`

NHS
North Hampshire
Clinical Commissioning Group

NHS South, Central and West Commissioning Support Unit

Service Equipment Disposal Policy

As the South, Central & West Commissioning Support Unit (SCW) provides IT networks, equipment and support to North Hampshire CCG, all CCG employees are required to adhere to the CSU IT Services information security policies. The following policy was developed by the CSU IT Services Team and adopted for use by the CCG.

This document can be made available in a range of languages and formats on request to the policy author.

Version:	2.1
Ratified by:	SCW CSU Corporate Governance Assurance Group
Date ratified:	29/11/2016
Name of Responsible Officer/author:	Stephanie Wilson – Head of Service Development and Support
Name of responsible committee/individual:	IT Services Leadership Team
Name of executive lead:	Suzanne Tewkesbury – Director of Corporate Development & Performance
Date issued:	09/01/2018
Review date:	25/05/2018
Target audience:	All NHS South, Central & West CSU staff and customers

Document Control Sheet

Title	**Service Equipment Disposal Policy**
CCG	All
Version	2.1
Status	Approved – Final
Author	David Walch
Date Created	19/12/2015
Date Last Updated	14/12/2017

History			
Version	Date	Author(s)	Comments
1.0	19/12/2015	David Walch	Version reset & re-write specifically for SCW CSU
1.1	08/09/2016	Arif Gulzar	Updated policy review date
1.2a	22/09/2016	Arif Gulzar	Updated as per approval feedback from IT SLT
1.2b	04/10/2016	Arif Gulzar	Policy signed off by Information Governance Steering Group
2.0	29/11/2016	Arif Gulzar	Version reset after ratification from Corporate Governance Assurance Group
2.1	14/12/2017	Arif Gulzar	Extended policy review date to align with GDPR after approval from SCW Information Governance Steering Group

Approval/Sign Off	
Name	Title and contact
Philip Evans	Associate Director of IT Services
Catherine Dampney	CIO

Contents

1. Purpose

Information, and in particular Personal Confidential Data Data (PCD), 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 PCD, confidential or sensitive information are disposed of in line with national requirements to prevent unauthorised disclosure.

2. Introduction

All NHS South, Central and West Commissioning Support Unit (CSU) 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 the Data Protection Act, 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.

3. Scope of this Policy

a. Scope

This policy applies to all staff in NHS South, Central and West CSU its customers and all contractors working for them.
This policy will focus on the disposal and destruction of all NHS South, Central and West CSU hardware. The Organisation’s disposal of confidential waste procedures also provide the guiding principles to adhere to when disposing of or destroying other types of confidential or sensitive information assets.

b. Policy Aim

NHS South, Central and West CSU has the responsibility to dispose of all redundant equipment, and hardware relating to the CSU 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 Personal Confidential Data (PCD), confidential or sensitive information which the equipment and hardware may have processed and may still contain or have stored.

c. Objectives

The objective of this policy is to limit any risk to NHS South, Central and West CSU and it's customers. The loss of any Personal Confidential Data (PCD), confidential or sensitive information 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 NHS South, Central and West CSU hardware including both desktop and other user devices and key infrastructure equipment, e.g. servers, back-up tapes and devices, firewalls, switches and data storage devices.

4. Responsibilities

a. NHS South, Central and West CSU ICT Service

NHS South, Central and West CSU ICT Service will ensure that equipment is disposed of in line with legislation and DH requirements.

b. Users

Users must ensure that they log a call, via the Service Desk, for the disposal of any equipment capable of storing Personal Confidential Data (PCD), confidential or sensitive information.

5. Legislation

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 anything that requires a current to flow though it to operate has to be recycled in accordance with the standards set out in the Directive. This includes all electronic IT equipment.
In addition to ensure that Personal Confidential Data (PCD), confidential or sensitive information held on NHS South, Central and West CSU hardware is destroyed using the correct methods, all electronic hardware must be disposed of and destroyed by adhering to the best practice guidance issued by the Department of Health, HSCIC 'Disposal and Destruction of Sensitive Data':
http://systems.hscic.gov.uk/infogov/security/infrasec/gpg/dadosdv2.pdf

6. Policy Principles

a. IG Toolkit

HSCIC IG Toolkit requirement: 110 – '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 NHS South, Central and West CSU hardware must be aware of and adhere to their obligations to protect Personal Confidential Data (PCD), confidential or sensitive information and to ensure the risk of loss is minimised.
The company must meet NHS South, Central and West CSU's IG Toolkit requirements.

b. Media Destruction

Once a specialist company or contractor has processed the media, there is a procedure for verification of data destruction, including ***the issuing of certificates*.**
NHS South, Central and West CSU will maintain a log, on the secured NHS South, Central and West CSU 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.

c. Hardware Disposal and Destruction Procedures

NHS South, Central and West CSU has a rigorous process in place for the condemnation and disposal of unserviceable IT equipment that conforms to the CSU's principles with regards to disposal of assets.

NHS South, Central and West CSU will only use an approved contractor that meets the standards outlined by the CSU's IG team:

- All data is destroyed to the standards set by the UK Government's Security Equipment Assessment Panel (SEAP). 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, the NHS South, Central and West CSU ICT Service will make arrangements with the disposal company to visit the site and collect equipment waiting to be disposed of. A list of the equipment to be collected will be issued to the disposal company before their visit. This list will be produced from the 'Condemnation' spread sheet by location.

Once a call has been logged with the CSU Service Desk, NHS South, Central and West CSU will assess whether or not the IT equipment has become redundant 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 PC Support 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 to be disposal of.

- The PC Support 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 ICT equipment that does not hold and data such as monitors, printers & keyboards etc. will be transported to the Loc'n'Store facility in Millbrook and stored neatly in the collection boxes.

- During the collection, NHS South, Central and West CSU will supervise the work carried out by the disposal company contractors making sure the correct equipment is removed and providing them access to the NHS South, Central and West CSU 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 6mm.

- Documentation will be provided by the disposal company to NHS South, Central and West CSU once they have completed the process and stored by the Business Management Team. The certificate will be reconciled with the internal list to ensure that all kit is accounted for.

- The following are not collected nor processed by NHS South, Central and West CSU:

    - Photocopiers
    - Televisions
    - Video recorders
    - DVD players
    - Monitor stands
    - Medical Equipment
    - Equipment belonging to the client
    - Hazard and General waste

Any media (e.g. memory sticks, CDs or floppy discs) that holds Personal Confidential Data (PCD), confidential or sensitive information will be dealt using in the following process;

- The owner of the media will raise a support call with the Service Desk giving details of the type of media, volume, physical location and local contact name.

- NHS South, Central and West CSU will contact the Organisation approved disposal company to obtain a cost to collect and dispose of the media requested by the client. The quotation will be based on the information provided on the support call. A full audit trail and certificate of destruction would be given as part of the service.

- NHS South, Central and West CSU would make the necessary arrangements with the disposal company to action the destruction of the media on a quarterly basis or as required in a period of significant infrastructure refresh.. The disposal company will request a signature from the client upon collection of the media. Details of what has been collected will also be recorded on the form.

- The disposal company will transport the media 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 media will be restricted to authorised staff only.

- Payment will only be authorised by NHS South, Central and West CSU when a certificate of destruction has been received from the disposal company detailing all hardware destroyed and after reconciling with the internal list to validate that all equipment is accounted for.

7. Training and awareness

This Policy will be promoted by NHS South, Central and West CSU including the training department 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.

8. Policy Review

The Information Security Manager 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 in 12 months from approval.