

Our Ref: NG/RM/26069
Date: 17th March 2026

Nicola Griffiths
Deputy Director of Governance
North Staffordshire Combined Healthcare NHS Trust
Lawton House
Bellringer Road
Trentham
ST4 8HH

Reception: 0300 123 1535

Dear

Freedom of Information Act Request

I am writing in response to your e-mail of the 4th March 2026. Your request has been processed using the Trust's procedures for the disclosure of information under the Freedom of Information Act (2000).

Requested information:

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. **The Trust's policies, procedures, and contractual arrangements for the disposal of IT equipment require that storage media is sanitised in accordance with recognised industry and government standards.**

These arrangements require that approved data erasure methods are used and that the process is documented and auditable. However, the Trust does not

require an explicit outcome-based warranty or guarantee stating that data on a specific storage device has been rendered irrecoverable as a final data state. Assurance is instead derived from compliance with recognised standards, the use of approved erasure tools or services, and the maintenance of audit records demonstrating that the erasure process has been completed.

- 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. **The Trust does not currently undertake software-based erasure of end-of-life storage media internally. This question therefore does not apply, and no internal evidential assurance records of the type described exist.**

- 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? **Certificates of erasure or destruction are provided by the supplier for devices processed. These confirm that erasure has been carried out in accordance with recognised standards and the supplier's certified processes. The Trust does not hold documentation constituting an explicit outcome-based warranty guaranteeing irrecoverability of data on each individual storage device.**

 - 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? **Beyond confirmation that the erasure process has been completed and reliance on supplier accreditation and recognised standards, the Trust does not hold device-specific documentation evidencing independent forensic verification or testing that 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. **The Trust acknowledges the distinction the requester draws between confirmation that an erasure process was executed and outcome-based evidence that a specific device's data has been rendered irrecoverable. The Trust does not hold the latter.**

The assurance framework relied upon is standards and process-based rather than outcome-verified at device level. This comprises:

- Compliance with recognised data sanitisation standards (e.g. NIST SP 800-88 or equivalent guidance)
- Use of certified or approved erasure tools and processes
- Supplier accreditation and industry certification where third-party services are used (for example ADISA certification, ISO standards, or equivalent)
- Certificates of erasure or destruction issued by the service provider
- Asset disposal records and audit trails linking erasure activity to specific devices
- Organisational policies and procedures governing secure disposal of IT equipment

The Trust considers this approach consistent with accepted NHS data security practice and proportionate to the risk profile of the devices processed. Standards-based assurance is the recognised model within the sector; outcome-verified forensic testing of individual devices is not a requirement under current NHS data security guidance or ICO expectations for organisations of this type.

If you are dissatisfied with the handling of your request, you have the right to ask for an internal review of the management of your request. Internal review requests should be submitted within two months of the date of receipt of the response to your original letter and should be addressed to: Dr Buki Adeyemo, Chief Executive, North Staffordshire Combined Healthcare Trust, Trust Headquarters, Lawton House, Bellringer Road, Trentham, ST4 8HH. If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Yours sincerely



Nicola Griffiths
Deputy Director of Governance