FREEDOM OF INFORMATION REQUESTS CONCERNING IT SECURITY INFORMATION, ATTACKS, RANSOMWARE AND MALWARE

Document status: Revised April 2026

Introduction

Gloucester City Council has robust IT and cyber security controls in place. The Council uses appropriate technical and organisational measures to protect its systems, infrastructure and information assets, and these controls are reviewed and updated regularly in line with relevant guidance and recognised good practice.

The Council has statutory obligations under the **Data Protection Act 2018** to ensure that personal data is processed securely. These obligations continue under the **UK General Data Protection Regulation (UK GDPR)**, including the requirement to protect personal data against unauthorised or unlawful access, loss or damage.

[UPDATED 2026] These obligations remain in force following recent UK data protection reforms, including amendments made by the *Data (Use and Access) Act 2025*. Nothing in those reforms reduces or removes the Council's duty to maintain appropriate security measures or to avoid actions that could weaken the security of its information systems.

Although the Council supports transparency and accountability, it must balance this against its legal responsibilities. Information disclosed under the Freedom of Information Act 2000 (FOIA) is effectively disclosed to the public at large. Excessive transparency in relation to cyber security arrangements may increase the risk of criminal exploitation and compromise system security.

While most requesters act lawfully, there remains an active and persistent threat from cyber criminals who seek to identify and exploit system weaknesses. Disclosure of detailed technical information could directly assist such activity.

The Council holds significant volumes of personal and sensitive personal data relating to residents, service users and staff. Protecting the confidentiality, integrity and availability of that data requires that certain information is not placed into the public domain.

The Council has also had regard to relevant Information Commissioner's Office (ICO) decision notices, including FS50662638, FS50600199, FS50665770 and FS50662675, which support the withholding of sensitive IT and cyber security information. These examples are illustrative rather than exhaustive

---

Freedom of Information Act requests

The Council frequently receives FOIA requests seeking information relating to its IT infrastructure and cyber security arrangements. Typical request categories are outlined below.

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 • Installation 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 services, including: • web services • Enterprise Resource Planning (ERP) • Customer Relationship Management (CRM) • Corporate applications • Commercial off-the-shelf software (COTS) • Line of business (LOB) applications • Operating systems	Information including: • Description / type • Manufacturer • Version • Operating systems • Number of users • Number and type of licences • Installation dates • Project documentation related to installations, upgrades and developments
Cyber Security	Cyber security measures used to protect Council infrastructure, systems and devices, including: • core infrastructure • physical security	Information including: • Description / type • Manufacturer • Model • Version

	• security functions • systems and developments	• Operating systems • Network diagrams • Installation dates • Project documentation • Number and type of cyber breaches • Action plans, improvements or guidance • Staff responsible for cyber security • Information that may influence the timing of a cyber attack

---

Application of FOIA exemptions

The Council has considered these categories carefully and has determined that disclosure would, or would be likely to, prejudice the prevention or detection of crime. The information is therefore exempt under **section 31(1)(a)** of the Freedom of Information Act 2000.

Where requests seek confirmation as to whether specific information is held, the Council relies on **section 31(3)** of the Act to provide a *neither confirm nor deny* (NCND) response.

[UPDATED 2026] NCND responses are applied consistently, where confirmation or denial alone would itself reveal information about the Council's security posture or system architecture regardless of whether the information is held.

Each request will continue to be considered on its own merits and exemptions will only be applied where the statutory tests are met.

Prejudice test

Applicable interest

The applicable interest is the prevention and detection of crime, specifically the protection of the Council's information systems from unlawful access, exploitation or disruption.

Disclosure of detailed technical information could be combined with other publicly available information, creating a "mosaic effect" that assists criminal activity. Any disclosure under FOIA is treated as disclosure to the world at large.

Nature of the prejudice

The likely prejudice includes increased risk of cyber-attack, unauthorised access to personal and sensitive personal data, disruption to essential public services, financial loss, regulatory consequences and reputational damage.

Disclosing details of systems, software versions or security controls would provide attackers with information that could be used to exploit known vulnerabilities.

Likelihood of prejudice

There is a real and significant risk that such prejudice would occur. The ICO and the National Cyber Security Centre continue to identify exploitation of known vulnerabilities as the most common cause of serious cyber incidents.

[UPDATED 2026] Recent ICO enforcement action following cyber incidents has reinforced the expectation that organisations avoid avoidable or unnecessary disclosure of sensitive technical detail.

Causal link

There is a clear causal link between disclosure of detailed cyber security information and the increased likelihood of criminal exploitation and harm.

Public interest test

Section 31 is a qualified exemption, and the public interest test has been applied.

Factors in favour of disclosure

- Promoting transparency and accountability
- Reassuring the public that systems are in place to protect data
- Supporting public understanding of Council operations

Factors in favour of withholding

- Strong public interest in crime prevention
- Protection of personal and sensitive personal data
- Avoiding disruption to essential public services
- Avoiding financial and reputational damage
- Maintaining compliance with data protection legislation

[UPDATED 2026] There is a clear public interest in ensuring that cyber security and data protection controls are not weakened through disclosure of information that could reasonably be exploited.

Conclusion

Having considered all relevant factors, the Council concludes that the public interest lies in maintaining the exemption under section 31 of the Freedom of Information Act 2000 and, where appropriate, issuing a neither confirm nor deny response.

This position remains consistent with current ICO guidance, FOIA case law and the Council's statutory obligations under the Data Protection Act 2018 and UK GDPR.

The Council will continue to review this policy regularly to ensure it reflects legal requirements and best practice.

Review date: April 2027