



Response Date:20/01/2024

2024/1095 - Systems

In response to your recent request for information regarding;

Please advise the products that your forces uses for;

**Command & Control Application
ICCS Application
Mobile Working Application(s)
Mobile Working Hardware
Airwave Handsets
Airwave Mobile Sets
ICCS Desktop Sets |
ICCS Portable Sets
ICCS Infrastructure**

**Detail if these products are owned outright, leased or part of a managed service. Where products are owned outright, list any support contracts for these.
Detail any managed service contracts, start dates & renewal dates.**

If any of the above products & technologies are due to be replaced and their replacement has been chosen, also detail the requested information for these.

Where products are shared with another service/force/agency, please detail this and who the lead service/force/agency is.

Where there is more the one instance of an application in your organisation, please also detail that.

Concerns have been raised in relation to disclosing the requested information.

Therefore, Section 31 Law Enforcement and Section 24 National Security is to be considered as part of the Public Interest Test. A Public Interest Test has been carried out to weigh up the reasons for and against disclosure of the information requested, to ensure the release is in the interest of the public as a whole and not just the applicant.

s24(1) National Security
s31(1) Law Enforcement)

Overall Harm for Sections and 24 and 31

Every effort should be made to release information under Freedom of Information. However a FOIA response is considered to be a release to the world as once the information is published the public authority have no control over what use is made of that information.

The Police Service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. In order to achieve these objectives all forces have a telephony and

communications network infrastructure to support the vital information technology essential to front line services. Disclosure of specific IT services, capabilities, or the lack thereof, in concert with any formal acknowledgement of strategic deficiency would reveal intricacies of those systems thereby highlighting vulnerabilities and compromising individual force information assurance.

As this request has been received nationally, disclosure would enable a geographical picture to be drawn up by those individuals who are intent on 'hacking' or defeating police systems; some of these individuals may include terrorists or terrorist organisations. In terms of duty of care, this would be detrimental to the public at large as disclosure could assist a malicious actor by highlighting vulnerable forces and leaving those forces open to disruption of Information Technology systems; thus compromising the effective delivery of operational law enforcement which in turn, is met by an increase of criminal offending.

Public Interest Test

Factors favouring disclosure - Providing information in respect of North Wales Police network infrastructure would allow the public to be better informed on the health state and performance of said Information Technology platform. In addition, forces are required to demonstrate efficient services to local taxpayers and satisfy audit requirements. This would provide transparency with regard to the use of public funds in so much as highlighting that funds are being used to correctly and appropriately ensure all forces have adequate infrastructure, which results in the smooth running of force Technology systems.

Factors favouring non-disclosure - Whilst there is public interest in providing reassurance that police forces are appropriately and effectively dealing with any threats posed by terrorist organisations against police force Technology capabilities, there is a strong public interest in safeguarding National Security and the welfare and safety of the general public at large. Any disclosure has the potential to undermine current and future data integrity, which in turn compromises the force's mandate to protect the security of the United Kingdom, e.g. counter-terrorism activity. The risk of significant harm or even death to the community at large would be increased. Any disclosure of information that may lead to compromise of force IT systems which ultimately affects law enforcement capabilities and hinders the prevention and detection of crime or terrorism, is not in the interest of the public.

Balance Test

The security of the country is of paramount importance and the Police service will not divulge any information if to do so would undermine law enforcement and therefore compromise the work of the police service. Whilst there is a public interest in the transparency of policing and force infrastructure, including any initiatives conducted with the private sector in relation to impacting on the crime or terrorist threat, there is a very strong public interest in safeguarding the integrity of these arrangements in this very sensitive area.

The points above highlight the merits for and against disclosure of the requested information. Disclosure would undoubtedly provide a greater openness and transparency to the community at large with regard to the Information Technology resources available to the police, and whilst there is always a public interest in the transparency of how a police force delivers effective law enforcement and ensures the National Security of the United Kingdom is robust, there is a very strong public interest in safeguarding the intricacies and tactical capabilities of the systems used when dealing with information.

In every case, public safety is the paramount focus and any information which would place individuals at risk and compromise the National Security of the United Kingdom, no matter how generic, is not in the public interest. The effective delivery of operational law enforcement and the National Security of the United Kingdom is crucial and of paramount importance to every force. This would have a negative impact on law enforcement and national security.

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 20/01/2025