DIGITAL DEVICE EXAMINATION – PRINCIPLES

Introduction

These principles of use seek to set the standard which will be adhered to by Police Scotland officers and staff when taking and examining a digital device and any data extracted.

Most of us lead lives facilitated by digital devices. It is therefore inevitable that during police investigations such a device may prove to offer a reasonable line of enquiry. Every device examination undertaken by Police Scotland must and will be justified as being lawful, necessary and proportionate.

Police Scotland recognise the risks and concerns associated with taking and accessing citizens' data during a digital device examination. Associated collateral intrusion and any infringement of the rights of individuals may not be eliminated entirely but can be minimised when guided by these principles.

Purpose of Digital Examination Principles

Police Scotland has engaged with community representatives to better understand the implications, needs and concerns in relation to taking and examination of digital devices in particular mobile phones. This engagement has identified the need for clear commitment from Police Scotland as to what will and will not be acceptable practice including the need for lawful, necessary and proportionate grounds to take and examine a device and infringe upon an individual's right to privacy.

Purpose of Digital Examination

As technology evolves so do the capabilities of digital devices and the associated volume of digital data stored.

This evolution means that personal data is now commonplace within devices in our communities, capturing intimate detail of individuals and the lives they lead. As both holders and investigators of that data, Police Scotland is required to govern, process, access and use that information lawfully and appropriately.

As such, taking a digital device and any subsequent examination of its contents undertaken by Police Scotland must only be carried out for a legitimate purpose and must comply with the principles of use outlined here in.

The legitimate purposes of digital device examination are;

- To preserve life
- To determine whether or not the contents of a device are of relevant (or appropriate) evidential value

- To capture any such evidential material

Requirements

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 undertaken. 'Necessary' is not the same as 'useful' or 'helpful'.

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 satisfied that some less intrusive option is not reasonably available. The officer must be content that any / further examination 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 basis 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 basis that an officer will take and subsequently examine 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 taken and examined.

Legal Considerations of Digital Device Examination

Policing

The general duties of a constable outlined in Section 20, Police Fire Reform (Scotland) Act 2012 include;

(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.

It is in line with execution of these duties that we will consider digital device examination.

Additionally, consideration is given to Section 164 of the Criminal Justice Licencing Scotland Act 2010 - Code of Practice which provides that the police have an obligation to pursue all reasonable lines of enquiry and to record, retain, review, reveal and where appropriate provide all information which may be relevant to the Crown.

Data Protection Act 2018

The Data Protection Principles

The principles set out in Part 3 of the Data Protection Act 2018 require personal data for Law Enforcement to be:

1 Processed lawfully and fairly (lawfulness and fairness)

2 Collected for specified, explicit and legitimate law enforcement purposes, and not further processed in a way which is incompatible with those purposes (purpose limitation)

3 Adequate, relevant and not excessive in relation to the purposes for which it is processed (data minimisation)

4 Accurate and where necessary kept up to date (accuracy)

5 Kept for no longer than is necessary for the purposes for which it is processed (storage limitation)

6 Processed in a way that ensures appropriate security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (integrity and confidentiality).

There is a likelihood that personal data, including sensitive personal data will be amongst material recovered from an examination of the contents of a digital device taken by police.

Police Scotland will process all such data in accordance with the Data Protection Act 2018, including the principles detailed above.

We will meet these principles in relation to the processing of such sensitive data by adherence to our commitments under each principle as outlined in the Police Scotland, Appropriate Policy Document (APD), 'Sensitive processing for law enforcement purposes'.

Human Rights

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

Article 5, the right to liberty and security of person, is a qualified right meaning its operation can be limited in certain circumstances provided for by the law. Article 6, the right to a fair trial or hearing, on the other hand, is an absolute right. The seizure and examination of digital devices, if carried out properly should not unlawfully infringe on an individual's Article 5 or 6 rights.

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 and can be qualified in certain circumstances. Infringement of the Article 8 right 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 that 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 considered in the context of being part of the role of the Police, and the 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 may materially assist in the speedy location of a missing person or dangerous individual. Similarly Articles 5 and 6, where the product of an examination directly supports the investigation of crime. This includes the potential identification of exculpatory evidence, which could result in the halting of a protracted investigation or criminal trial. This can be seen as being an additional safeguard to a person's rights under Articles 5 and/or 6.

Digital device examination can also impact upon the exercise of an individual's right under Article 10; the right to freedom of expression. This would not be by virtue of the data being reviewed, however could arise as a consequence of the effective denial of access to the device by which individuals exercise their right to expression via various communication and media platforms. 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 without undue delay.

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 requirement for digital device examination does not alter or extend existing police powers relating to the seizure and / or retention of productions.

Seizure and Examination

Victims and Witnesses

The authorities for taking 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).

Whenever consent is the legal authority used to take and examine a device, the consent should be voluntary, informed and given by a person with capacity to do so. The Police Scotland, Digital Device Consent Public Information Leaflet will be provided to the victim or witness in all such cases. Officers will ensure any consent is obtained in line with the below requirements.

Consent Requirements – The individual must;

- Have **capacity** - to understand the information given to them and make an informed decision.
- Be **informed** - What the process of taking and examination involves and their rights in terms of providing, refusing and withdrawing consent.
- Provide **voluntary** consent – the decision to either consent or not must be freely made by the person and free of coercion, pressure or influence.

Any action taken must be considered alongside other relevant applicable principles such as those outlined within Articles 5, 6 and 8 of ECHR.

Statutory Powers - Accused / Suspects / Temporarily Detained Persons

Search, seizure and examination will only be conducted when lawful - where there is an express statutory power, a warrant expressly conferring such a power or a power at common law. Various pieces of legislation (not reproduced here) such as Section 47 and 48 the Criminal Justice (Scotland) Act 2016 permit a police constable to search

any arrested person or seize and examine any item in their possession whether they have been charged with an offence or not.

Principles Governing Digital Device Examination

The examination of digital devices is now a major facet of modern policing. The principles and values that must be applied exist at all stages of the examination process from triage and analysis to storage and all associated data processing.

A fundamental value of Police Scotland's principles of service to our communities is policing with the consent of the public we serve. We police by consent so by extension what we do, we should do in the public's interest. Police Scotland digital device collection and examination is directed by that consent and the public expectation to undertake all legal means necessary to preserve life and bring offenders to justice.

The associated responsibility of the Service to meet the expectations of the public in this regard requires the highest standards and principles.

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.

The principles of fairness, integrity, respect and human rights form Police Scotland's core Policing Values. These values form a foundation on which our duties within digital forensics are carried out. The rights outlined within the Human Rights Act and in particular articles 5, 6, 8 and 10 must be considered by all officers in the execution of duty and the seizure and examination of devices. These principles are requirements for the use of Police Scotland powers and technical ability regarding 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 justify their actions in terms of necessity, proportionality, legitimacy and relevance, reviewing where possible only what is relevant to the investigation and consider, comply and act in accordance with the law and these principles all at times.

Commitments to the Principles

We will ensure;

- The principles outlined will apply at every stage of associated digital device examination processes;
    - Seizure
    - Administration
    - Examination
    - Data retention and disposal

- For all such seizures and examinations, there must be a reasonable belief that one or more of the following apply to the digital device:

    - Has been or is likely to have been used in the commission of a crime.
    - May contain information relevant to the prevention and/or detection of a crime.
    - Has been lawfully obtained.
    - Is believed to potentially be connected in some way to a police investigation or incident.
    - May contain information that is urgently required and essential to the preservation of life or mitigation of other significant threat.

- Examination is to the extent which is no more than is necessary to achieve the lawful objective.
- That no digital device examination will take place without appropriate authorisation and administrative processes being followed. Police Scotland, Digital Forensic Gateway staff or supervisors will authorise examination of digital devices and confirm that reasonable grounds, necessity and proportionality exist for examination of the item.
- There will be an auditable administrative authorisation process in support of digital device examination.
- Any use of equipment for digital device examination is only by trained staff that must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
- Any data recovered will be stored in compliance with the Police Scotland Record Retention SOP. The Record Retention SOP supports Police Scotland's Record Management Policy by defining specific retention rules for records held by Police Scotland. The application of these rules will ensure good business practice and also compliance with the relevant legislation and standards, including, but not limited to:
    - The Public Records (Scotland) Act 2011
    - The Freedom of Information (Scotland) Act 2002
    - Data Protection Act 2018 (DPIA 2018)
- The security of data we hold.
- Breaches of security, including, but not restricted to loss or misuse of Police Scotland examination capability or data, will be reported immediately to management and the Information Security Officer.
- Robust action will be taken regarding any suspected or actual misuse of our examination equipment / capability. Any such breach of conditions of use or impropriety will be reported via management for investigation and follow existing anti-corruption and disciplinary procedure.

- An audit regime is maintained in relation to Cyber Kiosk use to support these principles and allow review and consultation. Audit results will be subject of review by Cybercrime Management and findings published.

We will not consider;

- Items provided in to police that are believed to be irrelevant to a police investigation or incident.
- The examination of any digital device without reasonable and legitimate need.
- The use of examination equipment / capability for any personal purpose.

Responsibility and Accountability

Every officer / staff member is accountable for their actions regarding appropriate device acquisition, data review and investigation. It is the individual responsibility of each officer / staff member to ensure they act in accordance with the law and principles outlined.

The Strategic Business Owner, ACC Organised Crime, Counter Terrorism and Intelligence will be responsible for ensuring the information generated by digital forensic systems is protected and managed responsibly.

Detective Superintendent Cybercrime is responsible for the daily management, operation and use of the examinations systems. Responsibilities include compliance audits, data quality and escalating issues to the Strategic Business Owner.

Detective Chief Inspector, Cybercrime manages the users of the systems, local administration, in-life management of the systems and the information processed on them.

Definitions

A **production** is an article, document or other thing which has been appropriated by the police as it is believed to potentially be relevant in some way to a police investigation or incident. It is the evidence of material things including data, as opposed to the oral testimony of witnesses.

A **digital device** means any electronic device that can receive, store, process or send digital information and includes but is not limited to any mobile phone, lap top, computer, smart device, satellite navigation system, SD Card, USB, hard drive, digital camera etc.