Belfast Health and Social Care Trust
caring supporting improving together

FOI/34178

17 July 2025

How Public Sector Organisations Procure Cyber Security Services and Enterprise Software Platforms

1. Standard Firewall (Network)

Firewall services that protect the organisation's network from unauthorised access and other internet security threats.

2. Anti-virus Software Application

Programs designed to prevent, detect, and remove viruses, malware, trojans, adware, and related threats.

3. Microsoft Enterprise Agreement

A volume licensing agreement that may include:

Microsoft 365 (Office, Exchange, SharePoint, Teams)
Windows Enterprise
Enterprise Mobility + Security (EMS)
Azure services (committed or pay-as-you-go)

4. Microsoft Power BI

Or any alternative business intelligence platform used for data connectivity, dashboards, and reporting.

	Standard Firewall (Network)	Anti-virus Software Application	Microsoft Enterprise Agreement	Microsoft Power BI
	Firewall services that protect the organisation's network from unauthorised access and other internet security threats.	Programs designed to prevent, detect, and remove viruses, malware, trojans, adware, and related threats.	A volume licensing agreement that may include: · Microsoft 365 (Office, Exchange, SharePoint, Teams) · Windows Enterprise	Or any alternative business intelligence platform used for data connectivity, dashboards, and reporting.

17 July 2025

			· Enterprise Mobility + Security (EMS) · Azure services (committed or pay-as-you-go)	
1. Who is the existing supplier for this contract?	* Witheld	* Witheld	* Witheld	* Witheld
2. What is the annual spend for each contract?	* Witheld	* Witheld	* Witheld	* Witheld
3. What is the description of the services provided?	* Witheld	* Witheld	* Witheld	* Witheld
4. Primary brand (where applicable)	* Witheld	* Witheld	* Witheld	* Witheld
5. What is the start date of the contract?	* Witheld	* Witheld	* Witheld	* Witheld
6. What is the expiry date of the contract?	* Witheld	* Witheld	* Witheld	* Witheld
7. What is the total duration of the contract?	* Witheld	* Witheld	* Witheld	* Witheld
8. Who is the responsible contract officer? **Please include at least their job title, and where possible, name, contact number, and direct email address**	Contracts & Procurement Manager ITContractManager@belfasttrust.hscni.net	Contracts & Procurement Manager ITContractManager@belfasttrust.hscni.net	Contracts & Procurement Manager ITContractManager@belfasttrust.hscni.net	Contracts & Procurement Manager ITContractManager@belfasttrust.hscni.net
9. How many licences or users are included (where applicable)?	* Witheld	* Witheld	* Witheld	* Witheld

Disclosure of information about Belfast Trusts core digital infrastructure would put the Trusts digital infrastructure under elevated levels of security risk and become more vulnerable to a malicious cyber security attack. The disclosure of such information would:

a) (Section 31) Leave Belfast Trust, Patients, Clients & Staff more vulnerable to crime;

b) (Section 38) Be likely to endanger the safety, or the physical or mental health of individuals within Belfast Trust;

c) (Section 43) Pose a significant threat to the integrity & operation of the digital systems on which the day-to-day business of the Trust relies

17 July 2025

Section 31 – Law Enforcement

Section 31(1)(a) states that information is exempt if its disclosure is likely to prejudice the prevention or detection of crime. ICO guidance states that this can be used to protect information on a public authority's systems which would make it more vulnerable to crime. It can be used by a public authority that has no law enforcement function:

- To protect the work of one that does
- To withhold information that would make anyone, including the public authority itself, more vulnerable to crime

Section 38 – Health and Safety

Section 38 states that information is exempt if its disclosure could lead to the physical or mental harm of, or endanger the safety of, individuals.
Disclosure of the requested information would leave the Belfast Trusts digital infrastructure at significant risk of cyber security attack. A cyber-security attack may lead to the placing of sensitive health & social care information into the public domain and, as such, the Trust believes there is a link between the risk of endangerment for data subjects and the disclosure of the requested information. There would likely be a substantial detrimental effect on the physical or mental health of patients, clients, staff or their families should the requested information be released.

Section 43 – Commercial Interests

Section 43(2) states that information is exempt if its disclosure would, or would be likely to, prejudice the commercial interests of any person (including the public authority holding it). Disclosure of the requested information would leave the Belfast Trusts digital infrastructure at significant risk of cyber security attack. This would compromise the Belfast Trusts ability to provide Health & Social Care Services and carry on business-as usual should the digital systems be compromised.