REQUEST

Dear Mayor's Office for Policing and Crime,

Please can you provide me with a comprehensive list of all IT systems used across the organisation, including all business applications such as the GIS software or the content management system used.

I appreciate your assistance with this request.

RESPONSE

Thank you for your Freedom of Information request of 22 March to the Mayor's Office for Policing And Crime (MOPAC) and I apologise for the delay in replying to you.

I confirm that your request has been handled under the Freedom of Information Act 2000 and that MOPAC does hold some information relating to your request. This is attached as a spreadsheet.

We have withheld the details of our security related systems: intruder detection; firewall protection; anti-virus / malware detection. This information is exempt under Section 31(1)(a) of the Act. Please see below for more information about how this exemption was engaged.

Exemption: Section 31(1)(a) - the prevention or detection of crime
Section 31(1)(a) of the Act provides:
(1) Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice—
(a) the prevention or detection of crime

How the exemption applies to the information
Section 31(1)(a) covers all aspects of the prevention and detection of crime and can apply to information on general policies and methods adopted by law enforcement agencies. Section 31(1)(a) of the Act is engaged because the release of this information would, or would be likely to, prejudice the prevention or detection of crime.

The information we have withheld is the names of the security systems that MOPAC uses for intruder detection, firewall protection and anti-virus / malware detection.

The provisions of section 31(1(a) of the Act are engaged by information which could be used to commit crime. The release of this information would leave us more open to the risk of a cyber-attack. Individuals who know what systems we use can look at exploiting potential weaknesses that may have been reported with these products to assist getting access to our network and risk of crimes such as cyber attack; theft of data (and potentially blackmail or extortion attempts if followed up by demands for money, as in the 'WannaCry' ransomeware attack in 2017 that affected the NHS and other public authorities throughout the UK). The National Cyber Security Centre recently reported that there has been an increase in such attacks.

Public interest test
Considerations favouring disclosure – MOPAC acknowledges there is a legitimate interest in MOPAC being transparent and sharing information about the systems it uses - being accountable to the public about by demonstrating appropriate steps have been taken to protect

itself from cyber crime – MOPAC is also mindful of the assumption in favour of disclosure in 2(2)(b) of the FOIA.

Considerations favouring non-disclosure - There is a strong public interest in preventing crime - There is a substantial public interest in not jeopardising MOPAC's resilience to cyber threats, particularly given the likelihood of an attempt - Related to this, there is a strong public interest in protecting sensitive data and personal data held on our systems.

In this case, the public interest favours maintaining the exemption provisions s.31(1)(a) in relation to the withheld information.

If you are unhappy with the response to your Freedom of Information request, please see the MOPAC website on what the next steps are at:
https://www.london.gov.uk/what-we-do/mayors-office-policing-and-crime-mopac/governance-and-decision-making/freedom-information