FREEDOM OF INFORMATION REQUESTS RELATING TO ICT, CYBER/ICT SECURITY, CYBER ATTACKS, RANSOMWARE, MALWARE AND RELATED TOPICS

APPLICATION OF FOIA SECTION 31 – LAW ENFORCEMENT

This information is exempt from disclosure under Section 31(1)(a) and Section 31(3) of the Freedom of Information Act - Law enforcement. Disclosure of this information would be likely to prejudice the prevention or detection of crime.

Section 31(1)(a) provides an exemption where prejudice could be caused to allow criminals to use the information to gain unlawful access to Council systems and infrastructure.

A disclosure made under the Freedom of Information Act, is a disclosure to the world at large. Coventry City Council takes its Data Protection responsibilities very seriously and has robust arrangements in place to protect IT systems and infrastructure. Despite genuine requests for information, some individuals may intend to misuse information to cause damage. Disclosure of the information may lead to a number of avenues open to the criminals to exploit potential weaknesses to cause damage, disruption or profit using criminal means.

Disclosure of this information would result in the need to implement disproportionate steps and additional expense to the public purse to counter an increased risk that does not exist at present and this information will therefore not be released.

The Council have also taken into account the Information Commissioner's Office (ICO) Decision Notices IC-106031-D4Y0 FS50662638, FS50600199, FS50665770, FS50662675. not to release information in the Table 1 categories as outlined under Section 31(3) of the Freedom of Information Act.

Please note that the Council publishes its Contracts Register which shows details of current contracts every quarter. This includes a description of the contract, value, start and end dates and the supplier and can be accessed via the Council's website at: https://www.coventry.gov.uk/contractsregister

Table 1:

IT Infrastructure – Hardware • servers • end user devices • storage • data centres • switches • other networking devices • all other related aspects such as CCTV, power, air conditioning, cabling and dedicated comms rooms.	Information about: • Description/Type • Manufacturer • Model • Operating Systems • Version • Install Dates • Project documentation related to installations, upgrades and developments • Number of devices
Infrastructure – Software & Licensing *i.e. software, licensing and applications used by the Council both for internal purposes and to provide its services to customers.* • Web services • Enterprise Resource Planning (ERP) • Customer Relationship Management (CRM) • Corporate Applications • Commercial Off the Shelf Software (COTS) • Line of Business Applications (LOB) • Operating Systems (OS)	Information about: • Description/Type • Manufacturer • Version • Operating Systems • Number of Users • Number and Type of Licences • Install Dates • Project documentation related to installations, upgrades and developments

Cyber Security *Protecting the Council infrastructure, systems and devices* • core infrastructure • physical security • security functions • systems and developments	Information about: • Description/Type • Manufacturer • Model • Version • Operating Systems • Network Diagrams • Installation Dates • Project documentation related to installations, upgrades and developments • Number of cyber incidents/breaches • Type of cyber breaches • Action plans / improvements / guidance put in place to combat cyber breaches and protect the Council • Staff responsible for Cyber Security • Information that may influence the timing of a cyber attack (such as busy / quiet periods for a particular service or system; activity or processing timetables). • Cyber security policies and plans

Refusal Notice Section 31– Law Enforcement

The Council under Section 31(3) neither confirms nor denies whether requested information about specific systems, software, hardware, exists or is held by us.

The information is exempt from disclosure under Section 31(1)(a) and Section 31 (3) of the FOIA Act 2000. Section 31 of the FOIA relates to Law Enforcement and Section 31(3) removes the public authority's duty to confirm or deny whether information is held if to do so would, or would be likely to prejudice law enforcement. When the Council uses a neither confirm, nor deny response, you should not assume that the information is either held or not.

This is because it is the Council's view that the confirmation or denial of the possession of information relating to the Council's ICT assets, policies and cyber resilience, would be likely to compromise the Council's information security strategies by giving cyber criminals insight into vulnerabilities which may, or may not, exist.

Section 31(3) is a qualified exemption, as such we have gone on to perform a public interest test in order to assess the public interest arguments for and against declaring whether or not the requested information is held.

Factors for confirming or denying:

- Confirmation of possession would demonstrate a commitment to transparency with regard to the Council's undertaking and could provide assurance that the council have robust IT infrastructure in place.

Factors against confirming or denying:

- Maintaining the integrity and security of the Council's systems.

- Preventing cyber-attacks and similar against the Council systems. There is public interest in avoiding disruption to public services and functions of the Council.

- There is public interest in complying with the Council's legal obligations to keep personal information secure and to take appropriate measures which includes keeping areas confidential where necessary.

- The costs to the Council related to a recovery from an attack (modifying systems, new software, regulatory fines).

- The public interest in crime prevention.

Revealing the information may assist criminals/cyber criminal's insight into not only the strengths of the Council's cyber security, but also any potential weaknesses that may exist. This could ultimately result in a future cyber-attack. Cyber security measures are in place to protect the integrity of personal and sensitive personal information.

The occurrence of a future cyber-attack would prejudice the Council's legal duty to safeguard personal information from loss, theft, inappropriate access or destruction, which is why Section 31 has been employed in this case.

On balance the public interest in maintaining the exemption outweighs that in confirming or denying whether information is held and therefore the Council neither confirms nor denies, whether this information (detailed in the Table 1) is held.

Last updated: 2024