| Police Scotland logo | Freedom of Information ResponseOur reference: FOI 24-2752Responded to: 19 November 2024 |
| --- | --- |

Your recent request for information is replicated below, together with our response.

**I would like to request the following information for the period from January 1, 2019, to December 31, 2023**

**1. Breakdown of Crime Types: A breakdown of the types of crimes for which digital forensic analysis was conducted, including but not limited to the following categories:**

 **- Hacking and Unauthorized Access**

 **- Online Fraud (e.g., phishing, financial fraud)**

 **- Ransomware and Malware Attacks**

 **- Child Sexual Exploitation or Grooming**

 **- Terrorism-related Offences**

 **- Cyberstalking or Harassment**

 **- Data Breaches and Identity Theft**

 **- Drug Trafficking or Distribution involving digital evidence**

 **- Intellectual Property Theft or Copyright Infringement**

 **- Sextortion or Blackmail**

 **- Other types of cybercrime not covered in the above categories**

**2. Number of Cases: The number of cases where digital forensic analysis was required for each crime type listed above, broken down by year (2019, 2020, 2021, 2022, and 2023).**

Please note, our Cybercrime Case Management system uses a specified list of ‘Crime Types’ which does not directly align with the categories you have requested.

For Data held prior to 1st July 2019, the information sought is not held by Police Scotland and section 17 of the Act therefore applies. To explain, the crime types on our Cybercrime Management System were standardised in July 2019.

To be of assistance, Please see the table below for a breakdown of Cybercrime Examination Request Forms approved by our Cybercrime Gateway using the following criteria:

| **Crime Type** | **Number of Cybercrime Examination Requests Approved** |
| --- | --- |
| **2019 (1st July onwards)** | **2020** | **2021** | **2022** | **2023** |
| Communication Offences | 323 | 433 | 390 | 366 | 298 |
| Computer Misuse Act | 12 | 7 | 14 | 5 | 4 |
| Drug Supply  | 815 | 1384 | 1568 | 1629 | 1584 |
| Extreme Pornography | 22 | 20 | 12 | 23 | 14 |
| Fraud | 50 | 78 | 62 | 60 | 56 |
| Grooming of Children | 104 | 142 | 128 | 122 | 137 |
| Indecent Images of Children (IIOC) | 344 | 719 | 685 | 657 | 648 |
| National Security | 25 | 9 | 24 | 9 | 19 |
| Sextortion | 11 | 16 | 15 | 21 | 13 |
| Stalking | 146 | 146 | 126 | 110 | 92 |
| Threatening & Abusive Behaviour | 162 | 239 | 231 | 206 | 188 |
| Threats and Extortion  | 32 | 56 | 53 | 35 | 45 |

## 3. Forensic Involvement: For each crime type, please indicate whether the digital forensic analysis was carried out internally by Police Scotland’s forensic units or outsourced to external digital forensic firms/consultants.

Police Scotland do not outsource digital forensic examinations. All cases will be examined internally.

## 4. Success Rates: If available, please provide data on the success rates of retrieving and analyzing digital evidence for each crime type (e.g., percentage of cases where usable digital evidence was successfully obtained).

Unfortunately, I estimate that it would cost well in excess of the current FOI cost threshold of £600 to process your request. I am therefore refusing to provide the information sought in terms of section 12(1) of the Act - Excessive Cost of Compliance.

To explain, in 2023 alone, there were over 3000 Examination Request Forms approved and the only way to provide the information you are requesting would be to manually research each case individually to determine success rates, which would cost well over the threshold set out within the act.

## 5. Trends and Observations: If possible, please include any internal reports or summaries that discuss patterns, trends, or notable changes in the types of crimes requiring digital forensic analysis over the specified period.

I am refusing to confirm or deny whether the information sought exists or is held by Police Scotland in terms of section 18 of the Act.

Section 18 applies where the following two conditions are met:

- It would be contrary to the public interest to reveal whether the information is held

- If the information was held, it would be exempt from disclosure in terms of one or more of the exemptions set out in sections 28 to 35, 38, 39(1) or 41 of the Act.

If the above data was held, the following exemptions would be considered relevant:

**Section 31(1) - National Security and Defence**

Information is exempt information if it is required for purpose of safeguarding national security.

Disclosure would undermine any ongoing or future operations to protect the security or infrastructure of the United Kingdom and increase the risk of harm to the public.

The public entrust the Police Service to make appropriate decisions regarding their safety and protection and the only way of reducing risk is to be cautious with what is placed into the public domain.

**35(1)(a)&(b) – Law Enforcement**

The information requested is exempt, as its disclosure would or would be likely to prejudice substantially the prevention or detection of crime and apprehension or prosecution of offenders.

Disclosure would have an adverse impact on the ability of the Police to carry out its law enforcement role effectively, and thereby prejudice substantially the prevention and detection of crime.

**Section 39(1) – Health, safety and the environment**

Disclosure of the information requested would prove extremely useful for criminals and those intent on wrongdoing. To share information used by specialist departments within Police Scotland would assist them in circumventing the efficient and effective provision of law enforcement by the police service, which in turn would have an adverse impact on the safety of the officers involved and the general public.

This would increase the risk to the personal safety of individuals and also the safety of the police officers responding to incidents.

**Public Interest Test**

As you will be aware, the three exemptions detailed above are non-absolute and require the application of the public interest test. Public awareness may favour disclosure as it would contribute to the public debate surrounding any patterns, trends, or changings in the type of crimes requiring forensic analysis however, providing details of specific patterns, trends or changes in the use of technology to facilitate criminality would significantly increase the risk of criminal actors taking evasive measures to frustrate ongoing and future investigations, such as actively identifying devices which cannot currently be examined by Police Scotland and using these to evade detection / prosecution.

Therefore, I would contend that the efficient/effective conduct of the service and public safety favours retention of the information as it cannot be in the public interest to release information that would prejudice law enforcement, or which is likely to have an adverse impact upon public safety.

If you require any further assistance, please contact us quoting the reference above.

You can request a review of this response within the next 40 working days by email or by letter (Information Management - FOI, Police Scotland, Clyde Gateway, 2 French Street, Dalmarnock, G40 4EH). Requests must include the reason for your dissatisfaction.

If you remain dissatisfied following our review response, you can appeal to the Office of the Scottish Information Commissioner (OSIC) within 6 months - [online](http://www.itspublicknowledge.info/Appeal), by email or by letter (OSIC, Kinburn Castle, Doubledykes Road, St Andrews, KY16 9DS).

Following an OSIC appeal, you can appeal to the Court of Session on a point of law only.

This response will be added to our [Disclosure Log](http://www.scotland.police.uk/access-to-information/freedom-of-information/disclosure-log) in seven days' time.

Every effort has been taken to ensure our response is as accessible as possible. If you require this response to be provided in an alternative format, please let us know.