Overall harm for Section 31

ICT is fundamental to how the Police Service manages the technological challenges faced in modern policing. Information that exposes details of the ICT organisation could be used to the advantage of terrorist's criminal organisations and individuals. To plan and execute an attack on force systems or the service provider. Such attacks could take the form of data theft, denial of service or other deliberate disruptions. This could not help but have the effect of reducing the ability of the police to undertake relevant activities.

Factors favouring disclosure of information for Section 31

The public are entitled to know how public funds are spent and by disclosing this information the public would be able to see where public money is being spent and know that the Police are doing as much as they can to investigate and combat crime/terrorism.

The disclosure of the requested information would show which software/hardware/ systems is used by the police service and reassure the public that these systems are up to date and secure. This would also provide reassurance to what products we use and the way in which we use them.
Revealing this information would enable the public to have some reassurance that the force's ICT programme and systems are robust.

Factors against disclosure of information for Section 31

Disclosure of ICT strategy and plans along with current and future objectives would mean that law enforcement tactics would be compromised, which would hinder the prevention and detection of crime. It would expose police resources and create a mosaic effect highlighting 'soft' areas of the country that could be exploited. This would adversely affect public safety and have a negative impact on law enforcement.

Disclosure would provide those intent on disrupting police activities with enough information about the products we use to disrupt our systems or even to plan and execute a targeted attack. Within this plan the force are aware of the areas that need improvement and to disclose information as to our future plans to address these would mean the force is left in a vulnerable position and would be detrimental to the effective operation of police activities. Additional resources would be required to counter an attack if there was one and this would also have financial implications. Where systems were compromised, there is also the potential for sensitive information such as personal data, security information and other data to be made public.

Where current or future law enforcement role of the force may be compromised by the release of information, then this is unlikely to be in the interest of the public. In this case to provide details of the capabilities of West Midlands Police. This would allow criminals to judge the specific ability of the force and thereby change their tactics to avoid detection. This would compromise the future prevention and detection of crime.

In addition, the public has a reasonable expectation that the police service will protect their data, and any weakening of the security in place to protect this information could undermine the public's confidence in the police service. This could, in turn, reduce the public's willingness to engage with police agencies.

Ultimately any disclosure that would have a negative effect on our core functions of law enforcement would not be in the best interests of the public.

Balance test

Whilst there is a strong public interest in the transparency of policing technology however for a public interest test, issues that favour release need to be measured against issues that favour non-disclosure. The public interest is not what interests the public, or a particular individual, but what will be the greater good, if released, to the community as a whole.

On balance it is considered that the public interest in providing the information is outweighed by the potential impact release would have on future law enforcement activities.

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 protect this data, or providing information that would allow criminals to disrupt the service's use of this information, would not be in the public interest.

West Midlands police will not divulge information if it is likely that it will compromise the work of the Police Service or place members of the public at risk. Disclosure of the requested information would highlight areas that could be exploited by criminals.

This will adversely affect West Midlands police ability to detect and prevent crime, as it may alter the behaviours of those intent on criminal activity. This in itself could put members of the public at risk and hinder Law Enforcement. It is therefore our belief that the balance test lies in favour of not disclosing the information.