| Police Scotland logo | Freedom of Information Response Our reference: FOI 23-0661  Responded to: XX March 2023 |
| --- | --- |

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

## 1. Indicate whether Police Scotland recognises the lay designation of “cybercrime expert” and, if so, which officers or staff this might apply to – e.g., officers or staff operating in the Serious and Organised Crime Financial Investigation Unit

Whilst Police Scotland does have a dedicated Cybercrime Unit, local territorial divisions within Police Scotland also have officers who deal with cybercrime prevention and investigation. These officers will not be solely dedicated to cybercrime prevention and investigation for their role and will have other duties to conduct. Police Scotland do not record how much of a shift each officer dedicates to each enquiry and so it is not possible to collate what proportion of work conducted by particular officers would need to be included in those figures. Simply, we do not record the information required at a level which would allow your request to be answered.

As such, in terms of Section 17 of the Freedom of Information (Scotland) Act 2002, this represents a notice that the information requested is not held by Police Scotland.

## 2. How many a) officers and b) staff who might be considered “cybercrime experts” are currently employed by Police Scotland.

The requested information is considered to be exempt in terms of the Freedom of Information (Scotland) Act 2002 (the Act). Section 16 of the Act requires Police Scotland 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.

Where information is considered to be exempt, this letter serves as a Refusal Notice that information is held and an explanation of the appropriate exemption is provided.

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

Section 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. If the details of Police Scotland’s cybercrime resourcing was disclosed, experience has shown that it would allow those intent on committing crime or causing disorder to gauge the likelihood of detection or to take measures to negate the likelihood of detection. It would allow criminals to plan how best to engage or occupy existing police resources in an effort to maximise their chances of committing serious crime, therefore harming the efficient and effective conduct of the service.

Such information would prove extremely useful information for persons involved in criminality as they would be able to plan and conduct their activities to avoid detection. It would confirm the resources available in a specialised area of policing, which would allow those intent on wrong doing to judge the police response to a variety of incidents. In turn this would prejudice substantially the ability for our officers to prevent and detect crime and apprehend or prosecute 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.

This is a non-absolute exemption and requires the application of the public interest test.

Section 39(1) – Health, safety and the environmentDisclosure of the information requested would prove extremely useful for criminals and those intent on wrongdoing, to estimate the level of cybercrime resources deployed by the Police and 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.

This is a non-absolute exemption and requires the application of the public interest test.

Public Interest Test  
As you will be aware, the two exemptions detailed above are non-absolute and require the application of the public interest test. Public awareness would favour a disclosure as it would contribute to the public debate surrounding the use and deployment of unit and vehicle resources by the Police, particularly specialist vehicles.

I would, however, 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.

## 3. How many a) officers and b) staff who might be considered “cybercrime experts” have been i) recruited to or ii) promoted to positions where their remit includes the investigation of cybercrime.

I can advise that Police Scotland have no record of any job adverts being posted in relation to cybercrime investigation in the last five years. As noted in my response to Q1 above, local territorial divisions also employ officers and staff in relation to cybercrime but as they may not be specifically dedicated to this single role and you have asked for ‘cybercrime experts’ i.e. those responsible specifically for cybercrime investigation, they have not been considered for this question.

Furthermore, even if amended, any similar request would likely be subject to the exemptions detailed in our response to Q2.

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](mailto:foi@scotland.police.uk) 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](mailto:enquiries@itspublicknowledge.info) 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.