Our Ref: IM-FOI-2022-0522
Date: 17 March 2022

FREEDOM OF INFORMATION (SCOTLAND) ACT 2002

I refer to your recent request for information which has been handled in accordance with the Freedom of Information (Scotland) Act 2002.

For ease of reference, your request is replicated below together with the response.

Since 2020, there has been a notable increase nationwide in the expansion and recruitment of Digital Forensics Units in the United Kingdom and Channel Islands.

I appreciate some forces deliver Digital Forensic capabilities in different ways, with some 'sharing' the Digital Forensics function in a regional collaboration of Police forces – if this is the case, please can this request go to the host force Digital Forensic Unit/Cyber department?

Please could you answer the following questions – they are split in to two sections.

Basic Statistics and Training

1) In January 2022 how many Police Officers and Police Staff work in Digital Forensics/Cyber for you?

2) What are the job titles that exist in your Digital Forensic Uni/Cyber Unit? Can you please also tell me what the salary scales are for these roles? For example, one force might have Digital Forensic Technicians, Pay = Scale 5.

3) What is your annual budget allocation for Digital Forensics and Cyber Investigations?

Having considered questions 1 to 3, I can advise the information requested by you is held by Police Scotland, however it is considered to be exempt in terms of Section 16 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 following exemptions are applicable to the above requested information:

Section 35 (1) (a) – Law Enforcement

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.

Release of the information requested would adversely impact on the operational effectiveness of the Service. Being aware of the number officers and staff who work in digital forensics would allow persons or groups intent on committing offences or causing disorder with the means to make a reasonable assessment of the capabilities of Police Scotland. To disclose this information into the public domain would undermine the tactical options available and compromise the effective delivery of law enforcement.

This is a non-absolute exemption and the application of the public interest test applies.
It could be argued that the public are entitled to know how public funds are spent and resources distributed within an area of policing. However, security measures are put in place to protect the community we serve and disclosure of any information regarding to security would assist criminals and terrorists in carrying out their criminal and terrorist activities. This would ultimately increase the risk of harm to the general public and significantly undermine any ongoing or future operations to protect the security or infrastructure of the United Kingdom.

The public have an expectation that the police will make the 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. Disclosure of this information coupled with the disclosure of similar information from other forces and law enforcement agencies would give such criminals and terrorists a more detailed account of the tactical infrastructure of not only Police Scotland but also the country as a whole. Any incident that results from such a disclosure would by default affect National Security.

As much as there is public interest in knowing that policing activity is appropriate and balanced in matters of national security, this will only be overridden in exceptional circumstances.

In addition any disclosure by Police Scotland that places the security of the country at risk, no matter how generic, would undermine any trust or confidence individuals have in us.

4) Are you already ISO 17025 accredited with regards to Digital Forensics – Yes/No?

5) Are you working towards being ISO 17025 accredited – Yes/No?

In terms of the Freedom of Information (Scotland) Act 2002 a public authority is only obliged to provide recorded information.

Under Section 8 of the Act, information which requires opinion or a yes/no response is not in essence a valid request. However, in this insistence, we can advise question 4 is no and question 5 is yes.

6) Please can you confirm what mandatory courses new recruits are put on when they start work in Digital Forensics? For example, some forces insist on recruits going on the 'CoP Core Skills in data recovery and analysis' course. Just the names of the courses will be okay if possible.

Please see our response to questions 1 to 3.

7) Following on from the above Question 6 – if new recruits are put on specific courses, would them having a related degree in Digital Forensics negate the need for them to undertake a mandatory training course such as the 'CoP Core Skills in data recovery and analysis'?

Staff are placed on courses as part of our training pathway and previous learning/qualifications maybe taken into consideration when deciding on the courses shaped according to individual needs.

Staff Welfare

1) Are there any mandatory periodic psychological assessments or offers of counselling for Police Staff and Police Officers involved in Digital Forensics/Cyber? This relates to staff who have to view upsetting, graphic and illegal material such as child abuse images or terrorist material.

Yes, staff attend counselling sessions at set intervals, albeit individual needs are also considered.

2) Carrying on from the above Question 1 – if there are any psychological assessments or counselling, are they enforced and does this spend come out of a force wide budget or the Digital Forensics departmental budget?

The counselling sessions are carefully planned out, which staff willingly take part in thus negating the need for them to be enforced. The funding for this aspect is part of the wider Police Scotland commitment to Wellbeing and Welfare of staff.

3) On the subject of illegal images of children, when grading such content – are breaks away from the computer offered and enforced?

Staff are guided on the need to take regular breaks away from their screens regardless of their duties and whilst they have a personal responsibility to do this, they are managed carefully by line management to maximise the support to staff.

4) Do you have a limit on how many hours individual Police Staff and Police Officers spend grading illegal images at any one time?

No, there aren't any limits in place in terms of the number of hours individual Police Staff and Police Officers spend grading such images.

5) Does your Digital Forensic Unit routinely attend crime scenes?

Dedicated Digital Forensics staff attend crime scenes as part of operational duties, However, frequency of this cannot be predicted as it is dependent on a number of factors that are often unquantified.

6) If your Digital Forensic Unit Officers and Staff attend crime scenes – do they have access to body worn video equipment?

Digital Forensic Unit Officers and staff have access to Body Worn Video Equipment through divisionally trained staff should it be required and available.

7) If your Digital Forensic Unit Officers and Staff attend crime scenes – do they have access to PPE and body armour?

Police Officers all have access to PPE and body armour. Police staff have PPE, but no body armour, although it is important to note that they are not permitted access to a crime scene until the area has been secured and declared safe to do so by Police Officers in attendance.

Should you require any further assistance concerning this matter please contact Information Management – Glasgow at foiglasgow@scotland.police.uk quoting the reference number given.

If you are dissatisfied with the way in which Police Scotland has dealt with your request, you are entitled, in the first instance, to request a review of our actions and decisions.

Your request must specify the matter which gives rise to your dissatisfaction and it must be submitted within 40 working days of receiving this response - either by email to foi@scotland.police.uk or by post to Information Management (Disclosure), Police Scotland, Clyde Gateway, 2 French Street, Dalmarnock, G40 4EH.

If you remain dissatisfied following the outcome of that review, you are thereafter entitled to apply to the Office of the Scottish Information Commissioner within six months for a decision. You can apply online, by email to enquiries@itspublicknowledge.info or by post to Office of the Scottish Information Commissioner, Kinburn Castle, Doubledykes Road, St Andrews, Fife, KY16 9DS.

Should you wish to appeal against the Office of the Scottish Information Commissioner's decision, there is an appeal to the Court of Session on a point of law only.

As part of our commitment to demonstrate openness and transparency in respect of the information we hold, an anonymised version of this response will be posted to the Police Scotland Freedom of Information Disclosure Log in seven days' time.