Freedom of information requests concerning IT Infrastructure, IT security issues, attacks, ransomware, malware and related topics

Author: Leigh Jolly

Version: 1.3 (Published)

Last updated: 7th July 2022

Contents

Introduction

Luton Council operates a number of IT systems. To ensure our data and services are protected we use all the necessary tools to keep our systems and infrastructure safe and secure. We update our estate regularly and comply with the relevant guidance and codes of practice. We have a duty under the Data Protection Act 1998 to keep people's personal data safe and secure and we comply with that duty. Under the new General Data Protection Regulation which comes into force in May 2018 we will have a similar duty to keep personal data securely and safe from attack.

As a public body the council must demonstrate that it keeps its systems and infrastructure safe and complies with prevailing obligations, but at the same time we must be careful that transparency does not provide an opportunity for nefarious groups or individuals to attack the council. Most people will not intend to misuse information provided in good faith. However, there are criminals who try and exploit system weaknesses to cause damage. When we respond to a Freedom of Information request we cannot determine the intent behind every request. Providing information to one authentic requestor effectivity publishes the answer to all. For example, if the council provide information on when we last updated our security software this could be used to exploit any known weaknesses and attack the council. Similarly, revealing details about our infrastructure or the tools and methods we deploy to keep the council safe is valuable information in the wrong hands. The council's data is vast and often of a sensitive nature we must take all necessary steps to ensure we secure it. This means not giving people information that would criminals could exploit to gain unlawful access to our systems and infrastructure.

Freedom of Information Act requests

1. IT Infrastructure and IT security Issues.

We are frequently asked for detailed information about our IT infrastructure and IT security issues in Luton Council. We are often asked about what technology we deploy, and what IT security systems we have in place, the suppliers and versions of our IT security, how often we update and amend our security, whether we have identified particular issues or vulnerabilities and what we have done to strengthen those. The council has considered these issues carefully and we have decided that we do not release this information. This is because we consider it is exempt under section 31 of the Freedom of Information Act 2000. We have explained why below.

Refusal Notice Section 31(1)(a) – Law Enforcement

We will not release detailed information about our infrastructure and what IT security systems we have in place, the suppliers and versions of our IT security, the frequency at which we update and amend our security, details of vulnerabilities and what we have done to strengthen those. We consider disclosing this information could make the council a target of crime. Therefore this information is exempt from disclosure under section 31 of the Freedom of Information Act 2000.

Section 31(1)(a) says that we do not need to provide information that would be likely to prejudice the functions of law enforcement, in this case, the prevention and detection of crime. Luton Council believes that releasing this information would increase the likelihood of

- Criminals using the information to target attacks against council systems. Information about our security systems and infrastructure could allow criminals to determine what vulnerabilities within our estate and use this information for targeted attacks. Luton Council must not release information that would allow personal data it holds to be accessed illegally.

Public Interest Test:

As Section 31 is a qualified exemption we need to consider the public interest test.

Factors in favour of disclosure

- Evidences the council's transparency and accountability
- Reassures the public and partners that the council's systems are secure
- Provides information about how effective our security systems are

Factors in favour of withholding

- The public interest in Crime prevention
- Public interest in avoiding disruption to public services
- Public interest in the council avoiding the costs associated with any attacks recovery, revenue, regulatory fines)
- Public interest in preventing any threat to the integrity of council data
- Public interest in ensuring the council can comply with its duties to take all necessary steps to safeguard data

We believe that the balance of public interest lies in upholding the exemption and not releasing the information.

To provide assurance that council systems are secure we are happy to release details of the compliance standards the council currently meets at the time of the submission of any request. Or alternatively, the council's Cyber Essentials Plus certification can be checked at any time via https://www.ncsc.gov.uk/cyberessentials/search and searching for 'Luton Borough Council'

2. Malware, ransom attacks etc.

We are also often asked questions about malware, ransom ware, attacks and the like. Examples of common questions include whether we have been subject any cyber-attacks within a given period, the volume, whether they have succeeded and what actions we have undertaken to protect the council. We may be asked if we have been the victim of ransom ware, whether attacks were successful, if we paid ransoms, how often, when, to whom and for how much. We have decided that we do not tell requesters if we hold this information or not. Under Freedom Information Act this is called a 'neither confirm nor deny' response.

We can do this under section 31 of the act. We have explained why below.

Refusal Notice Section 31(3) – Law Enforcement

The council believes that informing requesters whether we hold information about cyber-attacks, ransom ware or the like will cause damage. Confirming whether we do or do not hold information would give cyber criminals insight into vulnerabilities which may, or may not, exist. This would pose a threat to damaging our cyber security systems and infrastructure. Therefore, we will use exemption in section 31(3) to respond to such requests. This allows us to refuse to confirm or deny if the information is held. When we use a neither confirm nor deny response you should not assume that we do, or do not, hold any information.

Section 31(3) is a qualified exemption which means we must undertake a public interest test comparing 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.

- Aids transparency and accountability of the council
- Reassure the public or partners about whether our systems are vulnerable or not
- Provides information about how effective our security systems are

Factors against confirming or denying if we hold relevant information.

- Confirming whether we hold information discloses how effective our security systems are. This would be likely to give criminals insight into the strengths and weaknesses of the council's cyber security. Confirming this information would therefore increase the chances of cyber-attack. Cyber security measures are required 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 details about the information it holds this could expose to criminals which of its systems are particularly vulnerable, encouraging attacks

- If the council confirms that it holds little information this could either demonstrate poor reporting and recording procedures which will encourage an attack. Conversely if the council demonstrates it has robust procedures this could encourage an attack by criminals' wishing to try out new techniques to further the capability to conduct criminal activity.

- 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 this information.

As stated in section 1, to provide assurance that council systems are secure we are happy to release details of the compliance standards the council currently meets at the time of the submission of any request. Or alternatively, the council's Cyber Essentials Plus certification can be checked at any time via https://www.ncsc.gov.uk/cyberessentials/search and searching for 'Luton Borough Council'

3. Your Rights

Although you have the right of a review please note that the council has considered this position and unless the law changes is unlikely to change its position on this matter.

However, if you have made a FOI request and you are not happy with how your response was handled you can request an Internal Review within 40 days of being directed to this advice if you wish to activate this please email FOI@luton.gov.uk quoting your case reference number. If you are not satisfied with the internal review outcome you can complain to the Information Commissioner's Office at casework@ico.org.uk telephone 0303 123 1113, or post to Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. The ICO website is www.ico.org.uk

Further references (hyperlinks):

More details about Cyber Essentials Plus

The ICO Website