Information Governance Team

Postal Address:
Coventry City Council
PO Box 15
Council House
Coventry
CV1 5RR

www.coventry.gov.uk
E-mail: infogov@coventry.gov.uk
Phone: 024 7697 5408

18 February 2022

Dear Sir/Madam

Freedom of Information Act 2000 (FOIA)
Request ID: FOI396657181

Thank you for your request for information relating to IT policies.

You have requested the following information:

1. Can you also supply me a copy of the following policies :

a. IT Disaster Recovery Plan (e.g. DR plan, backup)
b. IT Incident Response Plan (e.g. Cyber Attack, DDOS, Ransomeware)

With regards to the Questions 1a and 1b, the Council under Section 31(3) neither confirms nor denies whether the information you have requested exists or is held by us.

The information you have requested 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.

It is the Council's view that the confirmation or denial of the possession of information relating to the Council's 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.

For Disclosure:

• 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.

Against Disclosure:

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

• Preventing cyber-attacks and similar against the Council systems.

Revealing the information may assist 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 is held.

c. Clean desk policy

There is no specific Council policy, however the importance of keeping a clear desk, is covered in the Council's Data Protection and Information Security training which staff must complete every year.

In all open plan offices, it is the normal day to day business way of working to have clean desks as employees do not have allocated desks. These include ensuring all workstations are kept clear of clutter and personal items so staff can work flexibly and feel comfortable wherever they are in the building.

Employees working in open plan offices also have access to locker facilities and lockable drawer spaces.

d. Access control policy (Access to business applications or network resources)

We do not have a dedicated Access Control Policy.

2. Please detail:

a. Current measures in place to protect confidential information

Please refer to Question 1a.

b. How you monitor staff access to business applications in your Council and ensure staff have a right of access

Most access to applications is controlled by Active Directory (AD) group membership which can be reviewed if necessary. Some applications don't use AD groups and have access managed by the application. This is normally managed by individual business units responsible for the application.

c. How you implement and carry out checks to ensure staff are adhering to your clean desk policy

d. Please forward any communications to staff regarding your Clean Desk policy

For Questions 2c and 2d, please refer to Question 1c.

The supply of information in response to a FOI/EIR request does not confer an automatic right to re-use the information. You can use any information supplied for the purposes of private study and non-commercial research without requiring further permission. Similarly, information supplied can also be re-used for the purposes of news reporting. An exception to this is photographs. Please contact us if you wish to use the information for any other purpose.

For information, we publish a variety of information such as: FOI/EIR Disclosure Log, Publication Scheme, Facts about Coventry and Open Data that you may find of useful if you are looking for information in the future.

If you are unhappy with the handling of your request, you can ask us to review our response. Requests for reviews should be submitted within 40 days of the date of receipt of our response to your original request – email: infogov@coventry.gov.uk

If you are unhappy with the outcome of our review, you can write to the Information Commissioner, who can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF or email icocasework@ico.org.uk.

Please remember to quote the reference number above in your response.

Yours faithfully

Information Governance