Belfast Health and Social Care Trust
caring supporting improving together

# FOI/36477

**2 April 2026**

# Processes for software based data erasure of end of life IT equipment

**Under the Freedom of Information Act 2000, please provide the following recorded information held by your organisation regarding assurance processes for software based data erasure of end of life IT equipment.**

**For clarity, this request relates specifically to the erasure of storage media associated with end of life hardware such as laptops, desktops, servers, storage arrays, or other data bearing IT equipment. It does not relate to operational deletion of data within live systems, routine account management, or DSP Toolkit self assessment processes.**

**Physical destruction methods such as shredding, crushing, degaussing, or disintegration are outside the scope of this request. This request concerns software based erasure only.**

**This request seeks to distinguish between confirmation that an erasure process was carried out and recorded evidence demonstrating that the final data state of a specific storage device is irrecoverable. I am not seeking technical configuration detail or security sensitive information, only the recorded assurance basis relied upon when concluding that personal data has been rendered irrecoverable.**

**Please confirm:**

**1) Whether your organisation's policies, contractual terms, or internal procedures require an explicit outcome based warranty or guarantee that personal data on a specific storage device has been rendered irrecoverable as a final data state following software based erasure.**

**2) Where software based erasure of storage media is undertaken internally, what recorded evidential assurance is relied upon to conclude that the final data state of the specific storage device is irrecoverable, as distinct from confirmation that an erasure process was executed.**

**3) Where software based erasure is undertaken by a third party provider:**

**a. Do the certificates or contractual documents held constitute an explicit outcome based warranty or guarantee of irrecoverability for each specific storage device processed?**

**b. Beyond reliance on supplier accreditation or recognised standards including but not limited to ADISA certification, ISO accreditation, NIST alignment, HMG IA standards, NHS Digital guidance, or Data Security and Protection Toolkit assertions, and beyond confirmation that a wiping process was completed, does the organisation hold any recorded, device specific**

**documentation evidencing independent verification, testing, or validation that the data on the storage media has been rendered irrecoverable in practice?**

**4) If no explicit outcome based warranty or device specific outcome evidence is held beyond certification, accreditation, or confirmation of process completion, please confirm what recorded form of evidential assurance is relied upon when concluding that personal data has been rendered irrecoverable**

Belfast Health and Social Care Trust
caring supporting improving together

# FOI/36477

**2 April 2026**

Belfast Trust Response

| Item | Request Element | Information Held | Disclosure Decision | Exemption Applied | Harm / Risk Rationale | Safe Alternative Disclosure Provided |
|---|---|---|---|---|---|---|
| 1 | Whether policies/procedures require outcome-based warranty of irrecoverability | Framework-mandated confirmation of wiping/destruction; reliance on accredited standards | Partially disclosed | s31(1)(a), s24 | Confirming existence of assurance without disclosing outcome guarantees avoids mapping assurance thresholds that could be exploited to test residual risk. Aggregation with supplier standards would increase reconnaissance value. | Yes – high-level confirmation of standards-based assurance |
| 2 | Evidential assurance for internally conducted software erasure | Records of process completion and framework-aligned confirmation | Partially disclosed | s31(1)(a) | Detailed evidential artefacts or validation methods would expose operational controls and verification depth, enabling attackers to infer residual data risk or bypass thresholds. | Yes – confirmation that assurance is recorded and standards-aligned |
| 3a | Third-party outcome-based warranties | Supplier framework confirmation mechanisms | Partially disclosed | s31(1)(a), s24 | Disclosing whether warranties exist at device-level would allow attackers to differentiate higher-value targets and supply-chain weaknesses. Aggregation risk applies. | Yes – confirmation of contractual assurance via framework |

| | | | | | | |
|---|---|---|---|---|---|---|
| 3b | Device-specific independent verification/testing evidence | Supplier certificates and confirmations held | Withheld | s31(1)(a), s24 | Disclosure would reveal verification depth, sampling practices, and confidence levels, materially aiding cyber-reconnaissance and targeted exploitation of disposal lifecycle. | Yes – confirmation that accredited certification is relied upon |
| 4 | If no outcome warranty exists, what assurance is relied upon | Framework standards and accredited supplier processes | Partially disclosed | s31(1)(a) | Detailed articulation of assurance gaps or compensating controls would weaken overall security posture when combined with other publicly available information. | Yes – narrative assurance without operational detail |