on arrest
- Section 47 Firearms Act 1968 (Firearms)
- Section 23 Misuse of Drugs Act 1971(Drugs)
- Section 60 Civic Government (Scotland) Act 1982 (Stolen property)
- Section 4 Crossbows Act 1987 (Crossbows)
- Section 11 Protection of Badgers Act 1992 (Evidence of commission of an offence under that Act)
- Section 101 Conservation (Natural Habitat etc.) Regulations 1994 (Evidence of commission of an offence under that Act)
- Section 4 Wild Mammals Protection Act 1996 (Evidence of commission of an offence under that Act)

- Schedule 7, Terrorism Act 2000

Relevant Case Law

3.3 In *Rollo –v -HMA* (1997) JC 23, the defendant appealed his conviction on the basis that a digital device (a Sharp Memomaster 500) which had been seized under a search warrant issued under Section 23 Misuse of Drugs Act 1971 did not constitute a 'document' and therefore the examination was inadmissible. The Court found that access to certain information contained in the device (comprising a list of names and telephone numbers) was protected and required the use of a password (which police officers guessed). The High Court of Justiciary on appeal observed the essential element of a 'document' (for the purpose of the search under section 23 of the Misuse of Drugs Act 1971) to be something that contains recorded information of some sort and that a store of recorded information is not to be deprived of qualifying as a 'document' because it is protected in some way against unwanted access, deeming electronic security methods (passkey) as no different from a lock on a locked diary.

3.4 As a matter of general proposition, where a lawful power of search exists, the power of search enables a police officer to search for an item, seize it and examine it, *J.L. & E.I. -v- HMA (2014) HCJAC 35.* This case concerned an appeal against the Sheriff's decision to admit evidence obtained as a result of the interrogation of a mobile phone seized from a person detained under section 14 of the Criminal Procedure (Scotland) Act 1995. The data subject to challenge was a text conversation contained within an iPhone 5 in digital format. The stated grounds for appeal were that the police officers had no authority to examine the mobile telephone without either seeking permission or alternatively seeking a warrant. In the course of the appeal it was argued that the iPhone 5 device in question was a ''Smartphone'', a ''portable computer'' and was able to provide access to email, personal banking, health records, still images, moving images, audio files, personal calendars and was a ''living filing cabinet'' and the appellants ''private cyber-space'' for which there was no authority to examine.

3.5 The High Court of Justiciary stated that

'A power of search of the person comprehends looking for an item, seizing it and examining it. Accordingly if a police officer has lawfully arrested a person they may in exercise of the common law power of search following an arrest, take possession of the person's jacket or handbag, look inside the jacket pocket or handbag and on finding for example a diary, examine the entries made in that diary with a view to these entries forming a basis for further inquiry or being admitted as evidence in future criminal proceedings'.

'*The section 14(7) power of search used in this case includes power to examine. What will be required for the effective examination of a particular item will depend on the nature of that item and what is the nature of the information which it is hoped to elicit from the examination. For all that we were told, in the present case, examining the iPhone 5 involved little more than connecting the device to a power supply, switching it on and touching the appropriate portions of the screen. In our opinion, so doing was clearly within the powers conferred by section 14(7)'.*

There was found to be no speciality attributed to the article recovered simply because it was an electronic device, namely an iPhone 5, with the court not being satisfied that there was any illegality or irregularity in recovering the stored data which was contained within the device.

4. **Device Seizure and Examination - Victims and Witnesses**

4.1 The authorities to take a digital device for the purpose of examination from a victim or witness are; where consent is provided; where there is a warrant; or, where there is urgency (common law power).

4.2 The duty of a constable is outlined in legislation. The requirement this legislation imposes is also a consideration in actions taken by police officers (discharge of the general duty of an officer under Section 20 of the Police and Fire Reform Act 2012).

'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'.* 4.3 Additionally,Section 164 of the Criminal Justice and Licensing (Scotland) Act 2010 Code of Practice provides that the police have an obligation to pursue all reasonable lines of enquiry and to record, retain, review, reveal and where appropriate provide all information which may be relevant to the Crown. 4.4 Urgency is unique to the individual circumstances encountered. The general considerations for urgency would normally involve, a reasonable belief that a device contains evidence in circumstances where other legal authority (consent / warrant) are not reasonably achievable. The case should be sufficiently serious and apply only where necessary, proportionate and in the interests of justice to do so. Failure to act urgently, would likely result in the loss of life or loss of evidence. The disposable nature of digital evidence is such that urgency is likely to be a particular consideration. In such cases officers may consider common law powers of seizure. Such actions would still have to accord with other relevant applicable principles such as Article 8 of ECHR. 4.5 It may therefore be the case that seizure of a device at common law from a victim / witness may be justified in certain cases, if there is adequate 'urgency' to justify the action. This would require due regard to the specific facts and circumstances encountered at that time. 4.6 Where it is assessed that the device contains evidence that is required, a warrant is needed unless urgency applies. 4.7 Where urgency and warrant do not apply, police can only take a device for the purpose of examination with the consent of the victim or witness. 4.8 The admissibility of evidence is a matter for the court to decide having considered the evidence, and the specific facts and circumstances of the case and fairness to

		the accused of the approach taken. The courts decisions can inform and guide law enforcement activity. **5. Device Seizure and Examination - Other Device Owner / User – Deceased / Missing Person / Other.** 5.1 This includes any set of circumstances where the owner (or person entitled to possession of the digital device) cannot be identified or classified as a victim, witness, suspect or accused and thereby consent cannot be obtained. 5.2 In such circumstances, and in the absence of any other powers, the power of seizure and examination requires justification under common law and in discharge of the general duty of an officer under Section 20 of the Police and Fire Reform Act 2012. Such actions would still have to accord with other relevant applicable principles such as Article 8 of ECHR. Officers may consider using such powers where necessary, proportionate, in the interests of the public/individual's interests, in the interests of justice or where there is an urgency as failure to do so could result in a compromise to an individual's right to life or likely result in the loss of evidence and/or allow the ends of justice to be defeated. **6 Data Processing** 6.1 Authority to take a device can be by consent, statute, common law, or warrant. Any subsequent processing of recovered personal data is permitted by the Data Protection Act 2018 (the Act). 6.2 Law Enforcement Processing is under Part 3 of the Act, and sets out principles for data processing. The first principle - that the processing must be lawful and fair - is detailed in Section 35, with 35(2) making provision for processing where there is a basis in law for either (a) the data to be processed by consent (not to be confused with any consent relied upon for seizure), or (b) the data to be processed because it is necessary to perform a task for law enforcement purposes.

		6.3 In the case of data from a digital device police rely on Section 35(2) (b), with basis in law being provided by Section 20 of the Police and Fire Reform Act 2012 (duties of a constable) and Section 164 Criminal Justice and Licensing Scotland Act 2010 Code of Practice (obligation on police to pursue all reasonable lines of enquiry and to record, retain, review, reveal and where appropriate provide all information which may be relevant to the Crown). 6.4 There is likelihood that there will be sensitive data – that is to say personal data revealing racial or ethnic origin, political opinion etc. – amongst the data recovered from a device. This is referred to as sensitive processing and Section 35(4) and (5) of the Act outline requirements for such processing. Police Scotland meet the requirements by virtue of (i) The processing being strictly necessary for a law enforcement purpose; (ii) The processing meeting at least one condition in Schedule 8 of the Act, principally; 1 – the processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and is necessary for reasons of substantial public interest 3 - the processing is necessary for protecting individual's vital interests; 4 - the processing is necessary for the safeguarding of children and individuals at risk. (iii) At the time of the processing there being in place an Appropriate Policy Document (APD), namely the 'Law Enforcement Appropriate Policy Document' publicly available on the Police Scotland web site. 6.5 All data processing is compliant with the Act. **7. ECHR** 7.1 The European Convention on Human Rights is a consideration which underpins any decision made by Police Scotland.

		7.2 Article 5, the right of liberty and security of person, is a qualified right meaning its operation can be limited in certain circumstances provided for by the law. Article 6, the right to a fair trial or hearing, on the other hand, is an absolute right. The seizure and examination of digital devices, if carried out properly should not unlawfully infringe on an individual's Article 5 or 6 rights. 7.3 The examination of digital devices is likely to infringe upon an individual's Article 8 right to respect for private and family life however; this is not an absolute right. Infringement of Article 8 rights concerning a victim, witness, suspect or accused is permitted if that infringement is in '*accordance with the law, necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others'*. 7.4 'Necessary' for the purposes of Article 8, means the interference must correspond to a pressing social need (such as the administration of justice) and be proportionate to the legitimate aim pursued. 7.5 The examination of digital devices in accordance with the law pursues a legitimate aim and is necessary to ensure that the Police have adequate and reasonable powers for the prevention, investigation and detection of crime. 7.6 The seizure and examination of digital devices ought to be seen in the context of being part of the role of the Police, and its protection of human rights, in particular Article 2. This process may protect the public from risk, whether from themselves or others via seizure and examination of a digital device which might materially assist in the speedy location of a missing person or dangerous individual. Similarly Articles 5 and 6, where the product of such examination supports the investigation of crime including yielding exculpatory evidence which in some circumstances perhaps results in the halting of a protracted investigation or criminal trial. This can be seen as being in recognition of a person's rights under Articles 5 and/or 6. 7.7 Digital forensic examination can also impact upon the exercise of an individual's rights under Article 10, Right to freedom of expression. This would not be by virtue

		of the data reviewed but would arise in consequence of the effective 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 should be with due regard to the necessity and proportionality within the circumstances of the investigation. In terms of freedom of expression (Article 10), the rapid return of a digital device might enable an individual to resume their communication and expression. 7.8 To protect these rights, in every circumstance examinations require proportionality, necessity, legitimacy and relevance which must be recognised and guide police activity. It is a fundamental part of a police officer's decision-making processes to have regard to the foregoing principles and to act in accordance with them. 7.9 These Articles along with other legislative requirements impose obligations upon law enforcement to protect life, to prevent and detect crime and to maintain order whilst acting within the existing legal framework.
Q12	Describe the purpose of the processing (Refer to guidance **Note 5**)	All seizure and Triage using Digital triage devices - Kiosks will be strictly only for a policing purpose, in accordance with training and the associated 'Principles' document. Kiosks will only be used in cases where the evidential relevance of the device is unknown, but there is believe that a reasonable line of enquiry may be progressed via its examination. 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 Digital Forensic Hubs and reduce submission to hubs.

		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 existence of evidential content which may expedite investigations and detections. Only devices of evidential worth are submitted to Digital Forensic Hubs, thus allowing swifter evidence identification and criminal justice process. This permits increased prevention and detection of crime, reduction in harm and disorder and allows hubs to focus on high priority activity and evidence recovery. Resource saving and reduced data processing; 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. Allowing Digital Forensic Hub staff to focus their time and forensic tools on more high priority complex examinations requiring their higher skill set. The taking of contemporaneous notes. A contemporaneous note refers to notations made (pen and paper / Police Scotland official notebook) by the reviewer / enquiry officer for use in association with the investigation in question for example if during triage of a suspects phone, evidence is recovered that officer wishes to quote to the suspect verbatim during interview, a benefit being the early identification of evidence. Guidance in relation to such notes is made within the associated toolkit requiring officers to lodge any notes taken on paper making them subject to production processes (Audit) retention policy, locatable and secure. If noted within an officers

		notebook this would be again subject to the protections, audits function and retention periods associated to note books <u>Benefit to others</u> The return of devices to owners where the triage showed that the device does not contain evidence. Such a device returned to the owner post triage means no copying of the data within the device as is currently required (at a hub) to facilitate an assessment of each device seized. Focused Triage, allowing investigators to target specific, relevant areas of the device, for example, text messages, photographs etc., thus minimising intrusion into personal data. 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 currently submitted to Digital Forensic Hubs potentially 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 guidance **Note 6**)	High Risk Processing. The prevalence of Mobile phone / device use within the communities 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 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 some of this 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'. within a date range or using 'key word' search facilities 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; Examples of data include but are not limited to • Device information: Phone number, IMEI, IMSI, MEID, ESN, MAC ID • Phonebook – Contact Name and Numbers • Call Logs • Text and picture messages • Videos and Pictures (in some cases with GeoTag-location info) and creation • Date and time • Audio files • Emails and Web Browsing Information • GPS and location information • Social Networking messages and contacts • Deleted data – call logs, messages, emails • PIN lock and pattern lock

		• Attached media or memory card data (pictures, files, app data located on media card) • Wireless networks connected to the device The data will be assessed but not removed from the device. Contemporaneous notes may be taken by officers. A contemporaneous note refers to notations made (pen and paper / Police Scotland official notebook) by the reviewer / enquiry officer for use in association with the investigation in question for example if during triage of a suspects phone, evidence is recovered that officer wishes to quote to the suspect verbatim during interview. Guidance in relation to such notes is made within the associated toolkit requiring officers to lodge any notes taken on paper making them subject to production processes (Audit) retention policy, locatable and secure. If noted within an officer's notebook this would be again subject to the protections, audits function and retention periods associated to note books. Sufficient personal details to identify the Police Officer or member of Police Staff conducting the triage will be recorded by the Cyber Kiosk. The operator will be aware that their details are stored and all their activity on the Kiosk is auditable.
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 removed 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 include anyone who has created data on the device including the user and anyone who has interacted with them via the device enabled functions 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 • the exact role of the other organisation in the processing of the data?	No. No other organisation (including the manufacturer) will process in any way / view any of the data or devices subject to triage. system.
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) - N/A
Q23	What training will be provided for individuals: • Within Police Scotland • Partners • Contractors/subcontractors	All users of the Digital Triage Device - 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. The course is made up of the modules designed by the manufacturer for effective operation of the system but also has a module dedicated to understanding and ensuring compliance with requirements and processes of Police Scotland and Legislation including Human Right Implications Necessity, proportionality, relevance etc.

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, SyOps (contained within Toolkit at Appendix D) PSoS – 'Digital Device Examination, Principles' DPIA, EqHRIA Cellebrite – Kiosk User Manual. Public Information Leaflet Public Frequently asked Questions.
Q25	Data Flow analysis – (Refer to guidance **Note 9**)	

Part 3 – Assessment of Necessity and Proportionality

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

	Requirement – The Data Protection Principles		**Comments**
Q26	**DPA 2018** **1st Principle** **Sections 35 & 42** **Schedule 8**	**Lawful/Fair:** (Refer to guidance **Note 10**) • Is the processing based on consent and if so, why? • If the processing is necessary for the performance of a task? If so, provide details of the task.	The processing is not based on consent. All processing is under Section 35(2) (b) DPA 2018 – necessary for the performance of a task. Reliance is upon Section 20 of the Police and Fire Reform (Scotland) Act 2012, and Section 164 of the Criminal Justice and Licensing (Scotland) Act 2010 Code of Practice, for the legal basis. Section 20 of the Police and Fire Reform (Scotland) Act 2010 provides the general duties of a constable:

			(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 164 of the Criminal Justice and Licensing (Scotland) Act 2010 Code of Practice provides that the police have an obligation to pursue all reasonable lines of enquiry and to record, retain, review, reveal and where appropriate provide all information which may be relevant to the Crown.
		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. The processing is **not** based on consent. The processing is strictly necessary for law enforcement purposes and necessary for the exercise of police functions as laid down in Section 20 of the Police and Fire Reform Act 2012: (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 164 of the Criminal Justice and Licensing (Scotland) Act 2010 Code of Practice provides that the police have an obligation to pursue all reasonable lines of enquiry and to record, retain, review, reveal and where appropriate provide all information which may be relevant to the Crown. The following Schedule 8 conditions are relied upon: Below are the principle schedule 8 conditions (1-4) which cover instances where a kiosk use will process sensitive data with an example (s) for each 1This condition is met if the processing— (a)is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and Police Fire and 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 (b) is necessary for reasons of substantial public interest. Devices seized in connection with the investigation of crime, for example, a Counter Terrorism or Serious Organised Crime Investigation or otherwise for the purposes of the prevention / detection of crime.

			Protecting individual's vital interests (3) This condition is met if the processing is necessary to protect the vital interests of the data subject or of another individual. An example would be a high risk missing person where crucial data as to the potential location and ensuring their safety may be obtained; however, there may be other circumstances where data on a mobile device is necessary to protect vital interests. Safeguarding of children and of individuals at risk 4(1)This condition is met if— (a)the processing is necessary for the purposes of— (i)protecting an individual from neglect or physical, mental or emotional harm, or (ii)protecting the physical, mental or emotional well-being of an individual, (b)the individual is— (i)aged under 18, or (ii)aged 18 or over and at risk, A range off public protection enquiries regarding the protection of children subject or potentially subject to harm qualify in this regard- evidence of; assault / sexual offences etc. and the investigation of missing children. (c)the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and (d) the processing is necessary for reasons of substantial public interest. Police Fire and 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 (2)The reasons mentioned in sub-paragraph (1)(c) are— (a)in the circumstances, consent to the processing cannot be given by the data subject; Missing / kidnapped (b)in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing; Missing / kidnapped (c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1) (a). Within the legal basis as outlined – examination of the devices of suspects or accused where it is unlikely permission would be given.
Q27	**DPA 2018** **2nd Principle** **Section 36**	**Specified/Explicit/Legitimate:** • State the specific purpose for which the personal/sensitive data will be processed. (Refer to guidance **Note 11**) • Is the data to be used for any other law enforcement purpose? If so what other law enforcement purpose? Is the data to be used for any non-law enforcement purpose? (Refer to guidance **Note 11**) If so: • What is that purpose?	Cyber Kiosk triage is primarily for; The prevention, investigation, or detection of crime or the prosecution of offenders. 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 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, (only where there is a policing purpose) in relation to a police investigation or incident which may not be categorised as criminal, examples; missing persons, death investigations or other circumstances where there is immediate concern for life. Such investigations are undertaken by law enforcement for a law enforcement purpose, to ensure public safety but include a requirement to ensure there has been no

		• Why do you believe that this purpose is not incompatible with the specific reason for which you gathered it?	criminality involved in the disappearance or death. Such investigations therefore qualify as 'for law enforcement purposes' Not all law enforcement processing will necessarily result in the identification of criminal acts or linked to crimes that result in reports to COPFS. (For the avoidance of doubt, all death investigations are subject of report to COPFS). As mentioned previously, in order for a device to be subject to examination via a Cyberkiosk, it will be a production in a criminal case and as such data processing done using a Cyberkiosk will be done for the primary purpose of law enforcement. It is acknowledged that during the course of triage in relation to the specific criminal case in which the device is a production it may be identified that information exists thereon that could be of interest for non-law enforcement purposes, for example in relation to Police Scotland misconduct enquiries. In these circumstances a referral will be made to the relevant Police Scotland department.
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 Principles' guides officers in relation to what is adequate, relevant and not excessive and outlines 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 their 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 only review data which is potentially 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 conjunction 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 within the MI log. (Audit will also be undertaken using the request submission process, Electronic Recording Form (ERF) however this is a separate system).

			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 duration of use, the ID of the person using the kiosk, time/date the kiosk was used, the name of the device being examined 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 system updates, etc. At this time, using enhanced credentials, they will log into the kiosk and recover these logs. The logs will be aggregated at Cybercrime, 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: Complainer Witness Deceased Missing person Not officially accused Officially accused Other

			'Other' refers to other Device Owner / User and includes where the owner cannot be identified or classified as above and as a result where consent cannot be obtained. As the category 'Other' can be reviewed as an audit parameter during audit processes the types of enquiry that fall within this bracket and the associated Case management form (ERF) can be reviewed and part of any dip sampling process.
		• 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 is removed from the kiosk on each occasion it is downloaded. This information is no longer retained on the kiosk itself. It is then held centrally at cybercrime in line with the above Record Retention SOP.

			The audit data does contain personal data which 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. This data will be extracted by Cybercrime staff using encrypted devices, erased 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. This data will be anonymised removing all reference to the individual officers prior to any circulation or publication of management information data. 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. A new post of Data and Quality Assurance Manager within Cybercrime has been created and filled and this individual will ensure compliance with this 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 retention policy 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. Kiosks are situated in rooms in police Scotland estate. Only investigating officers and kiosk operators will view a device triage. Contemporaneous notes may be taken by officers. A contemporaneous note refers to notations made (pen and paper / Police Scotland official notebook) by the reviewer / enquiry officer for use in association with the investigation in question for example if during triage of a suspects phone, evidence is recovered that officer wishes to quote to the suspect verbatim during interview. Guidance in relation to such notes is made within the associated toolkit requiring officers to lodge any notes taken on paper making them subject to production processes (Audit) retention policy, locatable and secure. If noted within an officers notebook this would be again subject to the protections, audits function and retention periods associated to note books Kiosks will only be located within Police Offices. Their location has been determined and selected so as to ensure privacy during any triage process.

			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’ 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 from the current mobile device. The screen does not lock itself if left unattended. Each use of the Kiosk will produce associated Management Information (MI). MI Data retained / produced by the kiosk, (Time, date, user etc.) can only be accessed by Supervisory Cybercrime Staff. 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. MI data will remain within the secure, password protected system and be subject to Force retention policy of MI data.

Part 4 – Measures Contributing to the Rights of the Data Subjects			
In this section, assess how data subjects' rights will be protected.			
Q32	**DPA 2018 Section 44**	**Information – Controller's general duties:** (Refer to guidance **Note 14**) • How will data subjects be made aware of what is happening to their data? • Is it the intention to withhold any of the information listed under the exemptions? • If so, how do you propose to record your decisions?	Due to its less intrusive nature and quick turnaround officers will seek to use a kiosk wherever possible provided the investigation meets the criteria for Kiosks use. On such occasions the individual will be informed of this intention supported by the information products outlined below which will be provided and will be publicly available via the PSoS Website. A public information document / leaflet has been drafted and will be provided to all victims and witnesses (can also be given to suspects / accused) from whom a digital device is obtained/seized. This will provide information on the Kiosk and general digital device forensics. A flow process and a set of Frequently Asked Questions (FAQs) will be maintained, updated and published on the Police Scotland Internet and will advise subject's regards their data. This advice / documents will be published on the force internet and intranet. When consent is utilised for obtaining the digital device then Police Scotland will capture a signed consent within the statement of the victim/witness and in doing so will use an agreed form of words as follows: '*I understand that I do not have to provide consent. The Digital Device Consent Public Information Leaflet has been read to/by me and I can*

			confirm that I understand this information. I do/do not give my consent for Police Scotland to take my device for the purpose of examination. This will be taken in conjunction with the provision of the aforesaid Information Leaflet, which will include further details around rights and processes in the form of a FAQ. Police Scotland has a Law Enforcement Privacy Notice published on the PSoS website as below for the information of the public. Police Scotland processes a variety of personal data, including but not only for law enforcement purposes. The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 require us to be more transparent in explaining how we process that data, including what we do with it, how long we intend to keep it, and on what legal basis. Police Scotland do not intend to withhold details of what will happen to an Individuals device including that it may be subject to Triage process. Sufficient personal details to identify the Police Officer or member of Police Staff conducting the triage will be recorded by the Cyber Kiosk. The operator will be aware that their details are stored and all their activity on the Kiosk is auditable. Officers are made fully aware of this during Module 1 of Training which covers Human Rights and Data Protection compliance including clear intention and requirement to audit use of the Kiosk.
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	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 Digital Triage 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

		the processing of subject access requests?	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 or held within officer notebooks and subject to record retention policy and note book care proeedures and management. 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. It is antisipated that Audit data will be published on the PSoS public Internet site. 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. Information Management process requests when personal data is being processed as evidence or potential evidence as per their 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 inaccurate data? • What guidance will be in place to deal with the requirements under Section 48?	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 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 : • 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.	Section 62 requires that a controller (or, where personal data is processed on behalf of the controller by a processor, the processor) must keep logs for at least the following processing operations in automated processing systems. (a)collection; (b)alteration; (c)consultation; (d)disclosure (including transfers); (e)combination; (f) erasure. Kiosk Functionality only exists for A- collection and D – disclosure With regard the other requirements… Alteration. The Kiosk cannot alter device Data. Consultation. – The kiosk offer no facility to consult on device data Combination – The kiosk does not have any capability regard combination of device data. Erasure – The kiosk cannot delete device data 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 Digital Triage Device - Kiosk will record who the users of the system are and will Digital Triage 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 electronic recording form (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 displayed on the kiosk will not be encrypted.
		• Will the data be pseudonymised? If so how?	Any data displayed on the kiosk will not be pseudonymised.
		• How will the data be protected against risk of loss, confidentiality, availability and integrity?	Any data displayed 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 displayed 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?	Recruitment 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 and Seeking Views The course is made up of the modules designed by the manufacturer for effective operation of the system but also has a module dedicated to understanding and ensuring compliance with requirements and processes of Police Scotland and Legislation including Human Right Implications Necessity, proportionality, relevance etc.
		• 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 (including Syops), Digital Forensic examination, Principles.
Q38	**Consultation**	**Consultation Requirements:** (Refer to guidance **Note 19**)https://spi.spnet.local/policescotland/guidance/Force Forms/Police-Scotland/Data Protection Impact Assessment - Law Enforcement	The following groups (membership outlined below) were established In June / July 2018. This Impact assessment has been subject of review and consultation via these groups and National Independent Strategic Advisory Group (NISAG) who have contributed to its production.

		Processing - Guidance.doc - _Hlk507408266	Stakeholder Group ○ COPFS ○ HMICS ○ SPA ○ SPA Forensics ○ Information Management ○ Scottish Police Federation ○ PSOS Information Management External Reference group ○ Information Commissioner's Office (ICO) ○ Scottish Human Rights Commission (SHRC) ○ Privacy International ○ Open Rights Group ○ Scottish Institute of Policing Research (SIPR) ○ Academia ○ Rape Crisis Scotland ○ Mr. Aamer Anwar ○ Victim Support (Scotland) ○ NHS Gender Base Violence – Lanarkshire ○ ASSIST On 24th May 2018 a senior management facilitated demonstration of the Kiosk was delivered at Victoria Quay to COPFS, ICO, and the Scottish Executive were represented. A demonstration was provided to Murdo MacLeod QC - Senior Counsel to assist him in the preparation of his Opinion on the legality of 'Cyber Kiosks'. The Scottish Parliament, Justice Sub-Committee on Policing 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 13 September and 14 November 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 Out with 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.	Police Scotland has considered whether the new Investigatory Powers Act 2016 will have any impact on the processing described above with Kiosks. As this legislation relates primarily to covert activity and the triage of digital devices using a Kiosk is exclusively an overt activity it does not apply. This is because from the point of seizure the device has been isolated allowing no access to mobile data or Wi-Fi and as such it is not possible to receive or send communications. This is a process known as "Dead box Forensics". As such the device does not form part of a communications network. This therefore does not involve intercept of data. This position is supported by COPFS and Police Scotland's Central Authorities Bureau, who are responsible for processing Investigatory Powers Act 2016 applications across Police Scotland. RIPA and RIP(S) A have also been considered and do not impact on use of the Kiosks.
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	No

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

Part 5 – continued			
Q43		**Article 4: Prohibition of Slavery or Forced Labour** Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to be not held in servitude or forced to perform compulsory labour? For the avoidance of doubt, this is an absolute right; the following are excluded from being defined as forced or compulsory labour:	No

		• Work done in ordinary course of a prison or community sentence; • Military service; • Community service in a public emergency; and normal civic obligations	
Q44		**Article 5: Right to Liberty and Security** Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to be not deprived of their liberty subject to certain limitations? For avoidance of doubt, the following limitations apply when a person is: • Held in lawful detention after conviction by a competent court; • Lawfully arrested or detained for non-compliance with a lawful court order or the fulfilment of any lawful obligation; • Lawfully arrested or detained to effect the appearance of the person before a competent legal authority; • Lawfully detained to prevent the spreading of infectious diseases; • Lawfully detained for personal safety (applies to persons of unsound mind, drug addicts etc.); and • Lawfully detained to prevent unlawful entry into the country or lawful deportation from the country.	No - The practice will assist investigators in identifying relevant information either inculpatory or exculpatory to the enquiry. Kiosk use can 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 basis 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, 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 basis allowing us to lawfully obtain (voluntarily) / seize and examine mobile devices is compromised and has submitted evidence obtained from devices and secured numerous convictions in recent years.

			In his clear and unambiguous Opinion, Senior Counsel confirmed the existence and extent of police officers' powers in this connection and that their exercise complied with the relevant provisions of ECHR.
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. Voluntary submission with informed consent and seizure are the principal means by which an officer will take possession of a device from a victim / witness connected to an investigation. All seizures must be lawful, for a policing purpose and includes devices seized during execution of a search warrant or under legislative provision. 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 basis 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. In his clear and unambiguous Opinion, Senior Counsel confirmed the existence and extent of police officers' powers in this connection and that their exercise complied with the relevant provisions of ECHR.
Q46		**Article 7: Right to no Punishment without Law** Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to not be prosecuted for a crime that was not, at the alleged time of commission, constitute a criminal offence under national or international law? For the avoidance of doubt, this is an absolute right.	No
Q47		**Article 8: Right to Respect for Private and Family Life** Does the project involve new or existing data processing that adversely impacts an individual's right to respect for privacy in terms of their private and family life (subject to certain qualifications)? For the avoidance of doubt, the qualifications are: • Legal compliance; • National security; • Public safety;	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 Digital Forensic 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 devise triage across multiple investigations as opposed to individual investigating officers.

		• National Economy; • Prevention of crime and disorder; • Protection of public health and morals; • Protection of rights and freedom of others.	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 Forensic Hubs. The 'Digital Forensic Examination, Principles' 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. Legitimate - Acting with a legitimate aim, for a policing purpose and with the associated reasonable belief as outlined are the grounds on which the power of seizure described above and digital investigation are authorised. It is only with this legitimate aim that an officer should seize and subsequently review a device.
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?	No

		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.	
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 right to marry and found a family subject to certain restrictions? For the avoidance of doubt, the restrictions are regulated by law so long as they do not effectively take away the right , e.g. age restrictions apply	No
Q52		**Article 14: Right to Freedom from Discrimination** Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to be treated in a manner that does not discriminate the individual from others subject to certain restrictions? For the avoidance of doubt, this right is restricted to the conventions as set out in the European Convention	No

		of Human Rights 1950; the grounds for discrimination can be based on: • Sex • Race • Colour • Language • Religion • Political persuasion • Nationality or social origin • Birth • Other status	

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

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

Risk(s) identified to the rights and freedoms of data subjects	**Likelihood and severity score**	**Mitigation(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
There is a risk that without adequate safeguards personal data held on a digital device subject to examination using a Kiosk could be unlawfully accessed.	**Likelihood - Low (2)** **Severity - Medium. (3)** **SCORE - 6**	**- Existing Legal Basis** **-Certified Training** **- Kiosk Toolkit guidance** **- Audit Function** **- Robust Governance processes**	**Reduced -** **Likelihood - Very Low (1)** **Impact - Medium (3)** **The impact cannot be changed.**	**YES** **The mitigations placed on kiosk capability and the other activity outlined in the Mitigation section in this risk will greatly reduce the possibility of unlawful, unjustified access,**

		(including supervisor sign off) - Compliance Check / Dip sampling - Specified Users unique log in required. Specified officers are trained in the policy, practice, procedure supporting use and the considerations in terms of legal basis, justification, necessity and proportionality. All officers on Foundational traning courses are also tranined in Data Protection Act 2018 and ECHR considerations. Given the volume and personal nature of the data potentially held, accessability is high however potential for modification and deletion are low.	SCORE - 3	destroying, modifying, deleting or mishandling personal information. The guidance and processes take full acount of ensuring lawful data access in terms of necessity, proportionality relevance etc. The legal basis as outlined in this document has been deemed accurate and lawful.

There is a risk that without adequate safeguards personal data held on a digital device subject to examination using a Kiosk could be unlawfully modified or deleted.	Likelihood - Low (2) Severity - Medium. (3) SCORE - 6	The Kiosk is designed to offer View Only access to data with no ability to remove device data.	Reduced - Likelihood - Very Low (1) Impact - Medium (3) The impact cannot be changed. SCORE - 3	YES Mitigations placed on kiosk capability and the mitigations outlined in this risk will greatly reduce the possibility of unlawful, unjustified access, destroying, modifying, deleting or mishandling personal information. The guidance and processes take full acount of ensuring lawful data access in terms of necessity, proportionality relevance etc. The legal basis as outlined in this document has been deemed accurate and lawful.
Article 8 – There is a risk that without appropriate safeguards the use of Kiosks to triage data held on a Digital Device could breach an individuals ECHR Article 8 Right yo Respect for Private and Family Life.	Likelihood - Very high (5) Severity - high - (4) Score: 20	As per any enquiry or investigation involving digital media there is an element of collateral intrusion. This will be managed using developed and established policy, procedures,	Reduced - This right is qualified and infringment can be permitted if that infringement is in accordance with the law, to preserve life or it is necessary in a democratic society for the prevention of disorder or crime.	YES The impact is justified, compliant and proportionate within the bounds of police investigations. All trained kiosk users are bound by Guidance, 'Principles' and the Data Protection Act.

		practices, training and guidance. At the point were it is established there is evidential value the triage should cease and the device will be sent to Cybercrime. Without lawful authority this risk would be graded as 20, given the volume and personal nature of data potentially held.	The legal basis as outlined in this document is lawful permitting infringement of this right. The ability of the Kiosk to target specifically the area in which the data is situated in the device if known and training to facilitate this reduces the risk. Likelihood - Medium - (3) Kiosk are situated within police offices were there is no access to the public and in rooms suitable to reduce the ability of others to see the data restricting it to only those engaged in the examination. Impact - Medium (3) SCORE - (9)	The guidance and processes take full acount of ensuring lawful data access in terms of necessity, proportionality relevance etc. The legal basis as outlined in this document is lawful.
Article 6 – There is a risk that the use of Cyber Kiosks could impact on the evidence available to	Likelihood - Very low(1)	There is currently no threat of engaging this right	Eliminated - The impartial interrogation of data by Police is with a view to	YES

COPFS and impact on the right for any accused to a fair trial.	Severity - Very High (5) Score : 5	re Kiosk use as the legal framework for the seizure and review of devices exists.	establishing the facts and circumstances of any investigation. As such the kiosk use may equally identify data that exculpates an individual as incriminate them protecting this right. The guidance and processes take full acount of ensuring lawful data access in terms of necessity, proportionality relevance etc. The legal basis as outlined in this document has been deemed accurate and lawful. Likelihood - Very Low (1) Severity - Medium (3) SCORE : 3	If this changes this would significantly impact this right and require full review and change of process and police actions.
Article 10 – There is a risk that an individual's right to freedom of expression is impacted by having no access to the device that is currently with police.	Likelihood - High (4) Severity - 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	Kiosk use does not affect this right. It is the associated deprival of an individual device which engages and infringes this right. Provided that the acquisition of the device by police is lawful	Yes Providing the legal frameworks exists – The right is not removed entirely merely in relation to the opportunities within that device provide the

		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.	**including voluntary from the witness, including informed consent and /or lawfully seized as outlined in this document and the associated guidance the associated infringement is lawful. Guidance regards necessity, proportionality etc. throughout the associated document mitigates significantly against the risk that police could acquire a device unlawfully.** **Likelihood - Low (2)** **Severity - Very Low (1)** **SCORE : 2**	**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:	**Approved by Information Assurance**
Signature:	**By Email**
Date:	**11/11/2019**

Strategic Information Asset Owner:

Signature:	**ACC Angela McLaren (signed copy held by Information Assurance)**
Date:	**15/01/2020**