Reference: FOI.ICB-2526/435

Subject: Recorded Assurance for Software Based Data Erasure of End of Life IT Equipment

I can confirm that the ICB does hold the information requested; please see responses below:

QUESTION	RESPONSE
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.	South, Central and West Commissioning Support Unit (SCW CSU) provides end of life processes for IT equipment on behalf of BNSSG ICB. Please find attached the DDaT IT Disposal Policy v6.0 dated July 2025 which defines the policy for secure equipment disposal. Please note: FOI requests and responses are publicly available and therefore personal information has been redacted from the policy.

	The ICB considers the names of staff personal information and has therefore applied a Section 40 exemption to this information.
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.	n/a
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?	SCW CSU only use approved contractors who meet the standards outlined by NHS England: • All data is destroyed in accordance with the certification data capability requirement attached to the ADISA ICT Asset Recovery Standard • A UKAS accredited certification body have certified their processes and procedure to be compliant with the following standards: ISO 9001:2015 (Quality Management System) ISO 14001:2015 (Environmental Management System) ISO 27001:2013/2022 (Information Security Management System) ISO 45001:2018 (Occupational Health and Safety Management System) • Premises are an Approved Authorised Treatment Facility (AATF) for processing and recycling electrical waste and they have an Environmental Permit or exemption and Waste Carriers Registration • Able to securely sanitise data with an approved software solution independently tested to meet the Purge requirements

	as laid out in a recognised international standard eg IEEE2883-2022. If Purge commands are not supported by the asset the software shall fall back to Clear
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.	n/a

The information provided in this response is accurate as of 10 March 2026 and has been approved for release by Seb Habibi, Interim Chief Transformation and Digital Officer for NHS Bristol, North Somerset and South Gloucestershire ICB.

- OFFICIAL

DDaT IT Disposal Policy

Version 6.0 July 2025

Document control

Document name	Version	Status	Author
DDaT IT Disposal Policy	6.0	Final	[redacted]

Document objectives	This document defines the Policy for Secure Equipment Disposal.	
Target audience	The Policy provides the framework for SCW IT Asset Disposal ITAD) which must be followed by all SCW staff and external suppliers when managing assets on behalf of customers.	
Committee/group consulted	DDAT Finance Performance and Assurance Committee (FPAC)	
Monitoring arrangements and indicators	This policy will be monitored by the DDaT FPAC to ensure any legislative changes that occur before the review date are incorporated.	
Training/resource implications	Training and assistance in adhering to the Policy will be provided by DDaT, Service Delivery, IT Asset Management Team.	
Reviewed, Approved, and Ratified by	DDaT Senior Leadership Team	Date:08/07/2025
	Information Governance Steering Group	Date:
	Corporate Governance and Assurance Group	Date:
Equality Impact Assessment	Yes	Date:

Date issued	08/07/2025	Review date	07/07/2027
Practice Owner	DDaT Director of Service Delivery		
Policy Owner	ITAM Consultant		
Lead Director	Chief Digital Information Officer		

Version control Change record

Date	Author	Version	Page	Reason for change
18/07/2023	[redacted]	5.0		Reviewed by DDaT Senior Management Leadership Team
09/07/2024	[redacted]	5.1	8-10	Updates in line with industry standards
18/07/2024	[redacted]	5.1		Review and approval for 5.1 updates at the DDaT FPAC
13/05/2025	ITAM Managers	5.2	All	Review and update policy
11/06/2025	[redacted]	5.2		Full review by SME and Contributors completed prior to commencement of approval cycle
19/06/2025	[redacted]	5.2		Full review by the DDaT FPAC
08/07/2025	[redacted]	6.0		Approved by DDaT SLT

Reviewers / contributors

Date	Name	Version	Position
11/06/2025	[redacted]	5.2	Service Asset and Configuration Manager
11/06/2025	[redacted]	5.2	Technical Governance Lead
11/06/2025	[redacted]	5.2	Cyber Security Manager
11/06/2025	[redacted]	5.2	Software Asset Manager
11/06/2025	[redacted]	5.2	Hardware Asset Manager
19/06/2025	DDaT FPAC membership	5.2	DDaT Governance Committee

Contents

1. Introduction

Information, and in particular sensitive data disclosure has become a major risk to organisations, primarily due to the increasing dependence on electronic storage systems and the use of disposable media.

The purpose of the policy is to ensure NHS and third-party systems which deal with sensitive data is disposed of in line with national requirements to prevent unauthorised disclosure.

All NHS South, Central and West Commissioning Support Unit (SCW) employees are responsible for maintaining confidentiality. This duty of confidentiality is written into employment contracts and reinforced through mandatory training. Breach of confidentiality of information gained, either directly or indirectly, in the course of duty is a disciplinary offence that could result in dismissal. As such, confidentiality must be always maintained from the creation of a record or document, its use, its storage, retention, disposal and finally destruction. This policy supports the implementation of UK GDPR, The Freedom of Information Act, the Public Records Act and other related legislation, Department of Health NHS Codes of Practice in relation to Information Governance and best practice guidance, in particular the NHS best practice guidance on the Disposal and Destruction of Sensitive Data. This policy endorses Organisation policies relating to confidentiality and data protection, information security and information governance.

ITIL 4 introduce the concept of Practices which are a set of resources designed to perform work and accomplish objectives. In addition to the resources, they align the capabilities of the organisation to complete the process and procedures. ITIL 4 groups practices into 3 areas:

- Management Practices
- Service Management Practices
- Technical Management Practices

Disposal is part of the management of the Asset life cycle process and is part of the IT Asset Management Service Management Practice in ITIL 4.

2. Scope and definitions

This policy applies to all staff in SCW, customers and all contractors working for them. This policy will focus on secure disposal and destruction of all SCW managed IT equipment. The Organisation's process for the disposal of sensitive data also includes the guiding principles when disposing of or destroying other types of confidential or sensitive information assets.

SCW has the responsibility to dispose of all redundant IT equipment and data relating to SCW and its customer organisations. The objective of this policy is to ensure that the correct guidance is followed for IT equipment and data disposal, especially in relation to the destruction of sensitive data stored or processed on IT equipment.

Additionally, this policy aims to limit any risk to SCW and its customers. The loss of sensitive data, whilst in the care of the CSU, may incur legal and financial sanctions on SCW and its employees. Staff can be personally liable for any loss of IT equipment or sensitive data.

This policy focusses on the secure disposal and destruction of SCW hardware including end user computing, other user devices, and key infrastructure equipment, for example, servers, firewalls, switches and data storage devices.

The following are out of scope and therefore excluded from secure disposal:

- Photocopiers
- Televisions
- Video recorders
- DVD players
- Monitor stands
- Medical Equipment
- Equipment not in scope of SCW SLA
- Hazard and General waste
- Confidential waste

3. Details of the policy

The NHS is obliged to abide by all relevant UK legislation.

All redundant IT equipment must be disposed of following The Waste Electronic and Electrical Equipment Directive (WEEE). Under this Directive, equipment that requires a current to operate must be recycled in accordance with the standards set out in the Directive. This includes all electronic IT equipment.

In addition, to ensure that sensitive data held on SCW managed IT equipment is securely destroyed using the correct methods, all data bearing electronic assets must be disposed of and destroyed by adhering to the best practice guidance issued by the Department of Health and NHS England (NHSE) 'Disposal and Destruction of Sensitive Data'.

Principles

Data Security and Protection Toolkit

NHSE Data Security and Protection Toolkit (DSPT) – 'formal contractual arrangements that include compliance with information governance requirements are in place with all contractors and support organisations. These contracts must be reviewed annually to support DSPT requirements.

The company that is contracted to do the disposal and destruction of SCW IT equipment must be aware of and adhere to their service obligations to protect sensitive data and to ensure the risk of loss is mitigated.

Media Destruction

Data bearing assets must not be removed from site until all data is destroyed, unless data destruction is conducted at a secure facility in accordance with this policy.

Once a specialist company or contractor has processed the media assets, there is a procedure for verification of data destruction, including ***the issuing of data destruction certificates.***

SCW will maintain a log, stored on the secured SCW network from the disposal company, for each individual media device, which will include details and methods of data destruction.

It is important to maintain an effective method of managing the process of data destruction. This ensures that all media requiring destruction is correctly organised and properly audited.

Tracking of data bearing assets serial numbers should be used as the bare minimum for individual component tracking. The log will contain a section for destruction or removal certificates; these provide evidence certifying the destruction or sanitisation of the media and the date on which the destruction occurred for audit and compliance assurance.

Hardware Disposal and Destruction Process

SCW has a rigorous process in place for the disposal of retired IT equipment that conforms to SCW principles with regards to disposal of assets.

SCW only use approved contractors who meet the standards outlined by NHSE:

- All data is destroyed in accordance with the certification data capability requirement attached to the ADISA ICT Asset Recovery Standard
- A UKAS accredited certification body have certified their processes and procedure to be compliant with the following standards:
    - ISO 9001:2015 (Quality Management System)
    - ISO 14001:2015 (Environmental Management System)
    - ISO 27001:2013/2022 (Information Security Management System)
    - ISO 45001:2018 (Occupational Health and Safety Management System)
- Premises are an Approved Authorised Treatment Facility (AATF) for processing and recycling electrical waste and they have an Environmental Permit or exemption and Waste Carriers Registration

- Able to securely sanitise data with an approved software solution independently tested to meet the Purge requirements as laid out in a recognised international standard eg IEEE2883-2022. If Purge commands are not supported by the asset the software shall fall back to Clear
- Able to shred hard drives to 10mm particle size or degauss to 10,000 Oe and subsequently shred unscreened on-site or at secure facility
- All identifiable markings are removed and destroyed
- DDaT Asset Management team will periodically audit disposal contractors to ensure processes and procedures meet their contractual obligations
- Disposal collections are arranged on demand and dependent upon operational requirements (business as usual processes, IT refresh projects and ad-hoc requests)

Once equipment has been assessed or identified for decommission and agreed with the customer and/or departmental manager, the following process with be followed:

- Desktop Support update the service request. Details of the equipment will be recorded on the support call including the client's name, department, make, model and service tag. Telephony assets will be removed from MDM enrolment
- Desktop Support collect from site and transport equipment to a nominated secure storage location
- SCW Asset Management team are responsible to coordinate disposal collections using contracted and approved IT asset disposal partners
- SCW Asset Management supervise disposal collections, provide access and monitor any work carried out by disposal contractors, ensuring the correct equipment is removed
- The disposal contractor is responsible to securely wipe data on site or transport the equipment directly to their secure premises. Equipment must be held in a secure location while waiting to be processed. Access to equipment in the processing area must be restricted to authorised staff only

- Data destruction certificates will be provided by the disposal company to SCW once all prerequisite processes are complete. These certificates are electronically stored by Asset Management and records reconciled with asset registers ensuring all disposed equipment is accounted for and asset status updated on the fixed asset register

4. Roles and responsibilities

SCW DDaT will ensure all IT equipment is disposed of in line with legislation and DH requirements.

Key Stakeholder	Responsibility
Customers	Responsible for equipment refresh cycles in accordance with own business plans for assets in their care. Responsible to provide sufficient replacement stock. Consulted/ Informed.
SCW Executive Management Team	Accountable for approval of IT Disposal Policy.
Director of DDaT Chief Digital Information Officer	Accountable for operating in accordance with policy.
DDaT Senior Leadership Team	Responsible for operating in accordance with policy. Responsible for communicating policy to staff.
Director Service Delivery	Responsible for authoring and maintenance of policy. Responsible for operational service delivery activities in accordance with this policy. Responsible for assurance, lifecycle activities.

ITAM Consultant	Responsible for operating in accordance with agreed asset management processes and other related IT processes. Responsible for assurance, lifecycle activities. Responsible for preparing business cases for investment in people resources, technical tools, and data management.
3rd Party Suppliers	Responsible for operating in accordance with policy. Responsible for compliance with linked policies, for example Asset Management Policy. Informed.
DDaT staff	Responsible for operating in accordance with policy.
Cyber Security Manager	Consulted.
Information Governance	Consulted.

5. Training

This Policy will be promoted by SCW DDaT, Digital Portfolio Managers and Cyber Security Manager; each customer's Information Governance Team will also promote the policy. Any key amendments to the policy will be notified to each organisation for communication to staff groups. Staff are also required to complete mandatory Data Security and Awareness training annually.

6. Public sector equality duty - Equality Impact Assessment

The Equality Act 2010 requires public bodies to consider the needs of all individuals in their day-to-day work. At SCW we do this by completing an Equality Impact Assessment as described in the SCW Equality and Diversity Policy.

The Equality Impact Assessment for this policy can be found in Appendix A to this document.

7. Sustainability Impact Assessment

This policy will be delivered in alignment with the SCW Sustainability strategic aim.

ITIL defines sustainability as “A business approach focused on creating long-term value for society and other stakeholders, by addressing the risks and opportunities associated with economic, environmental and social developments.”

This policy supports the strategy in a number of ways including but not limited to:

- Ensure regulatory compliance to safeguard the business from breaches and potential financial impact
- Ensure IT Assets, which are no longer in use and classed as end of life, are securely disposed, reducing physical storage requirements and reducing cost
- Work with suppliers to ensure the disposal of equipment is not only secure but completed with minimal environmental impact
- Engage disposal partners with a zero-landfill waste policy, aligning with NHSE Carbon Net-Zero strategy

8. Monitoring compliance and effectiveness

Disposal of assets will be reconciled with WEEE disposal certification, and asset repository will be updated with certificate numbers. SCW Asset Management are responsible for monitoring completeness, accuracy and timeliness of asset inventory records. Monitoring is an ongoing process; remedial actions will be taken where exceptions are identified. Any exceptions to this policy must be approved by DDaT Senior Leadership Team.

1. Core SLA IT Asset Reports are provided quarterly (Hardware and Software) to customers, either electronically or automated.
2. Asset Disposal information is retained throughout the core reporting cycle in each financial year (Q1 – Q4).
3. Proactive audits are conducted by Configuration Management Team.
4. Exception reports shared with Hardware Asset Manager for reconciliation.

9. Review

The policy will be reviewed every two years by DDaT Senior Leadership Team unless changes are required outside of this review cycle.

10. References and associated documents

- NHSE 'Disposal and Destruction of Sensitive Data'
- DDaT Asset Management Policy
- DDaT Asset Management Process
- Remote working & Portable Device Policy
- Acceptable Use Policy
- DDaT Asset Management Standard Operating Procedure (SOP)
- Lost/stolen device process.

Appendix A – Equality Impact Assessment

DDaT IT Disposal Policy

1 What is it about?
a) **Describe the proposal/policy and the outcomes/benefits you are hoping to achieve** To provide a framework of guidance to NHS South, Central and West CSU (SCW) staff (as defined in the scope) regarding the security of IT assets and sensitive data.
b) Who is it for? All staff
c) How will the proposal/policy meet the equality duties? The policy will have no adverse effect on equality duties as it considers the confidentiality of information to be of equal status across all groups of people.
d) What are the barriers to meeting this potential? There are no barriers.
2 Who is using it?
a) Describe the current/proposed beneficiaries and include an equality profile if possible The policy is applicable to all.
b) How have you/can you involve your patients/service users in developing the proposal/policy? Patients and service users have not been involved in developing the policy as this is an operational policy.
c) Who is missing? Do you need to fill any gaps in your data? There are no gaps.
3 Impact Using the information from steps 1 & 2 above:
a) Does (or could) the proposal/policy create an adverse impact for some groups or individuals? Is it clear what this is? It is not anticipated that any adverse impact will be created.
b) What can be done to change this impact? If it can't be changed, how can this impact be mitigated or justified? This is not applicable.

c) Does (or could) the proposal/policy create a benefit for a particular group? Is it clear what this is? Can you maximise the benefits for other disadvantaged groups? This policy is equal across all groups.
d) Is further consultation needed? How will the assumptions made in this analysis be tested? No.
4 So what (outcome of this EIA)? ***Link to the business planning process***
a) What changes have you made in the course of this EIA? None.
b) What will you do now and what will be included in future planning? Not applicable.
c) When will this EIA be reviewed? At policy review.
d) How will success be measured? No equality issues are created.

Sign-off

Name of person leading this EIA: [redacted]	Date completed: 31st May 2023 Proposed EIA review date: July 2025
Signature of director/decision-maker [redacted], CDIO Name of director/decision-maker [redacted], CDIO	Date signed