| Police Scotland logo | Freedom of Information ResponseOur reference: FOI 23-1674Responded to: 13 July 2023 |
| --- | --- |

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

## Digital Evidence Department: a) Does your police force deal with video and image evidence? b) if so, which department deals with it?

In response to this question, I must advise that Police Scotland does not have one single department that manages video and image evidence.

## Software: a) What image and video software is used in this department?

In response to the question above, in terms of Section 16 of the Freedom of Information (Scotland) Act 2002, I am refusing to provide you with the information sought.

Section 16 requires Police Scotland when refusing to provide such information because it is exempt, to provide you with a notice which:

(a) states that it holds the information,

(b) states that it is claiming an exemption,

(c) specifies the exemption in question and

(d) states, if that would not be otherwise apparent, why the exemption applies.

The exemptions that I consider to be applicable to the information requested by you are:

Section 31(1) – National Security and Defence

Section 35(1)(a)&(b) – Law Enforcement

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

Section 31(1) – National Security and Defence

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

Disclosure of information relating to software used to detect crime could 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 with regard to their safety and protection and the only way of reducing risk is to be cautious with what is placed into the public domain.

This is a non-absolute exemption and requires the application of the Public Interest Test.

Section 35(1)(a)&(b) – Law Enforcement

If the information was disclosed it could assist groups, organisations, and those with hostile intent to identify, with some accuracy, Police Scotland’s technological capabilities and take steps to attack or hijack known vulnerabilities to Police systems directly or the supply chain. To provide the requested data could assist those with intent on doing harm with a tactical advantage when planning or perpetrating criminal plans and unlawful activities and maximise the impact of destruction, harm and disruption that may be caused.

Disclosure could have a negative effect on national security should the release of information be used and manipulated by criminal fraternities to try and attack public figures and other protected establishments and individuals.

Information is exempt information if its disclosure under this Act would or would be likely to prejudice substantially the prevention or detection of crime and the apprehension or prosecution of offenders.

This is a non-absolute exemption and requires the application of the Public Interest Test.

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

Disclosure of information relating to software used to detect crime may have the potential to increase the number of attacks on public figures, operational police officers and members of the public and the potential to present a risk to an individual’s personal safety.

Public Interest Test

I would suggest that public accountability may favour disclosure, given that the information concerns the efficient and effective use of resources by the Service. Likewise, disclosure of the information would also inform the public debate on the issue of policing and contribute to the accuracy of that debate.

However, any disclosure under FOI legislation is a disclosure to the world at large and any information identifying the focus of policing activity could be used to the advantage of criminals.

Consequently, in terms of the applicability of the exemptions listed above, the need to ensure the effective conduct of the service in relation to prevention and detection of crime and the public safety considerations involved in the delivery of operational policing clearly favour non-disclosure of the information requested.

It is important to note that the UK faces a serious and sustained threat from violent extremists and this threat is greater in scale and ambition than any terrorist threats in the past. The police service has a duty to promote the safety of all individuals, whether protected or not, and will not reveal any information that might jeopardise this goal. To provide details of resources allocated to their protection is likely to place individuals at serious and increased risk.

Accordingly, I would argue that the need to ensure the efficient and effective conduct of the service favours non-disclosure of the information requested and on balance is significantly in the public interest. I cannot identify any corresponding viewpoint in disclosing the requested information and therefore the exemptions are upheld.

I must advise you that it is doubtful it could ever be in the public interest to disclose information which would jeopardise the delivery of policing and the safety of individuals and prejudice the prevention or detection of crime.

## Challenges and limitations: a) What are the main issues you find with Video evidence? For example, underexposure or blur image/videos?

In response to this question, I must respond in terms of Section 8 of the Freedom of Information (Scotland) Act 2002. Section 8 states that a request must seek recorded information. This question requests an opinion and as such is considered invalid.

## Training and Expertise: a) Has your police force provided training to digital forensic staff on the use of Video Editing software? If yes, please provide details on the type of training given.

In reply to this question, I must refer you to the response within question 2. To identify training types may risk identifying any software used. I can advise however that Police Scotland officers are trained to use the software systems designed to assist with the recording of and the detection of crime.

## Amped Five: Do you use the software Amped FIVE in your department? if not, why is this and do you use external providers? b) if used, what factors influenced the decision to acquire Amped FIVE?

##  Frequency and Scope of Use: a) How frequently is Amped Five used within your police force's digital forensic investigations? b) In what types of cases or scenarios is Amped Five typically employed? c) Are there any specific features or capabilities of Amped Five that are particularly valuable in your investigative processes?

## Collaboration and Support: a) Does your police force collaborate with other law enforcement agencies or organizations in using Amped Five for digital forensic investigations? b) Do you have any established relationships or partnerships with Amped Software for technical support, updates, or feedback?

## Outcomes and Admissibility: a) Can you provide information on any cases where the use of Amped Five has contributed to successful outcomes or convictions? b) Have there been any instances where the results or findings obtained through the use of Amped Five have been challenged in court? If so, please provide brief details.

In response to questions 5 to 8, 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

The following exemptions are considered relevant:

Section 31(1) – National Security and Defence

Section 35(1)(a)&(b) – Law Enforcement

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

Disclosure of the requested information, if held, would substantially prejudice the ability of Police Scotland to safeguard National Security, ensure the prevention and detection of crime and the apprehension or prosecution of offenders while ensuring the safety of members of the public.

This explanation should not be taken as indicative or conclusive evidence that the information you have requested does or does not exist.

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.