Public Interest Test – 3299/20

Applicable exemptions:

Section 24(2) – National security
Section 31(3) - Law enforcement

Evidence of Harm

Every effort should be made to release information under Freedom of Information. However, any release under FOI is a disclosure to the world, not just to the individual making the request and therefore has an impact on all areas of the country.

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 Data Centres to house and support the 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 (such as a lack of Data Recovery plans) 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 created by those individuals who are intent on 'hacking' 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 those with malicious intent by highlighting vulnerable forces and leaving them open to disruption of Information Technology systems. Consequently, this would compromise the effective delivery of operational law enforcement which in turn, is met by an increase of criminal offending.

Public Interest Test

Factors favouring disclosure

Confirming or denying any information is held that confirms whether West Midlands Police, (A), has contingency planning in place in respect of a Data Centre, and (B), details of any on-site or Cloud based capabilities would allow the public to be better informed on the health state and performance of the our 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 Data Centres have adequate hardware and software, 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 Centre 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. In addition, by confirming or denying whether the force has partnered with third party companies by revealing budget information, is intelligence to those who would wish to exploit vulnerabilities in the service. This may result in compromised force IT systems which ultimately affects law enforcement capabilities and hinders the prevention and detection of crime or terrorism.

Balance Test

The security of the country is of paramount importance and the Police service will not divulge whether any information is or is not held 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 confirming whether any of the requested information is held. Confirmation of this would undoubtedly provide a greater openness and transparency to the community at large with regard to the Information Technology resources available to the police. 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 Data systems used when dealing with information.

In every case, public safety is of 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, for these issues the balancing test for confirming or denying whether any further information is held, is not made out.