FREEDOM OF INFORMATION REQUESTS CONCERNING IT SECURITY INFORMATION, ATTACKS, RANSOM AND MALWARE AND RELATED TOPICS

Introduction

Derby City Council has very robust IT security in place. The Council use the necessary products and tools to keep their systems and infrastructure safe and secure. The Council updates them regularly and complies with the relevant guidance and codes of practice. The Council has a duty under the Data Protection Act 2018 to keep people's personal data safe and secure and we comply with that duty.

Under the UK General Data Protection Regulation, the Council has a similar duty to keep personal data securely and safe from attack. Although the Council needs to show that it can do this and will comply with its obligations, at the same time the Council must be careful that too much transparency does not cause damage.

The Council recognises that most people are honest and law abiding and don't intend to misuse information to cause damage. However, there are criminals who try and exploit system weaknesses to cause damage or make money.

Under Freedom of Information, giving information to one honest requester is the same as publishing it to everyone in the world. If the Council provides information that tells criminals when security software was last updated, for example, they could use that to exploit any known weaknesses and try to hack Council systems.

The Council has a large amount of personal data because of its many public functions, spanning lots of different areas and departments. Naturally, this data includes a lot of very sensitive data – for example, about care that the local authority provides to vulnerable adults, or casework for childcare Social Workers. The Council must take all necessary steps to make sure such data is kept safe. This means not telling people information that would allow criminals to gain unlawful access to Council systems and infrastructure.

The Council have also taken into account the Information Commissioner's Office (ICO) decision notices FS50662638, FS50600199, FS50665770, FS50662675 to not disclose the following information.

Freedom of Information Act Requests

The Council is frequently asked for information about the categories shown in Table 1:

Table 1: Information Request Categories

Category	Description	Information
IT Infrastructure - Hardware	This relates to: • servers, • end user devices • storage • data centres • switches • other networking devices • all other related aspects such as power, air conditioning, cabling and dedicated comms rooms.	• Description/Type • Manufacturer • Model • Operating Systems • Version • Install Dates • Project documentation related to installations, upgrades and developments • Number of devices.
IT Infrastructure – Software & Licensing	This relates to all software, licensing and applications used by the Council both for internal purposes and to provide its services to customers. Software includes: • 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).	• 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	Cyber Security covers the following areas used to protect the Council infrastructure, systems and devices: • core infrastructure • physical security • security functions • systems and developments	• Description/Type • Manufacturer • Model • Version • Operating Systems • Network Diagrams • Install Dates • Project documentation related to installations, upgrades and developments • Number of cyber 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).

The Council has considered the Table 1 categories carefully and has decided not release this information under Section 31(3) of the Freedom of Information Act 2000.

Refusal Notice Section 31– Law Enforcement

The Council considers that telling requesters whether such information referenced in Table 1 is held, would or would likely cause damage and prejudice law enforcement. Therefore, the information requested is exempt pursuant to s31(1) and (3) Freedom of Information Act 2000

Section 31(1)(a) says that a public authority does not have to disclose information under section 1 Freedom of Information Act 2000 where doing so would or would likely prejudice the functions of law enforcement, in this case, the prevention or detection of crime.

Turning to information requests in respect of specific systems, software, hardware, exemption in section 31(3) is engaged. This allows an organisation to refuse to confirm or deny if the information is held. In other words, the Council can refuse to say if it holds information about this or not. When the Council uses a neither confirm or deny response you should not assume that the information requested is either held or not.

This is because disclosing whether the Council does or does not hold specific information would or would likely give cyber criminals insight into the infrastructure, hardware, software systems, and, as a result, any potential vulnerabilities which may, or may not, exist. This would or would likely result in damage to the Council's IT infrastructure and systems.

Prejudice Test

In engaging this exemption, it is necessary to consider the prejudice test as followed by the Information Commissioner's Office and adopted by the Information Tribunal in the leading case of *Christopher Martin Hogan and Oxford City Council v the Information Commissioner (EA/2005/0026 and 0030, 17 October 2006.* The following three stage test has been considered and applied as follows:

Applicable interest within the exemption

In this case the request relates to the details about the specific IT systems/software used by the Council.

The Council considers that the release of this information would or would likely put the Council at risk of being targeted by cyber criminals as it would reveal the specific IT systems/software used and would or would likely allow cyber criminals to target the specific system vulnerabilities to gain unlawful access to information. This could compromise millions of items of sensitive information held by the local authority and make it more vulnerable to crime.

Any disclosure made under the Freedom of Information Act, is deemed to be made to the public at large. There is a real risk that this information could be used for criminal activity either on its own or together with other information in a mosaic effect which increases the risk of prejudice to the prevention of crime.

The nature of the prejudice

It must be shown; that the prejudice that may result is “real, actual or of substance” and that there is a causal link between the disclosure and the potential prejudice. The prejudice in this case is the Council’s ability to prevent unlawful access, theft, vandalism to its systems and safeguard the data held in those systems.

As a government organisation the Council is a potential target for cyber criminals across the world. Disclosing information about the specific systems, software or hardware used would or would likely provide cyber criminals with the valuable information they need to target known vulnerabilities to gain unlawful access to information held by the Council, such as personal data held about residents, citizens, children and vulnerable adults as well as employees. Furthermore, the Council also holds commercially and politically sensitive information that, on balance, would or would likely cause prejudice to the Council both financially, contractually and reputationally if unlawfully accessed.

The real and actual prejudice described above would or would likely cause a detrimental effect on its citizens as well as to the business interests and reputation of the Council. The consequences of disclosing such information would or would likely be significant in its impact if Council IT systems were made vulnerable with millions of items of sensitive information of children and vulnerable adults as well as commercially sensitive information at risk of unlawful use.

The causal link between the disclosure under the FOI request to the prejudice that would or would likely be caused has been clearly demonstrated above. To be clear, placing such information into the public domain immediately weakens the security of the Council’s systems and, therefore, its ability to sufficiently protect the data it holds.

Providing information about the specific systems, software or hardware used into the public domain, given that disclosure under FOI is to the world at large would prejudice the Council's ability to prevent unlawful access to the information and would be a breach of its obligations under the Data Protection Act 2018 and UK GDPR to ensure personal data it processes is kept 'safe and secure' with appropriate technical and organisational measures. Divulging the details of such measures would or would likely prejudice the statutory duty to protect the same under the Data Protection Act 2018 as well as Articles 5 and 32 UK GDPR

The likelihood of prejudice

The Council has demonstrated that there is a real and significant risk that the prejudice in relation to the unlawful access to systems would or would likely occur.

The Information Commissioners Office – ICO ransomware and data protection compliance guidance highlights that:

"The exploitation of known vulnerabilities where patches were available to fix the issue is a common method used by attackers. This was much more common than zero-day attacks where the vulnerability exploited is not yet publicly known and is typically crafted by advanced levels of attackers".

This is also the view of the National Cyber Security Centre who advise that *"Exploitation of known vulnerabilities in software remains the greatest cause of security incidents".*

The Council increasingly provides its functions and services online to meet local people's needs - for example, revenues and benefits.

Disclosing information about the specific systems, software or hardware used into the public domain would provide cyber criminals with the valuable information they need to target known vulnerabilities in the systems to gain unlawful access to information held.

In undertaking this prejudice test, the Council considers that the above prejudice and subsequent harm/damage would or would likely occur if the information were

disclosed. “Would” means that, on balance, the disclosure would be more probable than not to lead to the prejudice. “Would likely” means that, on balance, there is a real and significant risk of prejudice occurring even though probability may be less than 50%.

In taking all of the above into account as well as the law, subsequent case law and ICO guidance, the Council concludes that the likelihood of prejudice would or would likely cause harm if the information were disclosed.

Public Interest Test

Section 31(3) is a qualified exemption which means the Council must undertake a public interest test where we compare the public interest for and against disclosing. The public interest test is not about whether we should disclose any information that we might hold. It is a test of whether we should say if we hold the information or not.

Factors in favour of confirming or denying

- It would help transparency and accountability of the Council.
- It would reassure people about whether the Council IT infrastructure and systems are secure
- It would provide information about how effective the Council IT infrastructure and systems are.

Factors against confirming or denying

Saying whether the Council holds information would provide information about how effective Council IT infrastructure and systems are. This would likely give cyber criminals insight into the strengths of the Council’s IT infrastructure and systems and any potential weaknesses that may exist. This would increase the chances of cyber-attacks. One of the reasons that cyber security measures are in place is to protect the integrity of personal and sensitive personal information, so increasing the chances of an attack would have potentially serious repercussions.

- If the Council confirms that it holds the information requested, then this could show criminals its infrastructure and systems are particularly vulnerable, encouraging attacks.
- If the Council confirms that it does not hold the information requested, this could either show it has poor reporting and recording procedures which will encourage an attack, or it could show it has robust procedures which could encourage an attack to try out criminals' new techniques or could encourage criminals to target other Councils' which would increase crime elsewhere.
- There is public interest in complying with the Council's legal obligations to keep personal data secure and to take appropriate measures which includes keeping areas confidential where necessary.
- The costs to the Council associated with recovery from an attack including updating/changing systems, new software, revenue and regulatory fines.
- Public interest in crime prevention.
- Public interest in protecting their personal data and preventing any threat to the integrity of council data.
- Public interest in avoiding disruption to public services and functions of the Council

On balance, the Council concludes that the balance of public interest lies in upholding the exemption and not confirming or denying if hold specific IT information that fall into the categories shown in Table 1 is held.

Last updated 4 August 2023