SCOTTISH POLICE AUTHORITY

POLICE SCOTLAND
POILEAS ALBA

Division	SCD	**Department**	SCD, Cybercrime
File Path Record			

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

This form is to be completed in accordance with the instructions as set out in the EqHRIA SOP. A step-by-step guidance on how to complete this form is also available. You can access relevant sections of the EqHRIA Form Guidance by hovering over headings in this form and following the instructions.

Name of Policy / Practice (include version number)	Digital Triage Device (Cyber Kiosks)
Owning Department	SCD, OCCTU, Cybercrime

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

Why the technology is required.
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.

Purpose of this technology
The objective of Kiosks is to allow Police Scotland to preview mobile devices in a focused, precise and less intrusive manner than is currently available whilst establishing if those devices contain potential evidence. This early identification of evidence enhances operational effectiveness and augments criminal justice processes before subsequent onward submission to Digital Forensic (Cybercrime) Hubs. Where no evidence is recovered the device can be returned to the owner.

A Digital Triage Device (DTD) or 'Cyber Kiosk' is a computer terminal which facilitates the viewing of data on a device in a targeted and focused manner,

only looking at what is necessary. It does not record or retain any data from the mobile device. This Kiosk examination quickly identifies whether a device holds information relevant to an investigation. This process is only performed by specially trained staff, in the region of 410 officers - 10 per Kiosk, working to specific, identified parameters, e.g. text messages, photographs, emails, between specific people and a specific date range. The current Kiosk configuration only provides a viewing facility.

The introduction of 41 Cyber Kiosks will increase digital forensic capabilities for Police Scotland by offering a local triage point in the examination process for some devices without the requirement for submission to a Digital Forensic Hub.

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

No device data is retained by the Cyber Kiosk. The equipment has the capacity to copy data however this facility is disabled and cannot be enabled by Kiosk operators. There is no intention to review functionality with a view to enhancing Kiosk capability at this time. Any change in the functionality of the devices, to be anything other than view only, will require a resubmission of an associated DPIA and EqHRIA.

Whilst the Kiosk is also capable of triaging some other devices such as Secure Digital (SD) cards or USB Memory Sticks, the use of a Kiosk to triage anything other than a mobile phone, tablet and any **associated** memory or SIM card is **not permitted.** Any change in the functionality of the Kiosk to include other items will require an update of an associated DPIA and EqHRIA as appropriate.

Associated guidance in the form of a 'Toolkit' and 'Digital Device Examination Principles' have been developed to give all police officers and police staff including Kiosk operators, guidance on the use of Kiosks and the authorisations and requirements of Kiosk use.

Intended outcomes:

- The swifter return of devices to owners where the triage shows that the device does not contain evidence.
- 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.
- 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.
- Allowing Digital Forensic Hub staff to focus their time and forensic tools on more high priority complex examinations requiring their higher skill set.

Note: The technology provided by Cyber Kiosks is not new to Police Scotland and has been utilised within the dedicated Digital Forensic (Cybercrime) Hubs for some considerable time. It is an additional process within existing digital forensic structure to eliminate devices of no evidential value from police

investigations. The Kiosk is essentially a simplified version of the technology used within hubs with appropriately limited capabilities. This project imbeds a simplified initial examination tool within Territorial Divisions in order to quickly and efficiently eliminate non evidential devices and data, minimising delays and offering the considerable benefits detailed above.

1B. Outline the Legal Basis for use. The test for 'in accordance with the law' is key for human rights assessments, not only to establish the necessity and proportionality of a measure, but also to give the public clarity and foreseeability about their rights.

The legal basis for the examination of digital devices was explored by Senior Counsel, Murdo MacLeod QC, whose opinion was sought in relation to legal basis for use of Digital Triage Devices (Cyber Kiosks). It is recognised that the legal basis, principles and considerations in respect of digital device seizure and examination regarding Cyber Kiosks within that Opinion are relevant to general digital device seizure and examination.
That opinion is;
'My principal conclusion is that there is a lawful basis for the use of cyber Kiosks'.

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 actions accord with the law as it is understood to be.

The powers outlined herein apply only to the contents of a device, commonly referred to as 'stored data' and not 'online data' accessed via that device.

Common Law Powers
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.

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'.

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.

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.

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.

Statutory Powers - Accused / Suspects / Temporarily Detained Persons (Powers of Search)

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.
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
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 1971did 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.

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.

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.

Victims and Witnesses

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).

The duty of a constable is outlined in legislation and 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'.

Urgency is unique to the individual circumstances encountered. The general considerations that urgency would normally involve include, 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, in the interests of justice and where there is urgency - failure to do so 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.

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.

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.

Other Device Owner / User – Deceased / Missing Person / Other.
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.

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.

ECHR

The European Convention on Human Rights underpins any decision made by Police Scotland.
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 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.

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'.

'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.

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.

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.

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.

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.

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.

The opinion of Senior Counsel in considering Human Rights was noted as follows:

''In terms of satisfying the ECHR test, it seems to me that the scheme for examination of digital devices by cyber Kiosk not only accords with domestic legal requirements but is also "necessary" and "proportionate". It is designed simply to ensure that Police Scotland can more efficiently exercise its existing powers in preventing, investigating and detecting crime. Importantly, the scheme has various safeguards in place such as the need for authorisation, together with the limitations of the Kiosk itself. It seems to me that the scheme would meet Strasbourg's expectations in terms of its accordance with domestic law, its necessity and its proportionality''.

Data Protection
Authority to take a device can be by consent, statute, common law, or warrant. Any subsequent processing of recovered personal data is permitted and governed separately by the Data Protection Act 2018 (the Act).

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.

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).

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;

- 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
- the processing is necessary for protecting individual's vital interests;
- 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.

All data processing is compliant with the Act.

Other opinion
As the Crown Office and Procurator Fiscal Service (COPFS) is responsible for the prosecution of crime in Scotland, the opinion of COPFS is highly relevant in any considerations with regards to the lawfulness of police activity.

It is the opinion of Deputy Crown Agent, Lindsey Miller, COPFS that:

''In order to conduct this "triage" the Digital Device Triage Systems will, as COPFS understands it, carry out a function which is already utilised by the Police Scotland Digital Forensic Hubs to examine information held on a device. That function will simply be carried out at an earlier stage in the investigative process in order to facilitate the quick return of a device to its owner where there is nothing of evidential value.

''It is perhaps of note that Police Scotland Digital Forensic Hubs currently examine thousands of digital devices every year, providing evidence to COPFS which is in turn presented in Court, subject to legal scrutiny, and is often crucial in securing convictions in all types of cases including the most serious and complex''.

''The Police do have powers of seizure and examination which apply irrespective of whether it is a digital device or any other item. Those powers are governed by legal provisions and principles. Where a digital device is seized by Police Scotland and examined then the seizure and examination should comply with the provisions and principles outlined, failing which, any evidence secured will risk being ruled inadmissible by a Court based on it having been secured unfairly. That applies whichever process is used to examine the device, including the use of the Digital Device Triage System''.

Consent

This Impact Assessment has been completed in relation to the Cyber Kiosks and can be read in conjunction with the EqHRIA completed with regards to Police Scotland's enhanced consent capture process.

This assessment will not therefore directly consider consent in every section and makes the assumption that any consent obtained has been so in accordance with the relevant guidance and requirements considered in those 'Consent' assessments and is compliant with the related processes (Digital Device Consent, Public Information Leaflet and Consent Declaration for taking of devices for the purpose of examination).

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

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

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

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

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

4. **Equality Impact Assessment – Consider which Protected Characteristics, if any, are likely to be affected and how.**			
4.1 Protected Characteristics Groups	**4.2 Likely Impact** Positive, Negative or No Impact (Assessment of Low / Medium / High impact)	**4.3 Evidence Considered** (e.g. legislation / common law powers, community / staff profiles, statistics, research, consultation feedback) **Note any gaps in evidence and any plans to fill gaps.**	**4.4 Analysis of Evidence** (Summarise how the findings have informed the policy / practice – include justification of assessment of No Impact)
General / Relevance to All	Positive impact on those whose personal data is processed by PSoS and officers and staff.	The triage of a device will only be undertaken when there is a requirement during a police investigation to review that data for evidential content. That requirement will form an essential part of investigations that must be taken in order for officers to fulfil their duty with regards the investigation of Crime (Section 20, Police Fire Reform (Scotland) Act 2012: (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. Such is the prevalence of devices amongst the public, Kiosks could potentially affect individuals with any protected	**Consultation** 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. <u>Stakeholder Group</u> ○ COPFS ○ HMICS ○ SPA ○ SPA Forensics ○ Information Management ○ Scottish Police Federation ○ PSOS Information Management <u>External Reference group</u>

		characteristic. Existing device examination procedures at Digital Forensic Hubs are already established to fulfil the requirements of evidential capture from devices. In relation to Kiosk procedures, the only protected characteristics which may be disproportionately affected are age, race, religion, sexual orientation and disability although some considerations are outlined in this assessment regard other characteristics. Principle positive outcomes are the reduction in intrusion, reduced data processing, early return of devices to owners where no evidence is recovered and early identification of evidence assisting investigation and thereby protecting communities. This positive impact would be particularly relevant to those communities who rely on their devices to support daily life e.g. • People with disabilities who use their devices for assisting with communication or accessing support from family or friends when required • Young people requiring support and safety through contact with parents or guardians. • Women (who are disproportionally) affected by domestic violence or sexual crimes.	○ 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 demonstration of the Kiosk by senior management was delivered at Victoria Quay to COPFS, ICO, and the Scottish Government 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', and Dr Brindley of Rape Crisis Scotland 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 by Police Scotland in relation to Kiosks.

			The Opinion of Senior Counsel was sought on the matter of legal basis for Kiosk use and is referenced in section 1B. It has been made clear during this engagement that the concerns considered in relation to Cyber Kiosks are not in relation to the principle Kiosk capability and use itself, but rather more general with regard police access to, review, process and management of digital data held within mobile devices. These wider concerns are reflected and considered within this assessment. <u>Training</u> New training of police officers in Kiosk use and train the trainer training has been considered in terms of implications with regard to the upskilling of staff and impact in terms of conditions or work pattern. There is no identified impact in this regard. Training has been completed and a review has been conducted with overwhelmingly positive feedback from the staff trained. Learning points were captured in post training assessment and incorporated in future training events. Module one of training was dedicated to Data Protection, Human Rights implications and requirements of Kiosk use. This was drafted using feedback received during wider consultation, including that of External Reference and Stakeholder Groups. Training was designed and delivered by Police Scotland staff to ensure appropriate importance and consideration.
Age	Medium Impact - Positive	There is potential that this practice impacts upon individuals of particular age ranges. However this introduces opportunity to return devices to owners where no evidence is identified.	There is a potential that this practice impacts more upon individuals of a particular age range due to the generational use, understanding and prevalence of digital devices and associated communications. These devices are more prevalent within those of working age as opposed to the elderly or very

		This positive impact would be particularly relevant to those communities who rely on their devices to support daily life including young people or the elderly requiring support and safety through contact with parents or guardians.	young. A peak 99% internet usage is seen within the age range 16 to 44, this dropping to 44% in the over 75s. (Office of National Statistics, Internet users UK, 2018). The impact upon these demographics is likely to be further impacted by overlap with the age range during which individuals are most likely to come into contact with police during police incidents and investigations. Whilst the impact is recognised, it is accepted as out with police control and subject to change and influence by digital culture, economics, media and other factors. Any formal engagement with a young person (including consent capture) will be subject to the standard requirements; namely parent / guardian / appropriate adult as appropriate.
Disability	Low Impact - Positive	<u>Public</u> Impact of police involvement on the collection of evidence from the device of a protected person may affect them disproportionately due to dependence on their device for support in daily life e.g. communication aids / family support (assisted by applications within) or as a means of contact and therefore security to enable daily living. However this introduces opportunity to return devices to owners where no evidence is recovered. This positive impact would be particularly relevant to those communities who rely on their devices to support daily life including disabled persons that use a device for assisting with communication or accessing support from family or friends when required. Addressing language/communication needs and barriers for people with sensory impairments is considered to be critical	<u>Public</u> As with all impacts, this must be considered with due regard to triage only where necessary, proportionate, justified etc. and as such should be compared with existing processes to identify additional benefits / disadvantage of use. Where there is an increased reliance on the device by an individual, as a result of an identified disability, the benefits of the Kiosk process are significant. Whilst on all occasions every effort will be made to ensure the speedy return of a device - existing process involves submission to a Digital Forensic Hub. A Kiosk provides the opportunity to triage the device immediately, limiting the impact on the individual and providing the opportunity for return if no evidence is found. If evidence is detected, any requirement to deny individuals of their device in these circumstances would consider the seriousness

		to ensuring positive engagement with those affected. The use of Police Scotland's 24/7 translating and interpreting service – including British Sign Language (BSL) and other communication support – will help to mitigate this barrier. Work is underway to improve access to BSL interpreters by enabling front line officers to use an NHS App via a mobile device; this will bring significant improvement in the time taken to facilitate communication with a BSL users and result in a more positive engagement for all involved. Consent capture related EqHRIA also provides details of how language and communication needs of individuals will be met. <u>Police - Kiosk User</u> Potential user accessibility issues to operate equipment effectively due to an existing disability relating to eye impairments or dyslexia.	of the offence and would only be taken if absolutely necessary and no other means were available to capture that evidence. As with existing requirements regarding any formal police engagement (e.g. statement taking), where a disability is associated with reduced mental ability, the examination and consent requirements would be undertaken with the assistance of next of kin and / or an appropriate adult were applicable. It is recognised that every effort will be taken to negate the need for denying the individual access to their device, including considering alternative means to capture the evidence and Police Scotland provision of replacement devices if appropriate and required. <u>Police - Kiosk User</u> The fonts and icons are fixed on the Kiosks by the manufacturer and cannot be adapted or modified. Local solutions will need to be considered dependent on the individual's requirements and would be assessed on a case by case basis. Existing support for users of police systems will be available to anyone who requires access to the Kiosks and may mitigate any potential issues relating to viewing data and operating the Kiosk. N.B. – Currently, no Kiosk user has identified any visual impairment that would impact on their ability to operate under the standard settings.
Gender Reassignment	No Impact	No Evidence available to suggest any impact due to membership of this protected group.	N/A
Marriage and Civil Partnership	No Impact	No Evidence available to suggest any impact due to membership of this protected group.	N/A

Pregnancy and Maternity	No Impact	No Evidence available to suggest any impact due to membership of this protected group.	N/A
Race	Medium Impact – Negative and Positive	<u>Language</u> <u>Public</u> There will be an accepted risk that issues with police communication may arise when engaging with a member of the public for whom English is not a first language. An interpreter may be required to ensure an informed process. <u>Police – Kiosk User</u> Potential that digital data may be in a language which the Kiosk user has limited or no ability to read, understand or translate. <u>Race</u> It has been considered that Race may be an applicable characteristic with regard potential opinion that BME groups are disproportionately affected due to a perceived susceptibility to stop and search that will result in device examination or 'digital stop and search'	<u>Language</u> <u>Public</u> As with existing requirements regarding any formal police engagement (e.g. statement taking), where a language barrier exists, this will be done with the assistance of a suitably qualified interpreter who will also be used to fulfil any requirement regarding informed consent. There is 24/7 availability of Interpreting services including British sign language and other communications support. <u>Police - Kiosk User</u> Where triage of a device identifies use of a foreign language, officers whose first language is English may need to refer to the Interpreting and Translating SOP. Devices requiring an interpreter to assess should not be triaged using a Kiosk and should be sent to the Cybercrime Hub and an interpreter arranged. <u>Race</u> It is the opinion of Police Scotland that there is no evidence to support this assertion. It is important to clarify this point with due regard to public concerns, potentially arising from misleading language from other sources such as 'digital stop and search' and 'digital strip search' and potential misinterpretation by the public. This suggests stopping members of the public who are not at that time connected with an investigation or under any suspicion, and examining their device to identify crimes and incriminate – in other words a 'fishing exercise'. This will not occur. Without relevant statutory authority, currently only provided for within terrorism legislation, any other activity would be deemed a 'Fishing Exercise'. **It must be made absolutely clear that this is not**

			and never will be acceptable practice. Police Scotland will not stop any members of the public and examine devices in the manner implied by such language. Other concerns raised with regard to disproportionate searching of BME groups are a matter for the Stop and Search EqHRIA.
		Increased use of mobile devices means that hate crime is often committed on-line, evidence of which can be contained within digital devices.	Where evidence is identified in a device belonging to a victim / witness, reduction in Cybercrime Hub backlogs as a result of Kiosk roll out would have the effect of faster digital device examination, swifter criminal justice process and potential earlier device return. From three Public Consultation events that were held during 2019 in relation to consent, wider consideration into the examination of digital devices including Kiosks was provided. During these events is was brought out that evidence on a device can be obtained both knowingly or unwittingly. Police Scotland regularly launch public appeals for mobile phone / digital evidence of hatred behaviour following disorderly marches, parades, public assemblies and protests where displays / expressions of racial hatred may have been captured on the mobile devices of members of the public. At the event on 29 May 2019, a Kiosk demonstration was provided. Although the event focussed on the consent aspect of this project the general consensus on the day appeared to be supportive of Kiosks due to the potential positive impacts detailed through this document.

Religion or Belief	Low Impact - Positive	Increased use of mobile devices means that hate crime is often committed on-line, evidence of which can be contained within digital devices. There is no direct evidence to suggest any impact of Kiosk due to membership of this protected group however, individuals who are part of and or practice beliefs about religion could be viewed as disproportionately subject to crime as per the other protected factors above. Figures from the Crown Office and Procurator Fiscal Service (COPFS) website indicate that whist the number of reported cases involving religion or belief has fallen, this may be due to the introduction of other legislation (Offensive Behaviour at Football and Threatening Communications (Scotland) Act 2012) being used to report crimes committed.	A Kiosk can be used in cases where the evidential value of a device is unknown and can allow the early return of such devices to victims in cases where this is negative. Where evidence is identified in a victim / witness devise, reduction in Cybercrime Hub backlogs as a result of Kiosk roll out would have the effect of faster digital device examination, swifter criminal justice process and potential earlier device return.
Sex	Low Impact - Positive	There is no direct evidence to suggest any impact of Kiosk due to membership of this protected group however consideration has been given to disproportion effect on females for some crime types such as rape or domestic abuse given the majority of victims are female. The impact outlined relates to the associated investigative requirements and is an impact that already exists in the requirement to capture evidence from devices supporting prosecution of these crimes undertaken in Cybercrime Hubs. It is probable but not always the case that when the victim of crime reports the matter to police they will be aware of any relevant data in their device. If this is known, a Kiosk is not used, as there is no need to triage, the device goes direct to the Digital Forensic Hub. There is positive implication where the evidential relevance of a device is not known and a Kiosk may result in the early return of the device to the owner, in particular women who are disproportionally affected by domestic violence or sexual crimes and those people (disproportionately women) who depend on their phones to provide caring support to	The principal impact in this regard relates to consent as is considered fully in the Digital Device Consent EqHRIA. Denial of a device to the victim of crime is a potential compromise to their safety. As per existing processes this is considered on a case by case basis and where that risk exists Police Scotland can provide victims with a mobile phone. Consent, a Warrant or in urgent circumstances (Common law) are the only means by which Police Scotland can take a device for the purpose of examination. A Kiosk can be used in cases where the evidential value of a device is unknown and can allow the early return of such devices to victims in cases where this is negative.

		children, elderly relatives and to vulnerable adults or people with disabilities.	
Sexual Orientation	Low Impact - Positive	Lesbian, gay, bi-sexual and transgender people could be viewed as disproportionately subject to crime as per the other protected factors above. Increased use of mobile devices means that hate crime is often committed on-line, evidence of which is contained within digital devices. Figures produced by the Crown Office and Procurator Fiscal Service (COPFS) on their website indicate for hate crimes occurring within Scotland during 2018-2019, Sexual Orientation was the second most commonly recorded. The number of charges reported has increased yearly since the legislation covering this protected characteristic came into force in 2010.	A Kiosk can be used in cases where the evidential value of a device is unknown and can allow the early return of such devices to victims in cases where this is negative. Where evidence is identified in a victim / witness devise, reduction in Cybercrime Hub backlogs as a result of Kiosk roll out would have the effect of faster digital device examination, swifter criminal justice process and potential earlier device return.

5. Human Rights Impact Assessment – Consider which rights / freedoms, if any, are likely to be protected or infringed?			
5.1 Rights / Freedoms Relevant to Policing	**5.2 Assessment** Protects and / or Infringes or Not Applicable	**5.3 Analysis** What evidence is there as to how the process / practice protects or infringes Human Rights.	**5.4 Justification** – Summarise the following: • Legal Basis • Legitimate Aim • Necessity
Article 2 Right to Life	Protects	In the event of an incident where there is a threat to life the proposed use of Cyber Kiosks could allow for use of the technology in support of preventing loss of life via the ability to quickly review device data immediately without the requirement (in some cases) to travel significant distances to a Hub as the 41 Kiosks will be distributed across Scotland. This may be particularly useful in the search for missing persons.	The legal basis for Kiosk use has been outlined in Section 1B. In the case of victims / witnesses, consent is required. This consent must be sought as per Police Scotland's Consent Process including public information leaflet and set form of words (EqHRIA + DPIA completed) which has been designed with due regard to the requirements of informed consent. Examination must be / have: **Necessary** – This means that the action taken is required 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 will 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 circumstances and requirements 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 will not be reviewed. **Legitimate Aim** - Acting with a legitimate aim, for a policing purpose with the associated reasonable belief as outlined are the grounds on which the power of seizure described above is based. It is only with this legitimate aim that an officer will seize and subsequently review a device.
Article 3 Prohibition of Torture	Protects	In the event of a report of torture, often associated with abduction and other serious crime, where there is an immediate threat to individuals the proposed guidance associated with use of Cyber Kiosks will allow for the use of the technology in support of investigations to quickly identify victims and accused persons to enable protective measures to be put in place. This is particularly prevalent where Kiosks use can negate the need for significant journey to a Hub for full examination and process which in itself takes longer than a Kiosk triage.	Legal Basis - As outlined in 1B above
Article 4 Prohibition of Slavery and Forced Labour	Protects	In the event of a report of Slavery or Forced Labour (Human Trafficking) where there is an immediate threat to individuals the proposed guidance associated with use of Cyber Kiosks will allow for the use of the technology in support of investigations to	Legal Basis - As outlined in 1B above

		quickly identify victims and accused persons to enable protective measures to be put in place. This is particularly prevalent where Kiosks use can negate the need for significant journey to a Hub for full examination and process which in itself takes longer than a Kiosk triage.	
Article 5 Right to Liberty and Security	Protects	The practice will assist investigators in identifying relevant information, both inculpatory and exculpatory to the enquiry. Kiosk use seeks to reduce the need for persons to be unnecessarily detained, as an assessment of digital evidence within a relevant device can be undertaken quickly and locally via Kiosk. This examination will take place quicker (in some cases immediately) much quicker than within existing Hub processes. As devices of suspects cannot currently be assessed for evidence without submission to a Hub, there is no means by which enquiry officer can quickly review devices and thereby consider exculpatory information which may lead to the liberation of a suspect. (i.e. a manual check is not permitted) out with Hub Procedure. This is particularly prevalent in the investigation of crimes, such as domestic incidents where bail / release conditions are imposed based on available evidence. Kiosks can also provide wider public security by earlier identification of offenders and potential lines of enquiry. This can lead to the capture of crucial perishable forensic evidence on a suspect or elsewhere which could otherwise be lost. This furthermore facilitates their timeous presentation into the criminal justice process. The seizure and examination of devices if carried out lawfully will not unlawfully infringe on an individual's Article 5 rights. However, if the legal basis as outlined was compromised, Article 5 could be engaged.	Legal Basis - As outlined in 1B above Police Scotland has a high level of confidence in the legal basis allowing lawful seizure and examination of mobile devices. Evidence obtained from devices under similar processes (Hubs) has assisted in securing thousands of convictions in recent years. This basis is supported by Senior Counsel's Opinion and COPFS. The examination of digital devices also serves to protect human rights. In particular, Article 5 where the product of such examination supports the investigation of crime including exculpatory evidence. The requirement to examine a device using a Kiosk includes a requirement to disclose all relevant information as part of disclosure process. Any compromise or change to the legal basis as outlined will require a review of the suitability of Kiosk use and require review and re-evaluation of this EqHRIA and associated DPIA.

		Triage of devices unlawfully seized or examined, could result in unlawful arrest and conviction of individuals in breach of Article 5.	
Article 6 Right to a Fair Trial	Protects	Article 6 – Absolute right - is engaged with regard to the legality of the possession, retention and review of a device by Police Scotland which may subsequently be triaged as part of the proposed implementation of Kiosks. Taking possession of devices by Police Scotland therefore must be for a policing purpose and connected to a police investigation. Voluntarily (consent) or by means of seizure (common law, warrant or statutory provision) are the ways by which an officer will take possession of a device connected to a police investigation. An individual's right to a fair trial could therefore potentially be compromised by the unlawful seizure and subsequent recovery and review of a device including its data. Each officer has the responsibility to ensure their actions in that regard are lawful thereby protecting these rights. The practice will assist investigators in identifying relevant information either inculpatory or exculpatory to the enquiry. The associated guidance documents outline seizure and handling of devices for evidential purposes. A Digital Forensics, Disclosure Guidance document is being drafted to assist, however all officers are trained in the requirements of disclosure of 'relevant information' and the requirement where possible to 'make all reasonable lines of enquiry' to fulfil that obligation. The seizure and examination of devices, if carried out as detailed, will not unlawfully infringe on an individual's Article 6 rights.	Legal Basis - As per 1B above. All devices must be lawfully seized (Common Law, Warrant or Statutory provision) or obtained with the consent of the owner in order that subsequent examination be lawful. These powers form the legislative basis under which we must consider appropriation of digital devices and by default, the data contained within. Processes are outlined within the Toolkit and training on disabling the ability of devices to connect to a network. This protects against any potential interception of data, whereby the only data reviewed will be that on the device at the time of seizure. Police Scotland has no reason to believe that the legal basis allowing us to lawfully seize and examine mobile devices is compromised. Evidence obtained from devices has secured thousands of convictions in recent years. The examination of digital devices also serves to protect human rights. In particular Article 6 where the product of such examination supports the investigation of crime including exculpatory evidence To protect these rights in every circumstance, examinations require proportionality, necessity, legitimacy and relevance which must be recognised and guide police activity. This question of fairness must also be considered in

			the context of the functions and scrutiny provided by the Scottish Courts, to test legality and the wider role of the Scottish Courts to: • Help protect our constitutional rights to equal protection and due process under the law. • Provide the opportunity for the parties to have their cases heard by neutral judges and/or juries ensuring that all cases are decided in a fair and consistent manner. • Provide a forum to resolve disputes and to test and enforce laws in a fair and rational manner. • Courts are an impartial forum, and judges are free to apply the law without regard to the states wishes or the weight of public opinion but in line with human rights. • Court decisions are based on what the law says and what the evidence proves; there is no place in the courts for suspicion, bias or favouritism. The procedures and decisions must be accessible and transparent and apply the rights found in the European Convention on Human Rights (ECHR). • Exist to do justice, to guarantee liberty, to enhance social order, to resolve disputes, to maintain the rule of law, to provide for equal protection to all regardless of background and to ensure the due process of law. • Exist so that the equality of individuals and the state is reality rather than empty rhetoric and to ensure that the rights enshrined in the ECHR are applied in its decisions and complied with by legislation. With the functions of the courts (as outlined above) in mind, such is the prevalence of digital devices that most trials have an element of digital examination involved in evidential submissions. This is particularly prevalent in solemn proceedings. This

			prevalence supports the determination that device examination within existing parameters is admissible as evidence passing the relevant tests of fairness including Article 6 considerations. Kiosks only provide a triage stage in existing processes. COPFS have provided Opinion that the addition of this triage process does not change this court tested process as outlined in their letter to Justice Sub-Committee on policing on the matter: *'The COPFS do not consider that the use of Cyber Kiosks would change the process currently in use for obtaining relevant evidence from cybercrime hubs'.*
Article 7 No Punishment without Law	N/A	N/A	N/A
Article 8 Right to Respect for Private and Family Life	Infringes / Protects	Article 8 concerns the qualified right to respect for private and family life. The examination of digital devices may infringe upon a person's right to respect for private life, however, this is not an absolute right. Infringement of an individual's Article 8 rights (victim, witness, suspect or accused) 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. 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 triage facility is a reduction in the copy, storage, and retention of data associated with devices thus potentially removing the device from Digital Forensics Hub processes in cases were no evidence is found. The Kiosk facility may also reduce the number of officers reviewing device data with those trained in Kiosk use being used for device triage across multiple investigations as opposed to each individual	Legal Basis – As per 1B above. It is important to clarify the Police Scotland position in relation to public concerns encouraged by the use of potentially misleading language from other sources such as 'digital stop and search' and 'digital strip search' and potential misinterpretation by the public. This suggests stopping members of the public who are not at that time under any suspicion and examining their device to identify crimes and incriminate, amounting to a 'fishing exercise'. Without relevant statutory authority any other activity would be deemed a 'Fishing Exercise' and it must be made absolutely clear that this is not and never will be acceptable practice. Police Scotland will not stop members of the public and examine devices in the manner implied by such language. The voluntary provision of devices by witnesses / victims must involve informed consent. A process including an information leaflet and a signature applied to a 'consent declaration' has been designed

		investigating officer, however the investigating officer may choose to be present for the triage. There is reduced impact to Article 8 rights over the existing full download during hub processes as the review of data during Kiosk triage can be focused using parameters including data type (texts / images/ calls etc.), date range and the search facility to retrieve specific data relating to the relevant number or name which is input to the search parameter field. The process of examining devices using the Kiosk does not retain data on the Kiosk itself. The data extracted from the mobile device to facilitate viewing is securely wiped from the internal storage on the Kiosk once the operator has finished the examination. The only data retained on the Kiosk as a consequence of the examination is the log in information retained for the purposes of auditing and assurance e.g. time, date, operator, reference number etc. Kiosks can only be used to examine lawfully obtained devices. No other devices should be examined on them. To enforce this, regular dip samples from the system logs will be taken for quality assurance purposes. Management information will be produced and scrutinised; including the aforesaid quality assurance data and data submitted during the Examination Request Form (ERF) submission and authorisation process. This includes what lawful authority was used, crime type, device owner (Victim, Witness, Suspect, Accused) etc. This article can be perceived as being infringed by individuals whose data is being viewed by police however, this action is permitted when conducted under and in accordance with the legal basis outlined, provided it is required to fulfil Police Scotland's	to capture this consent with due regard to the principle of informed consent namely; that it is voluntarily given, with informed decision making and the individual has sufficient capacity to decide. This enhancement to the public understanding of consent provided by the leaflet designed through public consultation allows the public to make an informed decision. This is supported by numerous materials available online to further enhance understanding of police process and includes a FAQ. All items use plain language having been drafted using feedback from the Police Scotland led Digital Device Examination and Consent External Consultation Events. These events included representatives from voluntary organisations that act as advocates for the rights of all of the main protected characteristics. This captured the key concerns of the group which Police Scotland has sought to address within the information leaflet provided. The consent process itself will be subject of EqHRIA assessment and has been considered by the External Reference and Stakeholders group including the Information Commissioner Office. The 'Digital Device Examination Principles' has been written to outline that which must be adhered to in the use of technology including Kiosks for general digital forensic investigations. To conduct diligent enquiry and maximize our capability to detect crime, the balance of investigative needs versus the public expectation of privacy must be met by doing what is lawful, ethical and in good faith and no more than is necessary and proportionate to achieve the lawful objective sought. Fairness, integrity and respect of property and right to privacy as outlined within Article 8 are the key principles which guide all officers in the execution of duty.

		obligations and duty enabling relevant Police investigations, the prevention and detection of crime.	These principles are requirements for the use of Police Scotland's 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. They must consider, comply and act in accordance with the law and existing well established practices and process in relation to the examination request submission, authorisation, legal basis and these principles all at times. **Necessary** – This means that the action taken is required to achieve the objective of the digital investigation of that device. If an action is not necessary then the intrusion cannot be justified and therefore will not be taken. **Proportionate** – This means that the officer has considered the intrusion that their activity will involve, with due regard to the implications in terms of respect for private and family life. The officer must be content that any / further interrogation is proportionate considering the circumstances and needs of the investigation. **Relevant** – This means that the data which the officer seeks to review is only that pertaining to the ongoing investigation forming part of a reasonable line of enquiry. If the data is not potentially linked to the crime/offence under investigation it will not be reviewed. **Legitimate** - Acting with a legitimate aim and associated reasonable belief in line with the duties of constable 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 will seize and subsequently review a device. **Justified** – Justification is required for both seizure and examination regardless of the power used. The

			action must be right and reasonable (for good reason). A reason means a fact, circumstance, or explanation that justifies the reasonable grounds on which a device is seized and examined. These considerations form part of Kiosk training and each operator has the power to refuse any request where they are not satisfied that any Article 8 infringement is in accordance with the above criteria. <u>Less intrusive means</u> It is recognised that means of obtaining evidence without the requirement to seize a device from a victim / witness may exist. Examples include evidence forwarded to officers via email, screen shots or prints of relevant data however, this does not meet the requirements of best / primary evidence and therefore can be challenged by the defence.
Article 9 Freedom of Thought, Conscience and Religion	Infringes / Protects	The seizure of digital devices may infringe upon a person's qualified right to freedom of thought, belief and religion, however, this is not an absolute right. Infringement of an individual's Article 9 rights can be permitted if that infringement is in accordance with the law, to preserve life or to prevent crime. With the vast majority of the population now owning or having access to a digital device, this provides a platform for individuals to exercise this right publicly via the numerous digital applications. Many will also use this device to practice their religion / belief through the use of application based religious texts and scripts. (YouVersion as of 04/09/2019 stated over 388 million copies of their Bible App had been downloaded) (YouVersion, 2019). Individuals may further exercise this right by contacting or communicating with others using digital devices. There is an element of enhanced protection of this right afforded by the Kiosk facility. The swifter and more focussed identification of evidence enables	Legal Basis – As per 1B above. Although removal of devices is acknowledged to infringe on the ability of an individual to 'manifest or show their thoughts, believes and religions' in a digital arena, this does not prevent them from demonstrating their beliefs digitally using another device or through traditional means in the physical world. As intimated within other relevant sections, devices will only be taken from a victim/witness where in these circumstances where there is lawful authority to do so (warrant / urgency) or they have provided their informed consent, and it is necessary and proportionate, therefore, infringement is justified. Devices will also be returned to victim/witnesses as soon as possible. The use of a Kiosk in the early return of a device following triage must be recognised in the potential protection of this right as opposed to the longer

		digital devices to be returned to the owner sooner if no evidential data is contained on the device. The use of a Kiosk triage will in turn reduce the workload going through Digital Forensic Hubs, which should result in quicker criminal justice processing and again potentially earlier return of devices to owners.	timescales involved in the current hub submission process.
Article 10 Freedom of Expression	Infringes / Protects	The Impact is not in direct relation to the use of this Kiosk facility as the impact associated exists within the current digital forensic processes employed by Police Scotland in particular seizure of devices. The introduction of triage to that process does not change this. The impact of digital forensic examination whether by Kiosk or otherwise impacts upon Article 10, not by virtue of the data reviewed, 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. There is an element of enhanced protection of this right by use of the Kiosk. Early Kiosk review identifies when there is no evidential data and the device is then returned to the owner. With Kiosk use reducing back logs at Digital Forensic Hubs, we will see swifter criminal justice processing and thereby potential earlier return of devices to owners.	Legal basis – As per 1B Above Principles effected. **Necessary** – This means that the action taken is required to achieve the objective of the digital investigation of that device. If an action is not necessary then the intrusion cannot be justified and therefore will not be taken. **Proportionate** – This means that the officer has considered the intrusion that their activity will involve, with due regard to the implications in terms of respect for private and family life. The officer must be content that any / further interrogation is proportionate considering the circumstances and needs of the investigation. **Legitimate** - Acting with a legitimate aim and associated reasonable belief in line with the duties of constable 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 will seize and subsequently review a device. **Justified** – Justification is required for both seizure and examination regardless of the power used. The action must be right and reasonable (for good reason). A reason means a fact, circumstance, or explanation that justifies the reasonable grounds on which a device is seized and examined.
Article 11 Freedom of Assembly and Association	Infringes / Protects	Article 11 as well as protecting the freedom of assembly and association in the physical world, enshrines an individual's right to peacefully assemble	Legal basis – As per 1B Above Although removal of devices is acknowledged to

		and association with others using the Internet, being deemed key to building and strengthening democratic societies (Council of Europe, 2014). Obtaining devices for triage therefore potentially infringes this right as they may be without a device for a period of time.	infringe on the ability of an individual to 'freely and peacefully assemble, associate and form/join trade unions for the protection of their interests' in a digital arena, this does not prevent them from manifesting these rights using other devices or in the physical world. As intimated, devices will only be taken from a victim/witness where in these circumstances where there is lawful authority to do so (warrant / urgency) or they have provided their informed consent, and it is necessary and proportionate, therefore, infringement is justified. Devices will also be returned to victim/witnesses as soon as possible. The use of a Kiosk in the early return of a device following triage must be recognised in the potential protection of this right as opposed to the longer timescales involved in the current hub submission process. Police can also infringe on an individual's Article 11 right in limited circumstances where prescribed by law and necessary in a democratic society in the interests of. • National security or public safety • Prevention of disorder or crime • Protection of health or morals • Protection of right and freedoms of others.
Article 14 Prohibition of Discrimination	N/A	N/A	N/A
Protocol 1, Article 1 Protection of Property	Infringes	The Kiosk Toolkit and Digital Device Examination Principles contain information regarding seizure and handling and examination of devices. This article might be perceived as infringed by the individual as they are deprived of their private	Legal basis as per 1B above. It is worthy of note that the introduction of Kiosks when compared to existing processes (Cybercrime Hubs) has significant potential for positive impact on all communities due to having a triage option

		property by Police. This is covered by legal basis on which Police Scotland proceed with this activity, enabling investigation of crime whether by seizure or the voluntary surrender of a device. All devices obtained will be treated as productions and protected by productions processes and audit.	allowing a quicker process for identifying the need to submit a device for full examination and where appropriate negate the need to deprive owners of their device.

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

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

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

Management Information (MI), Kiosk Use - The Kiosk will log that an examination has been undertaken and what the results were (positive/negative, times and dates, extraction type and duration etc.) Kiosks logs also produce the status of the individual (victim / witness / suspect / accused / other), the identity of the person doing the extraction, the type of device and the case reference number from our Case Management System. These logs are stored on the Kiosk itself but are not accessible by operators. This audit log will be available to the system administrator (Cybercrime) for quality audits. This will ensure all devices are being processed in accordance with agreed protocols, being assessed and triaged appropriately and accurate details are being recorded within the MI log.

Cybercrime staff will periodically visit the Kiosks to install updates, etc. At this time, using enhanced credentials, they will log into the Kiosk and recover these logs using encrypted USB storage devices. These logs will be aggregated and stored on the secure Cybercrime central repository.

Supporting and enhancing the audit, will be the availability of new data as a result of a new Examination Request Form (ERF) on which each examination request must be submitted. The enhanced form will allow for audit of associated crime type, owner (victim / witness / suspect / accused / other), status and power used to obtain that device
These will be used for training, business and audit purposes. A dip sample (volume to be confirmed once level of use of the Kiosks is better understood) will be taken of examinations from the logs. This will be compared against the Case Management System to ensure that the examination was authorised, that it was proportionate to the case and that the device was seized / taken legally and handled in accordance with productions processes. If the examination fails on any of these points then the appropriate action will be taken, whether by remedial training or by disciplinary process.

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

Issue / Risk Identified	Action Taken / to be Taken	Action Owner / Dept.	Completion Date	Progress Update
Proper and lawful use of the Kiosk	Training and guidance including the following documents have been consulted on with partners including; Human Rights Commission, Privacy International, SPA, Police Federation, Unions, Scottish Government, HMICS, COPFS, Information Management. The Digital Device Examination Principles, Toolkit, two day training course, DPIA, EqHRIA, Quality assurance measures (full auditable and accountable process from submission /seizure to Case Management System Submission, triage and beyond to Digital Forensics Hub	DCI Cybercrime Operations	Ongoing – Not subject to end date.	The legal basis as outlined is robust and supported by COPFS and the independent Opinion of Senior Council, Murdo McLeod QC in his review of Kiosk use. The aforementioned support is articulated in writing and published on the 'The Scottish Parliament' website. The Digital Device Examination Principles governing use and providing guidance will support the 'Cyber Kiosk Toolkit' document which outline role, responsibilities and guides officers in kiosk use. Training includes a module on the proper use of the technology in accordance with Law and ECHR. On 30 October 2018 the External Reference Group agreed the document set was sufficiently advanced to support the roll out of training, phase 1 of which (East) commenced in November 2018. The training has a module (22 slides) dedicated to understanding and compliance with the Legal Basis, ECHR and DPIA implications and restrictions. Training was rolled out across Scotland concluding in May 2019.

	examination) ensure compliance with law and responsibilities.			
Officer's awareness and clear parameters of their responsibilities re: data interrogation with regard to ECHR and necessity, proportionality and relevance.	Develop a 'Digital Forensic Examination Principles' document articulating this guidance, role and responsibilities, ensuring awareness to Kiosk operators via training and communications strategy. Ensure these parameters are reflected and outlined in all guidance.	DCI Cybercrime Operations	To be completed and ratified prior to Kiosk roll out (Summer 2019). Roll out delayed - is now planned for January 2020 Complete	11/10/18 Under development. Due ratification pre training. The training has a module (22 slides) dedicated to understanding and compliance with the Legal Basis, ECHR and DPIA implications and restrictions. 19/12/18 – PSoS continue to seek feedback and opinion from key stakeholders with regards to the legal basis for use. The document set cannot be finalised until this is fully considered. Any changes will be reflected throughout these and this document. 14/5/19 –. The 'Digital Forensic Examination Principles' document will be submitted to external reference and Stakeholder Groups for ratification on 11 June. This draft document was awaiting the consideration of COPFS and Senior Council Opinion prior to ratification. 29/10/19. The Toolkit outlines clearly roles and responsibilities and has undergone relevant consolation including Force Policy Unit circulation. The 'Digital Forensic Examination Principles' document has been considered by COPFS, both External Reference and Stakeholder groups and PSOS Legal Services. Feedback has been applied and ratified as fit for purpose. Both will be presented within the document set provided to the ACC Senior Responsible Officer (SRO) prior to publication. Document has now been signed off by ACC and published on both the Police Scotland website and internally on the Intranet.

Existence of legal framework under which triage and forensic examination is undertaken	PSoS are content that legal framework currently exists and is supported by COPFS , QC Opinion and current court cases in which such evidence is accepted. Several stated cases support this framework. Activity being developed to consider further the existing legal framework recognising change in device capability and content over time. HRC believe a warrant may be required to access a mobile phone. Their legal team are considering this and will share feedback with PSoS due W/C 15 October.	DCI Cybercrime Operations	Complete	11/10/18 – Draft letter to Crown with DCS McLean for ratification. 19/12/18 – No update received form Crown Office. Draft Legal Basis has been submitted to Legal Services for opinion. 14/5/19 - The legal basis as outlined in part 1B is robust and supported by COPFS and the independent Opinion of Senior Counsel, Murdo McLeod QC in his review of Kiosk use. The aforementioned support is articulated in writing and published on the 'The Scottish Parliament' website. The legal basis for device examination has been drafted and will be published with other Kiosk documents for officer and public reference.
Appropriate forum for the enhancement of ECHR knowledge / responsibilities of Kiosk operators.	Roles and Responsibilities of operators in terms of Digital Device Examination Principles, Toolkit, DPIA and EQHRIA have all been incorporated into the 2 day Kiosk operator training course.	DCI Cybercrime Operations	Estimate by May 2019 Update – Delivery completed in May 2019	11/10/18 Under development by Cyber Training Team. Force training aware, cited on proposal and content that no formal involvement is required from them. The training has a module (Module 1 - 22 slides) dedicated to understanding and compliance with the Legal Basis, ECHR and DPIA implications and restrictions. A feedback process has been designed within the Kiosk coordination and management process to capture any issues / queries from Kiosk operators and is outlined in the 'toolkit'.

				14/5/19 – Module 1 has supported training of all 410 officers. A full review of the training course has been conducted. Assessment of training provided that officers felt they understood well the requirements in this regard which form part of foundational training and everyday decision making for officers. Any remedial training will be identified as part of the proposed audit process and can be addressed. To maintain the required resilience of operator numbers training will continue as and when required and include enhancement to Module 1 as required.
Appropriate audit and assurance of Kiosk use to ensure compliance with ECHR, process, oversight and means to address issues.	Kiosks produce Management Information data providing oversight of use by each operator. A plan will be drafted which will outline what is being monitored including frequency and purpose of Kiosk use, dip sampling process, learning and remedial action taken. This data will be subject to regular review and dip sampling and will be published. Supporting and enhancing the audit will be the availability of new data as a result of a new Examination Request Form (ERF) on which each examination requests are submitted.	DCI Cybercrime Operations	Quarterly Following roll out	Under development by Cybercrime training. 14/5/19 - The Kiosks Implementation Plan includes the collection of associated Kiosk MI on the 1st of each month. This will be collected monthly and assessed until further notice. It is envisaged that any changes to audit and review will be considered and ratified by Senior management. A post Implementation review will be conducted six months after roll out. The scope of this review has been captured in a Terms of Reference ratified by The Kiosk Reference and Stakeholder Groups.

	The enhanced form will allow for audit of associated crime type, owner (victim / witness / suspect / accused / other), status and power used to obtain that device.			
Failure to appropriately or adequately circulate / propagate communications in relation to clear parameters of Kiosk operator responsibilities re data interrogation with regard to ECHR, necessity and proportionality	Communication Strategy has been developed to mitigate this risk to consider intranet publications of guidance and relevant documentation (Legal Basis, Toolkit, Impact Assessments). There is also established liaison with operators via divisional and Cybercrime SPOCs (emails / contacts list and FAQs etc.). All Kiosk operators will be given a user's pack containing the examination principles.	DCI Cybercrime Operations	Ongoing until the Kiosks are Business as usual.	Communications Strategy being drafted for sign off on 29/10/18 Communications Strategy has begun raising awareness of the Kiosk and capabilities. The training has a module (Module 1- 22 slides) dedicated to understanding and compliance with the Legal Basis, ECHR and DPIA implications and restrictions. A feedback process has been designed within the Kiosk coordination and management process to capture any issues / queries from Kiosk operators and is outlined in the 'toolkit'. All supporting products and documentation will be available via the Police Scotland intranet and advertised as part of communications at point of roll out. Communications includes the publishing and signposting of information and guidance materials. Each Kiosk operator will be provided a support pack via email which will include the 'Digital Device Examination Principles' guidance of proportionate use and relevant ECHR considerations.
Failure to ensure appropriate collation of issues identified and process for referral of any potential compromise to	A local SPOC has been identified for each Division. This SPOC will hold responsibility for the collation of all issues	DCI Cybercrime Operations	Complete	A feedback process has been designed within the Kiosk coordination and management process to capture any issues / queries form Kiosk operators and is outlined in the 'toolkit'.

ECHR obligations.	including those under this risk and will collate and articulate such issues to Cybercrime to address as appropriate. Kiosk Operators are aware of this via training / guidance and the toolkit. A list of SPOCs is included in the Guidance. A list of all SPOCs and Operators will be held at Cybercrime. Operators will also be identifiable via SCOPE as having completed Kiosk Training. This feed of issues will be monitored by Cybercrime staff and issues addressed via the communications mediums available to SPOCs and Operators. There are dedicated mail boxes for the reporting of issues direct to Cybercrime. Associated Kiosk Documents, EqHRIA, DPIA, Toolkit etc. can and will be changed if required.			Explanatory process map within the 'Toolkit' has been completed. Divisional SPOCs at supervisory level identified and aware of responsibilities in this regard. This will be monitored as part of the implementation plan in which there are dedicated feedback and assessment miles stones to ensure the capture of initial concerns or issues. Cybercrime Policy and Coordination Unit will have oversight.
8- Sufficient public awareness regarding lawful device seizure, rights and associated	A 'Digital Device, Consent Public Information Leaflet' has been developed and	DCI Cybercrime Operations	Estimate by June 2019 – Prerequisite of Kiosks deployment.	19/12/18 - Draft now includes the capture of consent as outlined above and the leaflet will be supported by the publication of FAQs (including the Legal Basis) and a flow process / chart showing the

police process and implications.	consulted on via the public[1] and partners within the various Stakeholder and Reference Groups listed above. This will be made available to frontline staff and will be provided to victims and witnesses on each occasion a device is requested via consent. This is supported by a number of materials (Processes, FAQs, Digital Device Examination Principles) drafted using feedback from the Police Scotland led Consent External Consultation Events on the matter, which will be available online explaining powers and process for seizure and examination, therefore also available to suspects and accused should they desire this information. This is designed primarily to support the voluntary provision of		Update – Development delayed to fully consider consent and legal basis – Roll out will be January 2020.	public what happens their device / data. 14/5/19 - A Consent Working Group has been established including representation from COPFS, Legal Services, Information Management, Equality and Diversity Unit and Cybercrime to ensure effective design and delivery of this product with all requirements and considerations addressed. This leaflet will be considered by the Stakeholder and Reference Groups. 9/8/19 - There have been two public consultation events in relation to consent which has included wider consideration in relation to device examination including Kiosks. As a result a number of products have been developed in consultation with the public to assist public understanding of police processes, powers and consent. At the event of 29 May a Kiosk demo was provided. Although the event focussed on the consent aspect of this project the general consensus on the day appeared to be supportive of Cyber Kiosks due to the potential positive impacts detailed above. All Kiosk and Consent materials / guides will be published and / or in use prior to Kiosk Roll out. 22/11/19 - A third public engagement event was held on 13/11/19. Feedback from these has supported the finalisation of FAQs, Public information leaflet and flow processes now completed and ready for publication on go live date. These were also provided / presented to the External Reference Group on 21/11.

[1] NHS Lanarkshire, National Independent Strategic Advisory Group (NISAG), Edinburgh Women's Aid, Scottish Women's Rights Centre, Who Cares? Scotland, Central Scotland Regional Equality Council (CSREC), Youth Link Scotland, Scottish Commission for Learning Disability, People First Scotland, Barnardo's Scotland & ASSIST, Scottish Government, Equality Network, Council of Ethnic Minorities Voluntary Sector Organisation (CEMVO), Deaf Action, Autism Network Scotland, Children in Scotland, 5 Rights Youth Commission, Centre for Youth and Criminal Justice, and Engender & Young Scot.

	devices by witnesses or victims and must involve informed consent. A Leaflet and consent declaration have been designed to capture this by means of victim / witness information and signature. This consent must be captured in a written statement form the victim / witness. Leaflet and the wording have been designed with due regard to the requirements informed consent.		Complete	The communications plan includes publication of these for go live. All documents supporting public awareness regarding the lawful seizure of devices, human rights, associated police processes and implications have now been signed off by Senior Management and been published on the Police Scotland Website.
Officers have the appropriate vetting for Kiosk use.	All police officers undergo Recruitment Vetting (RV) as part of the role. Force Vetting Unit have been consulted and confirm that RV vetting provides sufficient protection in relation to the proposed Kiosk functionality. RV is the minimum level required for all applicants to join SPA/Police Scotland irrespective of their role. Successfully attaining RV clearance allows access to police systems, assets, premises and classified	DCI Cybercrime Operations	October 2018	Complete

	information up to CONFIDENTIAL or OFFICIAL-SENSITIVE with occasional access to SECRET.			
Digital Examination without consent of victims and witness.	This is not an impact on Kiosks alone and relates to any digital device examination including Kiosks. Police Scotland have consulted with External Reference and Stakeholder Groups and agreed this requirement as per Senior Counsel's Opinion. A new process is in draft and key internal and external stakeholders including Equality and Diversity, Disclosure, Information Management, Legal Services, COPFS and other colleagues have been identified for the working group to progress the requirement through to delivery.	DCI Cybercrime –(Risk owner only with regard to oversight of Kiosk not the Consent capture requirement itself)	Ongoing - Summer 2019	Update - May 2019 - Police Scotland currently lead the 'Digital Device Examination Consent Working Group' the first meeting took place on 11 April 2019 and included representation from Legal Services, COPFS, Information Management, Digital Forensics and Policy Support. At this time the need for a workshop of key external representatives from the most effected protected groups (Age, Disability, Race, Victims of Crime (focus on sexual and domestic) was agreed along with the requirement for an EqHRIA for the consent capture process itself. A workshop with representation from all protected characteristics is planned for 29 May 2019. This will identify the concerns held regarding consent and device examination so that these can be understood, addressed or mitigated as appropriate. The full EqHRIA impacts will be contained in the 'Digital Device Consent' EqHRIA. Once drafted and appropriately consulted on with assessments complete this risk can be deemed mitigated. Update - July 2019 In addition to the above event a second Public consultation event took place on 5th July. Public engagement has been considerable and PSoS are drafting products in consultation with the public to assist their understanding of consent capture, processes and a form for use by PSoS to do so.

				Update 16/10/19 Following extensive review and consideration of consent capture by Programme and PSoS Legal Services a Force position in relation to the legal requirements and legislation governing consent has been established. This has allowed for simplification of the requirements of consent to focus on the 'Informed' aspect of victim / witness engagement and clarified that legal powers and obligation PSoS have in relation to the data obtained. This has in turn dictated requirements in terms of PSoS attaining consent eliminating any need to meet the requirement of article 4(11) GDPR (informed, specific, unambiguous and ongoing) – an unattainable benchmark for law enforcement. This clear position compliant with Section 35 (2(b) of the DPA (outlined in the legal basis in Part 1B) allows for much clearer and simplified information to the public further enhancing their decision making when providing consent. This EqHRIA has been updated throughout to reflect these findings. Complete All documents and processes in order to mitigate this risk have now been completed and signed off by Police Scotland Senior Management following full consultation with partners and stakeholders. Where applicable, documents providing guidance to officers/staff and the public have been published on the Police Scotland website and internally on the Force Intranet.