Belfast Health and Social Care Trust
caring supporting improving together

FOI/35851

24 February 2026

Monthly Spend Reporting (Over £25K)

As part of our ongoing effort to maintain accurate and complete financial datasets across NHS Trusts, I am reaching out to kindly request the monthly "Spend over £25k" report for your organisation. If available, could you please provide:

- **The latest monthly report(s) covering the last 3 financial years**
- **Preferably in Excel (XLSX) or CSV format**
- **Including standard fields such as *Entity, Expense Type, Supplier, Amount, Invoice Number, Transaction Number,* and *Source URL* (if applicable)**

Belfast Health and Social Care Trust's response to this request can be found in the attached Excel spreadsheet.

Please note the response has been partially redacted, as follows:

1. Where the supplier is a named individual, we have removed the supplier name. However we have left the associated amount, type of spend and period.

   We are unable to provide the identity of an individual as this information is exempt from release under Section 40(2) of the Freedom of Information Act - Personal Information relating to a third party because this would involve making an individual personally identifiable. Disclosure would constitute a breach of the principles of the General Data Protection Regulation 2018.

2. Payments that relate to ICT spend and ICT infrastructure have been removed in line with considerations below:

   - The current cyber security threat level associated with healthcare in Northern Ireland continues to be categorised as HIGH.
   - Healthcare organisations are a primary target for cybercriminals and this has been reflected in a number of targeted cyber-attacks on partner organisations, including Health Service Executive Ireland (HSE.ie), Queens University (QUB) and NHS Dumfries & Galloway.
   - Cybercriminals continue to target 3rd party suppliers as a way to gain access to customers' infrastructure, including current suppliers to HSCNI; disclosing information about spend against suppliers associated with specific core infrastructure, services or systems may result in directly or indirectly disclosing operational defences as well as 3rd party supply chain.

- All information provided about core health service digital infrastructure, services or systems is valuable cyber reconnaissance. This includes information about supplier payments. Disclosing information publicly, no matter how insignificant each piece may appear, facilitates cyber reconnaissance, increases the scale of the potential attack surface using actionable intelligence and could lead to an increase in targeted attacks.
- Once information is disclosed, it is assumed that it will at some point become publicly known.

*All of the information relating to ICT spend is exempt from release under Section 31(1)(a) - Law Enforcement, Section 38 – Health and Safety and Section 43 – Commercial Interests.

These exemptions are Qualified Exemptions and are therefore subject to a Public Interest Test (PIT).

I can confirm that we have now carried out a PIT and the outcome is to maintain the exemptions and withhold the information from release.