Belfast Health and Social Care Trust
caring supporting improving together

FOI/32832

30 December 2024

ICT Budget and Spending Plans for Next Fiscal Year

1. **The allocated budget for ICT in the next fiscal year.**

   No information available – 25/26 Budget for Digital Services has not yet been set

2. **A breakdown of planned spending within the ICT budget, including major projects or initiatives identified by name.**

   No information available

3. **Any documentation or reports that outline your ICT priorities or strategies for the next fiscal year.**

   Digital Strategy 2020-25 (redacted on basis of cyber security threat) attached.

   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

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 & 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.

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.