

Halton Borough Council's Statement on Requests for Technical Network Information

In accordance with **Section 31 of the Freedom of Information Act 2000**, Halton Borough Council is unlikely to disclose information relating to the technical or physical specifications of our computer network infrastructure. This includes, but is not limited to, details about:

- Network architecture and configuration
 - Data storage systems
 - Firewall technologies and configurations
 - Anti-virus and endpoint protection solutions
-

Section 31 – Law Enforcement Exemption

Under **Section 31(1)(a)** of the Freedom of Information Act 2000, information is exempt from disclosure if its release would, or would be likely to, prejudice the prevention or detection of crime. This is a **qualified exemption**, requiring an assessment of both the potential harm and the balance of public interest.

Evidence of Harm

Requests for information related to the Council's network security protections, even seemingly minor technical details, when combined with other publicly available data, could be used to build a profile of our IT infrastructure. This could enable targeted cyber-attacks or exploitation of specific vulnerabilities.

At a time of heightened global cyber threats, disclosing such information would increase the risk of unauthorised access to Council systems and sensitive data. It would also undermine the effectiveness of our security controls and expose the Council to greater operational and reputational risk.

Public Interest Test

Factors in favour of disclosure:

- Promotes transparency and public confidence in the Council's cybersecurity practices.
- May reassure the public that appropriate controls are in place.

However, these objectives are already met through:

- Independent assurance from third-party security specialists.
- Oversight by internal and external auditors.
- Compliance with national cybersecurity standards and frameworks.

Factors against disclosure:

- Could provide malicious actors with insights into the Council's security posture.
- May facilitate criminal activity, including offences under the **Computer Misuse Act 1990**.

- Could compromise the Council's compliance with **UK GDPR** and data protection obligations.
- Would weaken the Council's cybersecurity resilience and increase the risk of harm to individuals and services.

Conclusion

After careful consideration, we have concluded that the public interest in maintaining the exemption outweighs the public interest in disclosure. The release of this type information would be likely to prejudice the prevention or detection of crime and compromise the security of the Council's IT systems.

Accordingly, the requests for this type of information is likely to be withheld under Section 31(1)(a) of the Freedom of Information Act 2000..