

**Request:**

As part of a research project into Cyber Security resilience within Local Government in the UK. I would like to understand if the council currently have the below cyber security tools in place. It would also be useful to understand what providers if any currently provide these tools and when any existing contracts are due to expire or to be reviewed.

Web Security/Filtering Cloud Application Security (CASB) Email Security MFA Security Awareness Training Any additional information you may be able to provide will be greatly appreciated.

**Response:**

Section 31(1)(a) of the Freedom of Information Act 2000 (FoIA) states that information is exempt information if its disclosure under this Act would, or would be likely to, prejudice the prevention or detection of crime.

"Disclosure under the FoIA is deemed to be disclosure to the world at large, i.e. placing it in the public domain. Disclosure of the requested information would be valuable information to potential cyber criminals allowing them to identify patterns of previous attacks and possible weaknesses in cyber security systems.

We therefore believe that the exemption at section 31(1)(a) of the FoIA is engaged.

This exemption is subject to a Public Interest Test. Whilst the Council acknowledges the inherent public interest in transparency in its activities, it believes in this case the public interest in protecting the personal and sensitive data held on its systems is of more significance. Furthermore, the cost to the public purse of responding to cyber-attacks adds to the balance of arguments against disclosure. Taking these factors into consideration, the Council assesses the public interest is not in favour of disclosure".