Belfast Health and Social Care Trust
caring supporting improving together

**FOI/36709**

**30 April 2026**

# Use of Palantir Technologies

**This is an FOI request about Palantir Technologies.**

1. **Does this Trust or any Trust in Northern Ireland use Palantir software for any purpose or policy?**

   Belfast Health and Social Care Trust operates in a high cyber-threat environment and takes a risk-based approach to public disclosures about digital systems and suppliers to protect the resilience of essential healthcare services. The Trust does not routinely confirm or deny supplier / platform-specific usage were doing so could increase the risk of targeted cybercrime, including phishing, ransomware or supply-chain targeting. This includes consideration of the "mosaic effect", where multiple disclosures can be aggregated to create actionable intelligence.

   We can advise that the Trust uses a range of digital tools for analytics in specific service contexts and seeks to be transparent about governance and assurance, providing high-level assurance where feasible, whilst avoiding disclosure of details that would increase the attack surface.

   This type of information is withheld from disclosure under the following exemptions:

   - Section 24(1) — National security: safeguarding against threats including disruptive cyber-attacks
   - Section 31(1)(a) - Law Enforcement
   - Section 43 – Commercial Interests.

   Confirming or detailing specific products can contribute to cyber reconnaissance and supply chain targeting; ICO recognises software / infrastructure detail can aid attacks and may be compiled with other sources ("mosaic effect").

2. **If so, please state the name of the software, the date on which use commenced, and the purposes and policies for which it is used.**

   Information exempt from disclosure under:

   - Section 24(1) — National security: safeguarding against threats including disruptive cyber-attacks
   - Section 31(1)(a) - Law Enforcement
   - Section 43 – Commercial Interests.

Granular product name / date / purpose / policy information increases attack surface and supports targeted phishing / supply chain reconnaissance; ICO notes risk from disclosing IT infrastructure / software details.

3. **Do you upload patient data to Palantir, e.g. Foundry? Please state the name of this data, the policy under which it is uploaded and whether it is "de-identified", "pseudonymised" or anonymised.**

   Information, exempt from disclosure under:

   - Section 24(1) — National security: safeguarding against threats including disruptive cyber-attacks
   - Section 31(1)(a) - Law Enforcement
   - Section 38 — Health and safety

   Disclosure would materially increase attacker understanding of data value / handling and could facilitate unlawful access attempts; Trust notes phishing / ransomware risks and reconnaissance value; ICO flags risk where disclosure reveals weaknesses or usable system detail

4. **Have you conducted Data Protection Impact Assessments on your use of Palantir? Please provide a copy of these impact assessments if so.**

   DPIAs are mandated in Belfast Trust when new personal data is collected or existing data is used in new ways, shared with new parties, or when changes affect data management or security.

   Information, exempt from disclosure under:

   - Section 24(1) — National security: safeguarding against threats including disruptive cyber-attacks
   - Section 31(1)(a) - Law Enforcement

   DPIAs contain high-risk security-related content; ICO notes security arrangements / infrastructure detail can increase cyber-attack risk; Trust position emphasises reconnaissance and supply chain targeting

**If you use Palantir software:**

5. **Please provide copies of correspondence between relevant employees of your organisation and employees of Palantir related to the implementation and usage of - and troubleshooting issues with - Palantir software. Please define correspondence as emails, text messages and WhatsApp messages generated since 01/06/2022.**

As noted in Question 1, Belfast Trust uses a range of digital tools for analytics in specific service contexts - it does not routinely confirm or deny supplier / platform-specific usage. Information, exempt from disclosure under:

- Section 24(1) — National security: safeguarding against threats including disruptive cyber-attacks
- Section 31(1)(a) - Law Enforcement
- Section 38 — Health and safety
- Section 43 – Commercial Interests.

Correspondence with regard to any digital tools likely contains operational detail useful for reconnaissance and may include staff identifiers (targeting risk) and commercially sensitive content; ICO highlights risks of disclosing information that aids attacks and that attackers compile details from many sources.

6. **Please provide copies of internal correspondence related to the implementation and usage of - and troubleshooting issues with - Palantir software. Please define internal correspondence as emails generated since 01/06/2022.**

Same rationale as Q5; internal correspondence regarding any digital tools is likely to contain technical / operational and security-control context that increases risk; Trust highlights phishing / ransomware and supplier-targeting dynamics. Information, exempt from disclosure under:

- Section 24(1) — National security: safeguarding against threats including disruptive cyber-attacks
- Section 31(1)(a) - Law Enforcement
- Section 38 — Health and safety
- Section 43 – Commercial Interests.

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

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