



**HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE**

Response Date: 15/05/2020

2020/302 - Number of Laptops, PC's or Virtual Machines Using Microsoft Windows Versions Prior to Windows 10

In response to your recent request for information regarding;

Please advise the number of laptops, PC's or Virtual Machines running Versions of Microsoft Windows prior to Windows 10, also what release of Windows 10 are you currently using.

Concerns have been raised in relation to disclosing the information requested. Therefore, a Public Interest Test has been carried out to weigh up the reasons for and against disclosure; to ensure the release is in the interest of the public as a whole and not just the applicant.

The Public Interest Test has considered the following exemptions;

Section 24(1) National Security

Section 31(1)(a) Law Enforcement

Sections 24 and 31 being prejudice based qualified exemptions, both evidence of harm and public interest considerations need to be articulated to the applicant.

To provide information regarding North Wales Police's use of certain operating systems 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 provide information regarding North Wales Police's reliance 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 Considerations

Section 24(1) National Security

Factors favouring disclosure

The public are entitled to know how public funds are spent and how resources are distributed within an area of policing. To disclose information regarding the number of laptops, PC's or Virtual Machines running Versions of Microsoft Windows prior to Windows 10 used by North Wales Police, and what release of Windows 10 North Wales Police are currently using would enable the general public to hold North Wales Police to account by highlighting forces who 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.

Factors against disclosure

Security measures are put in place to protect the community we serve. As evidenced within the harm to disclose information held would highlight to terrorists and individuals intent on carrying out criminal activity vulnerabilities within North Wales Police.

Taking into account the current security climate within the United Kingdom, disclosure of such information may aid terrorist activity. 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 impactful 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(1) Law Enforcement

Factors favouring disclosure:

Disclosing information relevant to this request 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.

Factors against disclosure:

Disclosing information in this case would suggest North Wales Police take their responsibility to protect information and information systems from unauthorised access, destruction, etc., dismissively and inappropriately.

Balancing Test

The points above highlight the merits of non-disclosure regarding requested information. 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 non disclosure.

Therefore, in accordance with the Freedom of Information Act 2000, this letter acts as a Refusal Notice under section 17 (1) of the legislation.

THIS INFORMATION HAS BEEN PROVIDED IN RESPONSE TO A REQUEST
UNDER THE FREEDOM OF INFORMATION ACT 2000, AND IS CORRECT AS AT 12/05/2020