Our Ref: 153
March 2026

Doncaster and Bassetlaw Teaching Hospitals
NHS Foundation Trust

Freedom of Information Act Request

I am writing to request information under the Freedom of Information Act 2000.

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.

Response:
No. Our documented process does not use software-based erasure as the final method. Instead, drives are recorded, securely stored, and then sent for physical destruction (secure shredding) with a disposal certificate. Therefore, a warranty/guarantee specifically about software erasure producing an "irrecoverable" final state is not applicable to the process we follow

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.

Response:
Software-based erasure is not being carried out internally i. Our assurance is based on chain-of-custody controls and physical destruction, not proving irrecoverability after internal wiping

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?

Response:

The documented approach is physical destruction and **not software erasure**, supported by a supplier disposal certificate and a requirement to check each drive against that certificate.

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?

Response:
The documented process does not describe device-specific independent verification of software wiping, because the method used is physical destruction. The device-specific evidence held is the manifest/recording, and certificate reconciliation per drive.

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.

Response:
We rely on recorded evidence that supports secure handling and confirmed physical destruction, including:

- Each drive is logged with identifying details (for example serial number and asset number) and allocated to a manifest/batch.
- Drives are sealed in boxes and kept locked in the IT Storeroom until transfer to the Estates secure lock-up for destruction.
- Transfers are controlled and recorded against the manifest (including locations and dates/times)
- After disposal, each drive is checked off against the supplier's disposal certificate, and any discrepancies are escalated.

This is the evidential basis used to conclude data is rendered irrecoverable, because the drives are physically destroyed rather than software-wiped

If you are not satisfied with the handling of your request, you have the right to request

an internal review. Requests for an internal review should be submitted within 40 working days from the date of this response, and should be addressed to d.wraith@nhs.net.

If you remain dissatisfied after the internal review, you have the right to appeal to the Information Commissioner's Office (ICO). The ICO can be contacted at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113
Website: https://ico.org.uk/make-a-complaint/

Our Ref: 153
March 2026

Doncaster and Bassetlaw Teaching Hospitals
NHS Foundation Trust