Freedom of information requests concerning IT Security, infrastructure, and cyber attacks

North Tyneside Council use all necessary tools to keep our systems secure. We have a robust process where we regularly update and review guidance and consider current threats to the security of our data and systems to keep them safe from attack.

We have a responsibility under the Data Protection Act 2018 to keep our customer and staff data secure and we comply with that responsibility with appropriate technical and organisational measures that are in place.

We need to demonstrate how we meet our obligations, but at the same time we need to balance transparency with risk. Under freedom of information, the Authority is not just providing information to one individual, it is publishing the response to the world. There are people who will exploit system weakness to cause damage or defraud the organisation. If we provide information that tells criminals about our system updates for example, they can use this information to exploit any known weaknesses and hack systems.

The Authority hold large amounts of sensitive customer data because we provide many services, including social care and public health. The Authority must take all necessary measures to keep our data and systems secure. This means not advertising system information that would allow criminals to gain unlawful access to our systems.

IT Security Issues

We are frequently asked for information about our IT infrastructure, systems, and security issues, including what systems we have in place, the suppliers, and versions. We are asked how often we update and amend our security, if we have identified any vulnerabilities and what we have done to strengthen any weaknesses.

The Authority has considered these issues carefully and we have decided we do not release information that would fall under this category of data. This is

because we consider it is exempt under section 31 of the Freedom of Information Act 2000.

Refusal notice: Section 31(1)(a) – Law Enforcement

We do not release information that would identify issues or vulnerabilities of our IT systems, including details of suppliers and versions of our IT security, how often we update and amend our security and if we have identified fixes. We consider disclosing this information would make the Authority 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, the prevention and detection of crime. We believe that releasing this information places the Authority at risk and would increase the likelihood of criminals using the information to target attacks against Authority systems. The Authority must protect and safeguard the personal data it holds and not do anything which would allow personal data it to be accessed unlawfully. For example, knowing that last security update and version would allow criminals to know what vulnerabilities exist and target attacks on those.

Public interest test

As section 31 is a qualified exemption we need to apply the public interest test.

Factors in favour of disclosure

- Transparency and accountability
- Reassure customers that our systems are secure
- Provide information about how effective our security systems are

Factors in favour of non-disclosure

- Inherent public interest in crime prevention
- Public interest in protecting the public purse (costs to the authority associated with an attack)

- Public interest in protecting the non-financial cost to the Authority, such as reputational damage/publicity, distress, inconvenience and regulatory action associated with any attacks
- Public interest in preventing threat to the integrity of Authority data
- There is substantial public interest in ensuring that the Authority can continue to comply with its duties as a public Authority
- Public interest in ensuring that the Authority can comply with its duties to take all necessary steps to safeguard data

On balance of the public interest test, we believe that public interest lies in upholding the exemption and not releasing the information.

Malware, ransomware attacks etc

We are frequently asked for information about malware, ransom ware, attacks and other cyber security incidents, including how many attacks, if they succeeded and actions taken, including if we paid ransoms. The Authority have decided that we do not tell requesters if we hold this information or not. Under the Freedom of Information Act, this is a 'neither confirm nor deny' response. We apply this under section 31 of the act.

Refusal notice: Section 31(3)– Law Enforcement

The Authority do not release information that would allow cyber criminals insight into vulnerabilities which may or may not exist, this would likely damage our cyber security systems and plans. We consider disclosing any information would make the Authority a target for cyber-crime. Therefore, the Authority rely on section 31(3) of the Freedom of Information Act 2000. This allows the Authority to refuse to say if we hold any data and you should not assume that we do, or do not hold any data.

Public interest test

As section 31(3) is a qualified exemption we need to apply the public interest test. The public interest test is to determine if we should say if we hold the data or not, not whether we should disclose any data.

Factors in favour of disclosure

- Transparency and accountability
- Reassure customers that our systems are secure
- Provide information about how effective our security systems are

Factors in favour of non-disclosure

- Confirming we hold information on how effective our security systems are would likely give cyber criminals insights into the strengths of Authority systems and any potential weaknesses. This would increase the chances of a cyber-attack.
- The reasons that cyber security measures are in place is to protect the integrity of personal and official data, so increasing chances of a cyber attack would have potential serious repercussions.
- Public interest in protecting the public purse (costs to the authority associated with an attack)
- If the Authority were to confirm it held the data this could show criminals its systems are particularly vulnerable, encouraging attacks.
- If the Authority confirms that it holds little information this could demonstrate either poor or robust reporting and recording procedures which could encourage an attack or for criminals to try out new techniques or target crime elsewhere.
- There is a public interest in complying with our legal obligations to keep personal data secure and to take appropriate organisational and technical measures.

On balance of the public interest test, we believe that public interest lies in upholding the exemption and to neither confirm, nor deny we hold the data.

Right of review

You have the right to a review of the Authority decision; however, the Authority last reviewed its position in May 2023. The Authority will review this position annually.

If you have made a Freedom of Information request to the Authority and you are unhappy with the initial response you may request an internal review within two months of the response by contacting FOI.Officer@northtyneside.gov.uk please quote your FOI reference number.

If you are not satisfied with the response to your internal review, you may contact the information Commissioner's Office at www.ico.org.uk or via post below:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113