NHS
West Hampshire
Clinical Commissioning Group

IT DISPOSAL POLICY

Version 3.2

Subject and version number of document:	IT Disposal Policy Version 3.2
Serial number:	COR/047/V3.02
Operative date:	1 October 2019
Author:	SCW CSU Cyber Security Manager
CCG owner:	Senior Information Risk Owner
Links to other policies:	
Review date:	September 2021
For action by:	All Staff
Policy statement:	This policy provides the framework for SCW IT Equipment Disposal, which must be followed by all SCW staff and external suppliers when managing assets on behalf of customers.
Responsibility for dissemination to new staff:	Line managers at induction.
Mechanisms for dissemination:	All new and revised policies are promoted through the staff newsletter and published on the CCG websitet.
Training implications:	All staff should be made aware of where to find CCG policies at induction.
Resource implications	There are no resource implications in relation to this policy.
Further details and additional copies available from:	Website: https://westhampshireccg.nhs.uk/document-tag/ig-and-security-policies/
Equality analysis completed?	CSU equality impact assessment (EIA) framework used to evaluate the policy. EIA template appended to policy.
Consultation process	CSU IT Senior Leadership Team CSU Corporate Governance Assurance Group (CGAG) CCG Policy Sub Group
Approved by:	Policy Sub Group
Date approved:	11 September 2019

Website Upload:

Website	Location in FOI Publication Scheme	https://westhampshireccg.nhs.uk/document-tag/ig-and-security-policies/
Keywords:	*Insert helpful keywords (metadata) that will be used to search for this document on the intranet and website*	

Amendments Summary:

Amend No	Issued	Page(s)	Subject	Action Date
1	Jan 18	Cover	Review date extended to 25 May 2018 when GDPR becomes effective	Jan 18
2	Aug 18	Throughout	Amended throughout to reflect changes in terminology re GDPR. Addition of paragraphs 5, 7 and 9.	Aug 18
3	Aug 19	Pg 8	Additional policy statements. Amend regular review from annual to biennial	Aug 19
4				
5				

Review Log:

Include details of when the document was last reviewed:

Version Number	Review Date	Name of Reviewer	Ratification Process	Notes
1.1	Sept 16	CSU IT	As detailed above	No amendments to content
2	Aug 18	Throughout	CSU IT Senior Leadership Team, CSU CGAG, CCG Policy Sub Group	See amend 2 above.
3.02	Sept 19	CSU Cyber Security Manager	As above. Version control brought in line with CSU policy.	See amend 3 above

IT DISPOSAL POLICY

As the South, Central & West Commissioning Support Unit (CSU) provides IT networks, equipment and support to West Hampshire CCG, all CCG employees are required to adhere to the CSU IT Services core information security policies, in addition to those of the CCG.

The following policy was developed by the CSU IT Services Team and was adopted for use by the CCG. This has been identified as an IT Core Policy and as such cannot be amended by the CCG.

SUMMARY OF KEY POINTS TO NOTE

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

- The CSU has responsibility to dispose of all redundant equipment and hardware relating to the CSU and its customer organisations (eg CCGs) in accordance with legislation and Department of Health requirements.
- The loss of any sensitive data may result in legal and financial sanctions being imposed on the organisation, its directors and it staff – employees can be personally liable for this loss.
- Users must ensure they log a call via the IT service desk for the disposal of any equipment capable of storing sensitive data and must provide details of the type of media, volume, physical location and local contact name: this includes encrypted memory sticks. The CSU IT team will then action as appropriate.
- The following are not collected or processed by the CSU: photocopiers, televisions, video recorders, DVD players, monitor stands, medical equipment, equipment belonging to the CCG or hazard and general waste.

OFFICIAL

IT Disposal Policy

Version 3.2

South, Central and West Commissioning Support Unit

August 2019

DOCUMENT CONTROL

Document Name	Version	Status	Author
Document Name	*3.2*	*Final*	*Head of Service Development and Support*
Document objectives:	This document defines the Policy for Service Equipment Disposal.		
Target audience:	The Policy provides the framework for the SCW IT Equipment Disposal; which must be followed by all SCW staff and external suppliers when managing assets on behalf of customers.		
Committee/Group Consulted*:*	SCW IT Services Senior Leadership Team		
Monitoring arrangements and indicators:	The effectiveness of the Policy in meeting its aims and objectives will be kept under review and reports submitted as required to the SCW IT Services Senior Leadership Team.		
Training/resource implications:	Training in, and assistance in adhering to, the Policy will be provided by SCW Asset Management Team.		
Approved and ratified by:	*Information Governance Steering Group* *Corporate Governance and Assurance Group*	*Date: 19/08/2019*	
Equality Impact Assessment:	Yes	23 July 2018	
Date issued:	*19/08/2019*		
Review date:	July 2021		
Author:	*Head of Service Development and Support*		
Lead Director:	IT Services Director		

Version Control

Change Record

Date	Author	Version	Page	Reason for Change
29/11/2016	Arif Gulzar	2.0		Version reset after ratification from Corporate Governance Assurance Group
14/12/2017	Arif Gulzar	2.1		Extended policy review date to align with GDPR after approval from SCW Information Governance Steering Group
23/07/2018	Cathy Jukes	2.2		Review and approval by IT SLT
24/07/2018	Stephanie Wilson	3.0		Version changed after CGAG ratification
21/06/2019	Arif Gulzar	3.1	All	Policy reviewed and signed off by IT senior leadership team
12/07/2019	Arif Gulzar	3.2		As part of IG steering group sign off feedback, Added Policy statements to section 4 for clarity - Hardware and Destruction Process.
19/08/2019	Arif Gulzar	3.2	All	Policy ratified by SCW Corporate Governance & Assurance Group (CGAG)

Reviewers/contributors

Name	Position	Version Reviewed & Date
Simon Sturgeon	Director of IT Services	V3.1 21/06/2019
Andy Ferrari	Associate Director of IT Strategy and Planning	V3.1 21/06/2019
Cathy Jukes	Associate Director of IT Projects and Programmes	V3.1 21/06/2019
Michael Knight	Associate Director of Technology Management and Architecture	V3.1 21/06/2019
David Walch	Head of IT Service Delivery	V3.1 21/06/2019
Stephanie Wilson	Head of Service Development and Support	V3.1 21/06/2019

Version Number: 3.2	Issue/approval date: 19/08/2019
Status: Final	Next review date: July 2021

CONTENTS

1. INTRODUCTION

Information, and in particular Sensitive Data disclosure has become a major risk to organisations working with sensitive data, 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 has to be maintained at all times from the creation of a record or document, its use, its storage, retention, disposal and finally destruction. This policy supports the implementation of 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.

2. SCOPE AND DEFINITIONS

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

SCW has the responsibility to dispose of all redundant equipment, and hardware relating to SCW and its customer organisations. The objective of this policy is to ensure that the proper guidance is followed for IT hardware disposal, especially in relation to the destruction of Sensitive Data which the equipment and hardware may have processed and may still contain or have stored.

The objective of this policy is to limit any risk to SCW and customers. The loss of any sensitive data whilst it is in the care of the Organisation may impose legal and financial sanctions on the Organisation, its Directors and its staff. Employees can be personally liable for this loss.
This policy will focus on the disposal and destruction of SCW hardware including both desktop and other user devices and key infrastructure equipment, for example, servers, back-up tapes and devices, firewalls, switches and data storage devices.

The following are neither collected nor processed by SCW:

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

3. DETAILS OF THE POLICY

The NHS is obliged to abide by all relevant UK and European Union legislation. All redundant equipment must be disposed of following The Waste Electronic and Electrical Equipment Directive (WEEE). Under this Directive equipment that requires a current to flow though it 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 hardware is destroyed using the correct methods, all data bearing electronic hardware must be disposed of and destroyed by adhering to the best practice guidance issued by the Department of Health, NHS Digital (NHSD) 'Disposal and Destruction of Sensitive Data'

4. PRINCIPLES

Data Security and Protection Toolkit

NHSD Data Security and Protection Toolkit – formal contractual arrangements that include compliance with information governance requirements are in place with all contractors and support organisations.
The company that is contracted to do the disposal and destruction of SCW hardware must be aware of and adhere to their obligations to protect sensitive data and to ensure the risk of loss is minimised.

Media Destruction

Under no circumstances will sensitive data bearing assets be removed from site until all data is destroyed on-site in accordance with this policy.

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

SCW will maintain a log, on the secured SCW network (including details of the certificates of verification) from the disposal company, for each individual media device

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 hard disk serial numbers should be used as a bare minimum for individual component tracking. The log will contain a section for destruction or removal certificates; these provide evidence guaranteeing the destruction or sanitisation of the media and the date on which the destruction occurred.

Hardware Disposal and Destruction Process

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

SCW will only use an approved contractor that meets the standards outlined by their IG team:

- All data is destroyed to the standards set by NHSD (InfoSec HM5). No equipment will be resold or reused
- The British Standards Institute (BSI) have certified their processes and procedure to be compliant with the following standards:
    - ISO 9001:2000 (Quality Management System)
    - ISO 14001:2004 (Environmental Management System)
    - ISO 27001:2013 (Information Security Management System)
- The premises are an Approved Authorised Treatment Facility (AATF) for processing and recycling electrical waste and they have an Environmental Permit and Waste Carriers License
- Able to crush hard drives on-site, as well as shred to 4mm particles on-site. All asset tagging will be removed and destroyed.
- Annually, SCW IT services asset management team make arrangements with disposal contractor to review their processes, policies during site visits to ensure they are adhering to their contractual obligations and standards.
- Disposal collections are arranged on demand and dependent upon operational requirements (business as usual processes, IT refresh projects and ad-hoc requests.

Once a call has been logged with SCW or 3rd Party Service Desk equipment will be assessed to determine whether it should be decommissioned and is no longer fit for purpose or beyond economic repair. This will be following discussions with the customer and/or departmental manager. At this point the following process with be followed:

- The Desktop Technician will update the support call logged by the client via the Service Desk. Details of the equipment will be recorded on the support call including the client name, department, make and model, service tag and reason for the equipment being disposed

- The Desktop Technician will remove the Hard Disk / Storage Media and transport to a secure temporary storage location. The media will be degaussed on arrival to mitigate against the risk of theft / removal of sensitive data from the store

- The chassis and other IT equipment that does not hold and data such as monitors, printers & keyboards etc. will be transported to secure storage

- During the collection, SCW will supervise the work carried out by the disposal company contractors making sure the correct equipment is removed and providing them access to the SCW secure temporary storage location

- The disposal company will transport the equipment directly to their premises on a secure vehicle. It will be held in a secure location while it is waiting to be processed. Access to the equipment in the process area will be restricted to authorised staff only

- The disposal company will process the equipment. Hard drives will be shredded to 4mm

- Documentation will be provided by the disposal company to SCW once they have completed the process and stored by the Asset Management Team. The certificate will be reconciled with the internal list to ensure that all kit is accounted for.

5. ROLES AND RESPONSIBILITIES

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

Users must ensure that they log a call, via the Service Desk, for the disposal of any equipment capable of storing sensitive data.

6. TRAINING

This Policy will be promoted by SCW IT Services, the Training Team and Information Security manager; each customer organisation'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 IG training annually.

7. MONITORING COMPLIANCE AND EFFECTIVENESS

Disposal of assets will be reconciled with WEEE disposal certificate numbers, the Asset Repository will be updated with certificate numbers. SCW Asset Management team and 3rd party IT providers are responsible for monitoring completeness, accuracy and timeliness of asset inventory records. Monitoring is

an ongoing process. Remedial action will be taken where exceptions are identified.

8. REVIEW

The IT Senior Leadership Team (SLT) will ensure that any updates or new legislation will be reflected in this policy and disseminated throughout the Organisation if changes are made prior to the next revision of the policy, due 12 months from approval.

9. REFERENCES AND ASSOCIATED DOCUMENTS

NHSD 'Disposal and Destruction of Sensitive Data'

APPENDIX A - EQUALITY IMPACT ASSESSMENT

For IT Disposal Policy

1. Title of policy/ programme/ framework being analysed IT Disposal Policy.
2. Please state the aims and objectives of this work and the intended equality outcomes. How is this proposal linked to the organisation's business plan and strategic equality objectives? The IT Disposal Policy provides the framework for the SCW IT Equipment Disposal, which must be followed by all SCW staff and external suppliers when managing assets on behalf of customers.
3. Who is likely to be affected? e.g. staff (as defined in the scope), patients, service users, carers Staff.
4. What evidence do you have of the potential impact (positive and negative)? None expected.
4.1 Disability (Consider attitudinal, physical and social barriers) No impact
4.2 Sex (Impact on men and women, potential link to carers below) No impact
4.3 Race (Consider different ethnic groups, nationalities, Roma Gypsies, Irish Travellers, language barriers, cultural differences). No impact
4.4 Age (Consider across age ranges, on old and younger people. This can include safeguarding, consent and child welfare). No impact
4.5 Gender reassignment (Consider impact on transgender and transsexual people. This can include issues such as privacy of data and harassment) No impact
4.6 Sexual orientation (This will include lesbian, gay and bi-sexual people as well as heterosexual people). No impact
4.7 Religion or belief (Consider impact on people with different religions, beliefs or no belief) No impact

4.8 Marriage and Civil Partnership No impact
4.9 Pregnancy and maternity (This can include impact on working arrangements, part-time working, infant caring responsibilities). No impact
4.10 Carers (This can include impact on part-time working, shift-patterns, general caring responsibilities, access to health services, 'by association' protection under equality legislation). No impact
4.11 Additional significant evidence (See Guidance Note) Give details of any evidence on other groups experiencing disadvantage and barriers to access due to: • socio-economic status • location (e.g. living in areas of multiple deprivation) • resident status (migrants) • multiple discrimination • homelessness No impact
5. Action planning for improvement (See Guidance Note) Please give an outline of the key action points based on any gaps, challenges and opportunities you have identified. An Action Plan template is appended for specific action planning.
Sign off
Name and signature of person who carried out this analysis Beverly Carter Head of IG, NHS South, Central and West Commissioning Support Unit
Date analysis completed 23 July 2018
Name and signature of responsible Director Simon Sturgeon, IT Services Director

Date analysis was approved by responsible Director 23 July 2018

End of Policy Document