## Freedom of information requests concerning information technology security information, attacks, ransom, malware and related topics

Introduction

South Derbyshire District Council has very robust IT security in place. We use the necessary products and tools to keep our 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 we 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 we provide information that tells criminals when we last updated our security software for example, they could use that to exploit any known weaknesses and try to hack our systems. The Council has a large amount of personal data because we carry out so many functions, spreading lots of different areas and departments. We hold a lot of very sensitive data – for example, about care we provide to vulnerable adults, or casework for childcare Social Workers. The Council must take all necessary steps to make sure we keep it safe. This means not telling people information that would allow criminals to gain unlawful access to our systems and infrastructure.

We have also taken into account the Information Commissioner’s Office (ICO) decision notices [FS50662638](https://ico.org.uk/media/action-weve-taken/decision-notices/2018/2258588/fs50662638.pdf), [FS50600199](https://ico.org.uk/media/action-weve-taken/decision-notices/2016/1623677/fs_50600199.pdf), [FS50665770](https://ico.org.uk/media/action-weve-taken/decision-notices/2018/2258599/fs50665770.pdf), [FS50662675](https://ico.org.uk/media/action-weve-taken/decision-notices/2018/2258593/fs50662675.pdf) 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, and other networking devices, as well as all other related aspects such as the power, air | Description, Manufacturer, Model, Supplier Details, Operating Systems and Install Dates. |

|  |  |  |
| --- | --- | --- |
| **Category** | **Description** | **Information** |
|  | conditioning, cabling and dedicated comms rooms. |  |
| IT Infrastructure - Software | This relates to all software 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) and Operating Systems (OS). | Description, Manufacturer, Version, Supplier Details, Operating Systems, Number of Users or Licences and Install Dates. |
| Cyber Security | Cyber Security covers the core infrastructure, physical security and security functions we use to protect our infrastructure, systems and devices. | Description, Manufacturer, Model, Version, Supplier Details, Operating Systems, Network Diagrams, Install Dates, number of cyber breaches, type of cyber breaches, action plan/improvements put in place to combat cyber breaches and staff  responsible for Cyber Security. |

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

## Refusal Notice Section 31(3) – Law Enforcement

The Council believes that telling requesters if we hold information referenced in Table 1 will cause damage.

This is because saying if we do or do not hold specific information would/would likely give cyber criminals insight into vulnerabilities which may, or may not, exist.

This would likely result in damage to our IT infrastructure and systems. Therefore, we use the exemption in section 31(3) which allows us 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 we use a neither confirm or deny response you should not assume that we do, or do not, hold the information requested.

Section 31(3) is a qualified exemption which means we must do 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 if we hold relevant information.

* It would help transparency and accountability of the Council.
* It would reassure people about whether our IT infrastructure and systems are vulnerable or not.
* It would provide information about how effective our IT infrastructure and systems are.

# Factors against confirming or denying if we hold relevant information.

Saying if we hold information would provide information about how effective our 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 our legal obligations to keep personal data secure and to take appropriate measures which includes keeping areas confidential where necessary.

We believe that the balance of public interest lies in upholding the exemption and not confirming or denying if we hold IT information that fall into the categories shown in Table 1.