

Cybercrime First Responder Guide

National Guidance

## Notice:

This document has been made available through the Police Service of Scotland Freedom of Information Publication Scheme. It should not be utilised as guidance or instruction by any police officer or employee as it may have been redacted due to legal exemptions

Owning Department: Policing in a Digital World Programme

Version Number: 1.0

Date Published: 13/05/2022

## Introduction/purpose

This Cybercrime First Responder Guide has been compiled by Police Scotland Policing in a Digital World Programme and has been written to reflect both Scottish Legislation and current Cybercrime investigation techniques.

It is intended to provide police personnel at all levels with the skills and information required to investigate Cybercrime, including the identification and extraction of material that may be of evidential value.

## Cybercrime Definition

### Cyber-Enabled Crime

The commission or attempted commission of traditional crimes such as theft, fraud, extortion, threats, etc. using the internet, or by otherwise accessing a computer system, device or network.

Common types of Cyber-Enabled crime include, but are not limited to:

* Abuse - Twitter, Facebook, Instagram, WhatsApp etc.
* Threats via email.
* Online fraud and other economic crime.
* Theft from online bank accounts.
* Sexual exploitation and sextortion.
* Grooming and offences against children as included in the Sexual Offences (Scotland) Act 2009.
* Stalking.

Note: Cyber-Enabled crimes include common law and statutory offences.

### Cyber-Dependent Crime

The commission or attempted commission of crime in order to compromise a computer device, network or system where the devices are both the tool for committing the crime and the target of the crime.

Common types of Cyber-Dependent crime include, but are not limited to:

* Creating, selling, distributing or deploying Computer Viruses, Malware (malicious software) or Trojans with nefarious intent.
* Attacking or impairing the normal use of a website – Distributed Denial of Service (DDoS).
* Hacking/network intrusion/account takeover or any other unauthorised access of Information and Communications Technology (ICT).
* Corrupting or controlling a system via email or other means.

Note: The majority of Cyber-Dependent crimes are offences under the Computer Misuse Act 1990.

### Markers

Where appropriate, the Cybercrime marker should be applied as follows:

* **Storm/C3** - The ‘Cybercrime’ tag should be applied.
* **SID** - The subject heading ‘Cybercrime’ should be added.
* **Crime recording systems** - In line with local procedure – for example, by adding as a ghost nominal, marker, or aggravator.

## Cybercrime Harm Prevention Advice

Often, First Responders will be dealing with members of the public where as well as taking investigatory actions, they may be asked for, or wish to provide preventative and cyber safety advice.

Police Scotland’s Cybercrime Harm Prevention Team which is based across the North, East and West of Scotland work closely with Police Scotland's Cybercrime Investigations Unit and partners in the public, private and third sectors to deliver Cybercrime prevention advice and online safety guidance.

The Cybercrime Harm Prevention Team liaise with the Scottish Government, National CYBER Prevent/CYBER Protect Networks and Regional Organised Crime Units to share best practice, develop our understanding of emerging cyber and digital crime threats, and trends providing the most up to date information for officers.

The Cybercrime Harm Prevention Team have developed The Cybercrime Harm Prevention & Online Safety Advice guide. The guide provides police officers and police staff with advice, information and links to useful websites and resources which can be disseminated to victims or witnesses of crime.

Some of the topics covered by the guide include but are not limited to;

* Securing your passwords and Two-Factor Authentication (2FA).
* Securing your device and data.
* Social Media.
* Understanding your digital footprint.
* Online gaming.
* Parental controls and staying safe online for children.
* Cyber Security advice for businesses and charities.
* Common cyber problems and FAQs including fraud, identity theft, suspicious text/calls/emails.

Any additional instruction included in geographical appendices must be considered carefully and only include information that is materially different from the main content of the document.

## Preserving Evidential Integrity of Data – General Principles

The ‘ACPO Good Practice Guide for Digital Evidence’ has been adopted by the National Police Chiefs Council (NPCC) as well as by Police Scotland. It provides national, best practice for dealing with electronic evidence. There are four general principles that an investigator must adhere to in order for the evidential integrity of the data to be preserved.

**Principle 1:** No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.

**Principle 2:** In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

**Principle 3:** An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

**Principle 4:** The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

## Lawful Authority for Seizure of Digital Devices

The fragility of digital data is such that it can easily be damaged or destroyed. Therefore, measures will need to be taken if its evidential integrity is to be preserved.

The lawful authority for seizure and examination of digital devices is outlined in Legal Basis for the Seizure and Examination of Digital Devices which covers the legal basis for the seizure and examination of digital devices. The four authorities for seizure are:

* Under statutory power;
* Where consent is provided (victims and witnesses only);
* Where there is a warrant; or
* Where there is urgency (common law power).

In all cases the best evidence will be the digital device on which evidence is stored. However, in routine cases or when dealing with low level crime, a victim or witness may not give consent for their digital device to be seized and examined, and the use of an alternative power may not be proportionate.

In such cases, whilst remaining cognisant of the potential for the original data to be altered, it may be more appropriate to obtain a copy of the data either via a screenshot, recording, or print out.

### Suspects (Not Officially Accused) or Accused Persons

Search, seizure and examination of a digital device from a suspect or accused will only be conducted when lawful. It can only be done where there is an express statutory power, a warrant expressly conferring such a power, or a power at common law.

Consent isnot applicable to suspects/accused.

### Victims and Witnesses

The authorities for taking a digital device for the purpose of examination from a victim or witness are:

* By consent;
* Under warrant;
* At common law (urgency).

### Consent

Consent is only applicable to victims and witnesses – not suspects and accused. In the absence of urgency (common law) or a warrant, police have no power to compel a victim or witness of crime to hand over their digital device for examination or to seize it from them. In these circumstances therefore, police require their consent.

Where practicable the First Responder should seek cooperation and consent from the victim or witness to secure the device in order that any evidence can be acquired forensically.

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.

In terms of these 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.

The Police Scotland, Digital Device Consent Public Information Leaflet will be provided to the victim or witness in all such cases. Where required to ensure understanding, further explanation must also be provided.

Although the wishes of the victims and witnesses will be taken into account when deciding on the extent of any examination, it should be noted that police have to make a decision in line with the wider circumstances of the investigation, and it may not therefore always be possible to limit the examination to that stipulated by the victim/witness.

 Where consent cannot be obtained, the First Responder must consider whether it is appropriate to obtain a warrant or use common law powers (urgency) in order to seize the device.

### Withdrawal of Consent

Victims or witnesses who have given their consent to have their devices seized and examined also have the right to withdraw their consent at any time. To do so they need merely attend a police station or call 101.

There may be some situations when consent is withdrawn but it is not suitable for a victim or witness to have their device returned to them. In such cases a First Responder should look to retain the digital device by means of an alternative power. Full details can be found in the Digital Device – Consent – Officer Guidance document.

### Statutory Power

An example of a statutory power to seize a digital device without warrant is under Section 47 and Section 48 of the Criminal Justice (Scotland) Act 2016 which permits a police constable to search without warrant any arrested person and seize any item in their possession whether they have been charged with an offence or not.

### Common Law (Urgency)

In circumstances where there is imminent danger of potential evidence being lost or destroyed police can use powers at common law to seize and examine a digital device.

Whilst there is no specific guidance as to the circumstances under which this would be deemed competent for a digital device, the concept of police permission to overcome the security of property was explored in Paton v Dunn 2012 (HCJAC) 49, with the Court stating;

“The question will generally be whether the police officers had reasonable grounds for taking the intrusive step they did of forcing entry to a private dwelling. Such a major invasion of privacy requires justification as a necessary and proportionate act having regard to the prevailing circumstances.”

Taking this approach to secure the device may be necessary and proportionate in circumstances where there is a risk that evidence which might be essential to establishing a serious offence, could be lost or where there is a risk to life if the device is not seized immediately.

There should be careful consideration of the circumstances prior to taking this approach.

More information on the legal basis for digital device seizure and examination can be found within the Digital Device Seizure and Examination Legal Basis document on the Police Scotland intranet. In certain circumstances an officer may be allowed to manually examine a device. However, contact your local Cybercrime Digital Forensic Unit/Cyber On-Call for advice; and refer to Police Scotland Memorandum 007-21 as to when you may be authorised to do so.

### Warrants

Where there is a reasonable cause to suspect that a digital device contains evidence relating to a crime or incident under investigation, and urgency or consent (consent only being applicable to victims and witnesses) are not appropriate, police can apply to the court for a warrant authorising them to search for, take possession of and examine a digital device for the purposes of that investigation.

## Search Guidance

**Information has been removed due to its content being exempt in terms of**

**the Freedom of Information (Scotland) Act 2002, Section 35, Law**

**Enforcement.**

## How to Seize a Computer or Laptop – Switched Off

**Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 35, Law**

**Enforcement.**

## 8. How to Seize a Computer or laptop – Switched On

**Information has been removed due to its content being exempt in terms of**

**the Freedom of Information (Scotland) Act 2002, Section 35, Law**

**Enforcement.**

## 9. Home Networks – Overview

**Information has been removed due to its content being exempt in terms of**

**the Freedom of Information (Scotland) Act 2002, Section 35, Law**

**Enforcement.**

## 10. How to Seize a Mobile Telephone or Tablet

**Information has been removed due to its content being exempt in terms of**

**the Freedom of Information (Scotland) Act 2002, Section 35, Law**

**Enforcement.**

## 11. The Internet of Things

**Information has been removed due to its content being exempt in terms of**

**the Freedom of Information (Scotland) Act 2002, Section 35, Law**

**Enforcement.**

## 12. Cloud Storage

**Information has been removed due to its content being exempt in terms of**

**the Freedom of Information (Scotland) Act 2002, Section 35, Law**

**Enforcement.**

## 13. Use of Older Devices for ‘Secure’ Storage

**Information has been removed due to its content being exempt in terms of**

**the Freedom of Information (Scotland) Act 2002, Section 35, Law**

**Enforcement.**

## 14. Cryptocurrency

**Information has been removed due to its content being exempt in terms of**

**the Freedom of Information (Scotland) Act 2002, Section 35, Law**

**Enforcement.**

## 15. Securing CCTV Evidence

**Information has been removed due to its content being exempt in terms of**

**the Freedom of Information (Scotland) Act 2002, Section 35, Law**

**Enforcement.**

## 16. Capture of Source Material

**Information has been removed due to its content being exempt in terms of**

**the Freedom of Information (Scotland) Act 2002, Section 35, Law**

**Enforcement.**

## 17. Offences and Relevant Legislation

This section is intended as a summarised overview only and to provide awareness of relevant legislation. Please refer to Police Scotland Legal Database for full legislation & Police powers.

### Computer Misuse Act 1990

S1 - Unauthorised Access to Computer Material.

It is an offence to cause a computer to perform any function with intent to gain unauthorised access to any program or data held in any computer.

S2 - Unauthorised Access with Internet to Commit Other Offence.

This offence is committed where an offence is committed as per S1, but the offence is committed with the intention of committing or facilitating a further offence, whether alone or with another.

S3 - Unauthorised acts with intent to impair a computer.

An offence is committed if any person does an unauthorised act with the intention of impairing the operation of any computer.

S3A - Making, Supplying or Obtaining Article for use in S1 or S3 offences.

The Police and Justice Bill 2006 created a new S3A offence of making, supplying (including offers to supply) or obtaining articles for use in S1 or S3 computer misuse offences.

### Civic Government (Scotland) Act 1982

S51 - Obscene Material

An offence for any person to display obscene material in a public place; or sells, distributes, makes, keeps, has obscene material for eventual sale or distribution.

S51A - Extreme Pornography

An offence for any person in possession of an extreme pornographic image.

S51B - Extreme pornography: excluded Images.

An offence is not committed under S51 if the image is an excluded image.

S52 - Indecent Child Photographs.

An offence for any person who takes, permits to be taken or makes; distributes or shows; has in possession; publishes or causes to be published - any indecent photograph or pseudo-photograph of a child.

S52A - Possession of Photographs

An offence for a person to have any indecent photograph or pseudo-photograph of a child in his possession.

### Sexual Offences (Scotland) Act 2009

(Grooming Offences etc.).

S31 - Causing an older child to participate in a sexual activity.

An offence for person who has attained age of 16 years to intentionally cause child who has attained age of 13 years but not attained age of 16 years, to participate in a sexual activity.

S32 - Causing an older child to be present during a sexual activity

An offence for person who has attained age of 16 years who intentionally engages in sexual activity in the presence of a child who has attained age of 13 years but not attained age of 16 years, or causes said child to be present whilst a third person engages in such activity.

S33 - Causing an older child to look at a sexual image.

An offence for person who has attained age of 16 years to intentionally cause child who has attained age of 13 years but not attained age of 16 years, to look at sexual images.

S34 - Communicating indecently with an older child etc.

An offence for a person who has attained age of 16 years to intentionally sends by whatever means, a sexual written communication to, or directs by whatever means a sexual verbal communication to, a child who has attained age of 13 years but not attained age of 16 years.

### Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005

S1 - Meeting a child following certain preliminary contact.

A person commits an offence if, person ‘A’ having communicated with person ‘B’ (who is under 16 years or is a constable) on at least one earlier occasion intentionally meets B, travels with the intention of meeting B, or arranges for B to meet A; and intends to engage in unlawful sexual activity involving B or in presence of B during or after meeting in any part of the world. Person A must reasonably believe that B is not 16 or over, and the meeting or communication on an earlier occasion must have a relevant Scottish connection, and Person A must be a British citizen or resident in the UK.

### Communications Act 2003

Section 125 - Dishonestly obtained electronic communication services. It is an offence to dishonestly obtain the use of an electronic communication service with intent to avoid payment of the charge applicable to that service. (This would cover the unauthorised use of another person’s Wireless Internet).

Section 126 - Possession or supply of apparatus etc. for contravening S125.

It is an offence to possess, supply or offer to supply anything in order to dishonestly obtain such a service or in connection with obtaining such a service.

Note: Broadcasting Services (Cable TV Services etc.) have been specifically excluded from the offences under sections 125 and 126 because they are covered by other offences under Section 297(1) Copyright, Designs & Patents Act 1998.

Section 127 - Improper use of a public electronic communications networks.

It is an offence if anyone sends a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or causes any such matter to be sent. If for the purpose of causing annoyance, inconvenience or needless anxiety to another sends a message that he knows to be false; or causes such a message to be sent or persistently makes use of a public electronic communications network.

## 18. Additional Resources

### Child Exploitation and Online Protection Service (CEOP):

CEOP is here to keep children safe from sexual abuse and grooming online. CEOP provides Internet Safety advice and how to make a report.

https://www.ceop.police.uk/Safety-Centre/

**Have I Been Pwned?**

Website allowing you to input an email address or phone number to see if it has been compromised as part of a known data breach.

https://haveibeenpwned.com

**Internet Watch Foundation (IWF):**

The Internet Watch Foundation (IWF) is the UK internet Hotline for anyone to report online child sexual abuse imagery and non-photographic child sexual abuse images anonymously. IWF works internationally to make the internet safer. They help victims of child sexual abuse worldwide by identifying and removing online images and videos of their abuse. Don’t ignore it, report it!

https://www.iwf.org.uk/

**Stop It Now! UK and Ireland:**

Stop It Now! is at the forefront of activity to prevent child sexual abuse. Campaigning and awareness raising are essential tasks for local, regional and national projects in order to empower and enable adults to address personal, family and community concerns.

http://www.stopitnow.org.uk/

**Think you Know:**

An education programme for advice about staying safe when you’re on a phone, tablet or computer.

www.thinkuknow.co.uk

**Home Activity Packs:**

Download home activity packs with simple 15-minute activities for your child to support their online safety at a time when they will be spending more time online at home.

www.thinkuknow.co.uk/parents/Support-tools/homeactivity-worksheets

**Internet Matters:**

Get expert support and practical tips to help children benefit from connected technology and the internet safely and smartly.

www.internetmatters.org

**Project Evolve:**

Resources to equip children and young people for digital life.

www.projectevolve.co.uk

**UK Safer Internet Centre:**

Promote the safe and responsible use of technology for young people and provide online safety tips, advice and resources to help children and young people stay safe online.

www.saferinternet.org.uk

**Childline:**

Childline is a free and confidential service for children and young people. You can phone them on 0800 11 11 or you can visit their website.

www.childline.org.uk

**NSPCC:**

If you are an adult and worried about a child you can call the 24-hour NSPCC helpline on 0808 800 5000 or visit their website.

www.nspcc.org.uk

**ParentLine Scotland:**

Call 08000282233 or email: parentlinescotland@children1st.org.uk Parent Line’s opening hours are from 9am-10pm (Mon-Fri) and 12 noon-8pm at weekends.

**Crimestoppers:**

Call 0800 555 111 or visit their website

www.crimestoppers-uk.org

**Cyber Aware:**

• Internet Safety Advice
• Crime Prevention Advice Personal & SME’s
• Free anti-virus software.
• Cyber Essentials for Business

http://www.cyberstreetwise.com

**Spamhaus:**

• Information and advice about SPAM email

www.Spamhaus.org

**APWG:**

• Anti-Phishing Working Group

www.APWG.org

## 19. Key Contacts

**Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 30 – Prejudice to effective conduct of public affairs.**

## Compliance record

EqHIRA completion/review date: 02/05/2022

Information Management Compliant: Yes/No

Health and Safety Compliant: Yes/No

## Version control table

| Version | History of amendments | Approval date |
| --- | --- | --- |
| 1.00 | Initial Approved Version | 13/05/2022 |

## Feedback

All Police Scotland service delivery Policies, Standard Operating Procedures (SOPs) and National Guidance are subject to regular reviews. It is important that user feedback is taken into account when documents are reviewed.

If any officer / staff member wishes to provide comment, or make suggestions for improvements to this or any associated document, Force Form 066-014 should be used.