Keeping People Safe

FREEDOM OF INFORMATION REQUEST

Request Number: F-2020-00824

Keyword: Organisational Information/Governance

Subject: Coronavirus (Covid 19) Remote Working Resources

Request and Answer:

Your request for information has now been considered. In respect of Section 1(1)(a) of the Act I can confirm that the Police Service of Northern Ireland does hold some information to which your request relates and this is being provided to you. We further consider the information you seek in request number 3 part b PSNI are providing a Neither Confirm nor Deny response and have detailed our rationale as to why this applies. We have also provided you with links to guidance issued by the Information Commissioner's Office which we have followed in responding to your request.

Request 1
I would like to know what policies are in place within your organisation to enable remote working during the Covid-19 lockdown since the start of the calendar year please.

Answer
PSNI have a 'Remote Working' Information Security Standard which details the procedures to be adhered to and the responsibilities of individuals who have a requirement to work outside of PSNI premises with information assets.

Request 2
Breakdown of the number of new devices purchased by your organisation:
a. Laptops
b. Tablet computers
c. Mobile Phones

Answer
a. Since the start of the calendar year PSNI have purchased 1,592 laptops.
b. 100 tablets.
c. Approximately 3,200 mobiles.

Request 3
Detail on remote working software/licences purchased
a. Number of Zoom accounts created
b. Number of new office 365 account purchased

Answer Part A
A total of 20 Zoom accounts were officially created.

In addition to the responses provided above and in accordance with the Act, the Police Service of Northern Ireland can neither confirm nor deny that it holds the information you have requested in request 3 part b.

Section 1 of the Freedom of Information Act 2000 (FOIA) places two duties on public authorities. Unless exemptions apply, the first duty at Section 1(1)(a) is to confirm or deny whether the information specified in the request is held. The second duty at Section 1(1)(b) is to disclose information that has been confirmed as being held.

Where exemptions are relied upon Section 17(1) of FOIA requires that we provide the applicant with a notice which

a) states that fact,
b) specifies the exemption(s) in question and
c) states (if that would not otherwise be apparent) why the exemption applies.

The Police Service of Northern Ireland (PSNI) can Neither Confirm Nor Deny that it holds the information relevant to your request as the duty in Section 1(1)(a) of the Freedom of Information Act 2000 does not apply by virtue of the following exemptions:

Section 24(2) – National Security – confirmation or denial would likely prejudice safeguarding national security.

Section 31(3) – Law Enforcement – confirmation or denial would likely prejudice the prevention or detection of crime and the apprehension or prosecution of offenders.

The full text of exemptions can be found at www.legislation.gov.uk and further guidance on how they operate can be located on the Information Commissioners Office website www.ico.org.uk.

Neither Confirm nor Deny' (NCND)
There may be occasions when complying with the duty to confirm or deny under section 1(1) (a) would in itself disclose sensitive or potentially damaging information that falls under an exemption. In these circumstances, the Act allows a public authority to respond by refusing to confirm or deny whether it holds the requested information.

The decision to issue a 'neither confirm nor deny' response is not affected by whether we do or do not hold the information but relates to the consequences of confirming or denying the information is held. The starting point and main focus in most cases will be theoretical considerations about the consequences of confirming or denying that a particular type of information is held. The decision to neither confirm nor deny is separate from a decision not to disclose information and needs to be taken entirely on its own merits.

PSNI follow the Information Commissioner's Guidance in relation to 'NCND' and you may find it helpful to refer to this at the following link:

https://ico.org.uk/media/for-organisations/documents/1166/when_to_refuse_to_confirm_or_deny_section_1_foia.pdf

Sections 31 and 24 are prejudice based qualified exemptions and there is a requirement to evidence the prejudice (harm) in disclosure and consider the public interest to ensure neither confirming or denying that information is held is appropriate.

Harm in Confirming or Denying that Information is held
Policing is an information-led activity, and information assurance (which includes information security) is fundamental to how the Police Service manages the challenges faced. In order to comply

with statutory requirements, the College of Policing Authorised Professional Practice for Information Assurance has been put in place to ensure the delivery of core operational policing by providing appropriate and consistent protection for the information assets of member organisations, see below link:

https://www.app.college.police.uk/app-content/information-management/

To confirm or deny whether PSNI use a certain operating system would identify vulnerable computer systems and provide actual knowledge, or not, that this software is used within individual force areas. In addition, this would have a huge impact on the effective delivery of operational law enforcement as it would leave forces open to cyberattack which could render computer devices obsolete.

This type of information would be extremely beneficial to offenders, including terrorists and terrorist organisations. It is vitally important that information sharing takes place with other police forces and security bodies within the UK to support counter-terrorism measures in the fight to deprive terrorist networks of their ability to commit crime.

To confirm or deny whether or not PSNI relies on a certain operating system would be extremely useful to those involved in terrorist activity as it would enable them to map vulnerable information security databases.

Public Interest Test

Section 24(2) National Security – Factors Favouring Confirmation or Denial
The public are entitled to know how public funds are spent and how resources are distributed within an area of policing. To confirm whether PSNI utilises Office 365 would enable the general public to hold PSNI to by highlighting forces that use out of date software. In the current financial climate of cuts and with the call for transparency of public spending this would enable improved public debate into this subject.

Section 24(2) National Security – Factors Against Confirmation or Denial
Security measures are put in place to protect the community we serve. As evidenced within the harm to confirm information is held would highlight to terrorists and individuals intent on carrying out criminal activity vulnerabilities within PSNI.

Taking into account the current security climate within Northern Ireland, no information (such as the citing of an exemption which confirms information pertinent to this request is held, or conversely, stating 'no information is held') which may aid a terrorist should be disclosed. To what extent this information may aid a terrorist is unknown, but it is clear that it will have an impact on a force's ability to monitor terrorist activity.

Irrespective of what information is or isn't held, 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.

The cumulative effect of terrorists gathering information from various sources would be even more impactive when linked to other information gathered from various sources about terrorism. The more information disclosed over time will give a more detailed account of the tactical infrastructure of not only a force area, but also the country as a whole.

Any incident that results from such a disclosure would, by default, affect National Security.

Section 31(3) Law Enforcement – Factors Favouring Confirmation or Denial
Confirming that information exists relevant to request 3 part b would lead to a better informed public which may encourage individuals to provide intelligence in order to reduce the risk of police networks being hacked.

Section 31(3) Law Enforcement – Factors Against Confirmation or Denial
Confirmation or denial that information is held in this case would suggest PSNI take their responsibility to protect information and information systems from unauthorised access, destruction, etc, dismissively and inappropriately.

Decision
The points above highlight the merits of confirming or denying the requested information exists. The Police Service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. As part of that policing purpose, information is gathered which can be highly sensitive relating to high profile investigative activity.

Weakening the mechanisms used to monitor any type of criminal activity, and specifically terrorist activity would place the security of the country at an increased level of danger.

In order to comply with statutory requirements and to meet NPCC expectation of the Police Service with regard to the management of information security a national policy approved by the College of Policing titled National Policing Community Security Policy has been put in place. This policy has been constructed to ensure the delivery of core operational policing by providing appropriate and consistent protection for the information assets of member organisations. A copy of this can be found at the below link:

http://library.college.police.uk/docs/APP-Community-Security-Policy-2014.pdf

In addition, anything that places that confidence at risk, no matter how generic, would undermine any trust or confidence individuals have in the Police Service. Therefore, at this moment in time, it is our opinion that for these issues the balance test favours neither confirming nor denying that information is held.

If you have any queries regarding your request or the decision please do not hesitate to contact me on 028 9070 0164. When contacting the Corporate Information Branch, please quote the reference number listed at the beginning of this letter.

If you are dissatisfied in any way with the handling of your request, you have the right to request a review. You should do this as soon as possible or in any case within two months of the date of issue of this letter. In the event that you require a review to be undertaken, you can do so by writing to the Head of Corporate Information Branch, PSNI Headquarters, 65 Knock Road, Belfast, BT5 6LE or by emailing foi@psni.pnn.police.uk.

If following an internal review, carried out by an independent decision maker, you were to remain dissatisfied in any way with the handling of the request you may make a complaint, under Section 50 of the Freedom of Information Act, to the Information Commissioner's Office and ask that they investigate whether the PSNI has complied with the terms of the Freedom of Information Act. You can write to the Information Commissioner at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. In most circumstances the Information Commissioner will not investigate a complaint unless an internal review procedure has been carried out, however the Commissioner has the option to investigate the matter at his discretion.

Please be advised that PSNI replies under Freedom of Information may be released into the public domain via our website @ www.psni.police.uk

Personal details in respect of your request have, where applicable, been removed to protect confidentiality.