

17 December 2025

## **Wide Area Network Services**

### **Contract 1 – Wide Area Network (WAN) Services (Including HSCN)**

#### **WAN Provider(s)**

**Please confirm the main supplier(s) for your WAN services. If this information is not available, please explain why.**

\*Information withheld on the basis of cybersecurity threat

#### **Contract Expiry Date**

**Please provide the expiry date for each WAN contract (DD/MM/YYYY or MM/YYYY acceptable).**

\*Information withheld on the basis of cybersecurity threat

**If rolling, please state the terms.**

#### **Contract Description**

**Please provide a brief summary of the scope of each WAN contract.**

\*Information withheld on the basis of cybersecurity threat

#### **Number of Sites Covered**

**Please indicate the number of sites supported by the WAN. An approximation is Acceptable.**

Digital infrastructure is available across the entire Trust Estate  
<https://belfasttrust.hscni.net/about/facilities/>

#### **Annual Average Spend**

**What is the annual average spend for WAN services? Please break this down by provider**

\*Information withheld on the basis of cybersecurity threat

**if more than one.**

#### **Procurement Route**

17 December 2025

**Please provide details of how each WAN contract was procured. If a framework was used, please include the framework name and reference number.**

The Belfast Trust complies with the Public Procurement Act 2023, Procurement Regulations 2024 and Northern Ireland Public Procurement Policy. All procurement is carried out in conjunction with the Business Services Organisation (BSO) Procurement and Logistics Service (PaLS) as the CoPE for HSCNI.

\*Details related to specific digital infrastructure contracts is withheld on the basis of cybersecurity.

### **Internal Contact**

#### **Responsible Contact Person(s)**

**Please provide the full contact details for the person(s) responsible for each of the above contracts, including:**

Contracts & Procurement Manager [ITContractManager@belfasttrust.hscni.net](mailto:ITContractManager@belfasttrust.hscni.net)

**Full name**

**Job title**

**Direct phone number**

**Email address**

**If full details cannot be provided, the job title alone is acceptable.**

#### **\*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

**17 December 2025**

### **Section 38 – Health & 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.

### **Outcome**

There is an overwhelming public interest in keeping Health & Social Care digital systems and critical national infrastructure secure which would be served by non-disclosure. This outweighs the public interest in accountability and transparency which would be served by disclosure.