

# 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: V2.00

Date Published: 08/03/2024

Contents

[Cybercrime First Responder Guide 1](#_Toc171066557)

[1. Introduction/purpose 4](#_Toc171066558)

[2. Cybercrime Definition 4](#_Toc171066559)

[Cyber-Enabled Crime 4](#_Toc171066560)

[Cyber-Dependent Crime 5](#_Toc171066561)

[Markers 5](#_Toc171066562)

[3. Cybercrime Harm Prevention Advice 5](#_Toc171066563)

[4. Preserving Evidential Integrity of Data - General Principles 6](#_Toc171066564)

[Police Scotland’s Digital Device Examination Principles 7](#_Toc171066565)

[5. Lawful Authority for Seizure of Digital Devices 7](#_Toc171066566)

[Suspects (Not Officially Accused) or Accused Persons 8](#_Toc171066567)

[Victims and Witnesses 8](#_Toc171066568)

[Digital Device Examination by Agreement – Victims and Witnesses 8](#_Toc171066569)

[Capturing Agreement for Device Examination 9](#_Toc171066570)

[Withdrawal of Agreement to Device Examination 10](#_Toc171066571)

[Statutory Power 11](#_Toc171066572)

[Common Law (Urgency) 11](#_Toc171066573)

[Warrants 12](#_Toc171066574)

[17. Offences and Relevant Legislation 13](#_Toc171066575)

[Crimes against the Person 13](#_Toc171066576)

[Computer Misuse Act 1990 13](#_Toc171066577)

[Civic Government (Scotland) Act 1982 13](#_Toc171066578)

[Sexual Offences (Scotland) Act 2009 13](#_Toc171066579)

[Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005 14](#_Toc171066580)

[Communications Act 2003 14](#_Toc171066581)

[18. Additional Resources 14](#_Toc171066582)

[Child Exploitation and Online Protection Service (CEOP) 14](#_Toc171066583)

[Have I Been Pwned? 14](#_Toc171066584)

[Internet Watch Foundation (IWF) 14](#_Toc171066585)

[Stop It Now! UK and Ireland 15](#_Toc171066586)

[Think you Know 15](#_Toc171066587)

[Home Activity Packs 15](#_Toc171066588)

[Internet Matters 15](#_Toc171066589)

[Project Evolve 15](#_Toc171066590)

[UK Safer Internet Centre 16](#_Toc171066591)

[ChildLine 16](#_Toc171066592)

[National Society for the Protection of Cruelty to Children (NSPCC) 16](#_Toc171066593)

[Parentline Scotland 16](#_Toc171066594)

[Crimestoppers 16](#_Toc171066595)

[Cyber Aware 17](#_Toc171066596)

[Spamhaus: 17](#_Toc171066597)

[APWG: 17](#_Toc171066598)

[Compliance record 17](#_Toc171066599)

[Version control table 18](#_Toc171066600)

[Feedback 18](#_Toc171066601)

## Introduction/purpose

This Cybercrime First Responder Guide has been compiled by Police Scotland’s 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

Cybercrime is not a crime but a crime type. Cybercrime has two categories which assist in understanding what type of Cybercrime is being referred to. Anything that can be categorised under either of these headings is Cybercrime:

### 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 - X, 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 – Denial of Service (DoS).
* 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, Cybercrime markers should be applied as follows:

* STORM Unity- The ‘Cybercrime’ tag should be applied.
* SID- The subject heading ‘Cybercrime’ should be added.
* UNIFI – The ‘Cybercrime’ tag should be applied.

## 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 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 Frequently Asked Questions (FAQs) including fraud, identity theft, suspicious text/calls/emails.

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.

## 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.

### Police Scotland’s Digital Device Examination Principles

Police Scotland also has its own set of principles which also must be followed when taking and examining a digital device from any person, including any data extracted from it. These are outlined in Digital Device Examination - Principles.

## 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. The four authorities for seizure are:

* Under statutory power.
* By agreement (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 agree 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.

Where copies have been obtained cognisance should be taken to requirements under Schedule 8 of the Criminal Procedure (Scotland) Act 1995.

### 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.

### Victims and Witnesses

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

* By agreement.
* Under warrant.
* At common law (urgency).

### Digital Device Examination by Agreement – Victims and Witnesses

#### Background

In 2020 Police Scotland reformed how agreement for digital device examination was obtained and recorded from victims and witnesses of crime. This was to ensure full understanding regarding the right to refuse or withdraw their agreement for examination to be conducted on their devices, and to explain how digital evidence might be used to progress investigations.

On Tuesday 8th November 2022 The Police, Crime, Sentencing and Court Act 2022 (‘the Act’) came into force. Chapter 3 sets in law the rights of victims and witnesses of crime when providing electronic devices to police for the purposes of digital forensic examination.

Section 39 Subsection 3 of the Act requires that the victim/witness (or suitable responsible person in the case of a child) be provided the following information in writing:

1. specifying or describing the information that is sought;
2. specifying the reason why the information is sought;
3. specifying how the information will be dealt with once it has been extracted.
4. stating that the owner may refuse to provide the device or agree to the extraction of information from it and;
5. stating that the investigation or enquiry for the purposes of which the information is sought will not be brought to an end merely because the owner refuses to provide the device or agree to the extraction of information from it.

In order to comply with this new legislation, Police Scotland have developed a Digital Device Processing Notice which must be completed whenever devices are seized from victims or witnesses of crime with their express agreement. A separate form must be completed for each device.

### Capturing Agreement for Device Examination

Digital devices should only be taken/seized from victims and witnesses where there is reasonable belief, they may contain evidence or information relating to an investigation or incident.

Any subsequent examination must also be necessary, proportionate, relevant and legitimate in relation to the investigation of the crime/incident being undertaken.

Taking digital devices for examination by agreement with the owner/user will only ever be applicable to victims and witnesses. Officers should be mindful however, that victims/witnesses are under no obligation to agree to provide their device.

This does not affect how an enquiry should be treated and the investigation of all other reasonable lines of enquiry should be pursued.

* When seeking to obtain an electronic device from a victim/witness by agreement, officers must complete a Digital Device Processing Notice (DPN) and provide a copy of this to the victim/witness.
* This form ensures that the victim/witness is fully aware of why examination of their device is necessary to progress the investigation, what will happen to their device and their right to refuse consent or withdraw their agreement at any time.
* One form must be completed in full for each device and lodged as a case related document on the UNIFI productions system.
* The decision regarding whether or not the victim or witness agrees to provide their device for examination should be recorded in any official police statement.
* If the victim or witness is not willing to provide their device (in the absence of urgency or a warrant) then there is no lawful basis to take or examine it.
* For the purposes of this legislation a child is defined as under 18 years of age. A child cannot agree to provide a device for data to be extracted and a parent / guardian / responsible authority must be consulted on their behalf.

When the Digital Processing Notice is completed a scanned copy of each signed form must be emailed to the Cybercrime Gateway. No Electronic Request Form (ERF) featuring a device seized by agreement can be approved without the Gateway having a copy of the relevant DPN.

### Withdrawal of Agreement to Device Examination

Victims or witnesses who have agreed to have their devices seized and examined also have the right to withdraw their agreement at any time. Agreement can be withdrawn, and the return of the device requested at any time by a victim or witness by;

* Contacting the investigating officer.
* Calling 101 or;
* Attending at a Police Station.

The Digital Device Examination Agreement Withdrawal Form must be completed by the officer or staff member who receives the request.

As with refusal there may be times that Police Scotland need to keep the device despite withdrawal of an agreement for the device to be examined; in these cases one of the other powers (warrant or common law) must be used.

If agreement for examination is withdrawn prior to data being extracted, and warrant or common law are not used, information will not be taken from the device and it may be returned to the owner.

If agreement is withdrawn after the extraction of information has taken place, it may not be possible to delete the data or return the device as it could form a crucial part of the evidence in the case.

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.

In all cases extracted information and the device will only be retained where there is a lawful basis to do so and only for as long as necessary.

### 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 Cybercrime Gateway/Cyber On-Call for advice; and refer to Police Scotland Memorandum PS 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 agreement (agreement 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.

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 and police powers.

### Crimes against the Person

* Threats and Extortion

### Computer Misuse Act 1990

* S1 - Unauthorised Access to Computer Material.
* S2 - Unauthorised Access with Internet to Commit Other Offence.
* S3 - Unauthorised acts with intent to impair a computer.
* S3ZA – Unauthorised acts causing, or creating risk of, serious damage
* S3A - Making, Supplying or Obtaining Article for use in S1 or S3 offences.

### Civic Government (Scotland) Act 1982

* S51 - Obscene Material
* S51A - Extreme Pornography
* S51B - Extreme pornography: excluded Images.
* S52 - Indecent Child Photographs.
* S52A - Possession of Photographs

### Sexual Offences (Scotland) Act 2009

* S31 - Causing an older child to participate in a sexual activity.
* S32 - Causing an older child to be present during a sexual activity
* S33 - Causing an older child to look at a sexual image.
* S34 - Communicating indecently with an older child etc.

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

* S1 - Meeting a child following certain preliminary contact.

### Communications Act 2003

* S125 - Dishonestly obtained electronic communication services.
* S126 - Possession or supply of apparatus etc. for contravening S125.
* S127 - Improper use of a public electronic communications networks.

## 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.

Child Exploitation and Online Protection Service (CEOP) Website

### 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.

Have I Been Pwned? Website

### 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!

Internet Watch Foundation (IWF) Website

### 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.

Stop It Now! UK and Ireland Website

### Think you Know

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

Think you Know Website

### 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.

Home Activity Packs Download Page

### Internet Matters

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

Internet Matters Website

### Project Evolve

Resources to equip children and young people for digital life.

Project Evolve Website

### 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.

UK Safer Internet Centre Website

### 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.

Childline Website

### National Society for the Protection of Cruelty to Children (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.

NSPCC Website

### Parentline Scotland

Call 08000 28 22 33 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.

Crimestoppers Website

### Cyber Aware

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

Cyber Aware Website

### Spamhaus:

Information and advice about SPAM email.

Spamhaus Website

### APWG:

Anti-Phishing Working Group

APWG Website

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

EqHRIA completion/review date: 06/03/2024

Information Management Compliant: Yes

Health and Safety Compliant: Yes

## Version control table

| Version | History of amendments | Approval date |
| --- | --- | --- |
| 1.00 | Initial Approved Version | 13/05/2022 |
| 2.00 | Insertion of guidance regarding:  - Legally Professionally Privileged material.  - Section 49 RIPA 2000  - Unmanned Arial Vehicles/ UAV (Drones)  - Guidance regarding seizure of Cryptocurrency under POCA 2002  Amendments to guidance regarding:  - witness/victim “consent” to “agreement and associated processes for capturing and withdrawing agreement.  - CCTV seizure guidance.  - Contact details for Key Contacts.  - Replacement of Twitter with X  - Hyperlinks updated.  - Minor grammar | 06/03/2024 |

## 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.