NHS
Pennine Care
NHS Foundation Trust

DOCUMENT CONTROL	
Title:	**Permitted Use of Removable Media**
Version:	**4**
Reference Number:	**HI001**
Scope:	
This policy applies to all staff and contractors both internal and external around all removable media for use on information systems owned or operated by Pennine Care NHS Foundation Trust. This includes but is not limited to: tapes, floppy discs, removable or external hard disc drives, optical disc DVD or CD ROM's, solid state memory devices including memory cards, mobile phones and SIM Cards, USB Pen drives.	
Purpose:	
The purpose of this document is to describe procedures to prevent unauthorised disclosure, modification, removal or destruction of Trust information assets, which may cause disruption to Trust's business activities.	
Keywords:	
Removable Media, DVD, USB, CD, Memory	
Supersedes:	
Version 3 – This policy was previous a Corporate Policy CO50 – Agreed to move all IT policies under Health Informatics (HI)	
Description of Amendment(s):	
• Service desk telephone number updated • Updated job title section 3 paragraph 4 and 5 • Section 4 penultimate bullet updated to reflect revised reporting arrangement	
Owner:	
Head of ICT Service Delivery, Rob Brocklehurst	
Individual(s) & group(s) involved in the Development:	
This document has been developed in collaboration with the following interested parties: • Rob Brocklehurst • Chris Reynolds • Health Informatics Steering Group	

Individual(s) & group(s) involved in the Consultation:	
The document has been circulated for consultation and comments have been taken into consideration and the document amended accordingly: • Health Informatics Steering Group – 12th April 2018	
Equality Impact Analysis:	
Date approved: **Reference:**	22nd of May 2018 HI-EIA001
Freedom of Information Exemption Assessment:	
Date approved: **Reference:**	22nd of May 2018 2018/0645
Information Governance Assessment:	
Date approved: **Reference:**	2nd of May 2018
Policy Panel:	
Date Presented to Panel: **Presented by:** **Date Approved by Panel:**	3rd of May 2018 Chris Reynolds 18th of May 2018
Policy Management Team tasks:	
Date Executive Directors informed: **Date uploaded to Trust's intranet:** **Date uploaded to Trust's internet site:**	22nd of May 2018 24th of May 2018 24th of May 2018
Review:	
Next review date: **Responsibility of:**	May 2021 Head of ICT Service Delivery
Other Trust documentation to which this guideline relates (and when appropriate should be read in conjunction with):	
Policy Associated Documents	
TAD_HI001_01	Service Request to Use Writable Media
Other external documentation/resources to which this guideline relates:	
CO051	Electronic Transfer of Person Identifiable Data Policy V5
CO052	Disposal and Destruction of Removable Media V5

CQC Regulations **This guideline supports the following CQC regulations:**	

Contents Page

1. INTRODUCTION

All removable media for use on information systems owned or operated by Pennine Care NHS Foundation Trust are covered by this policy.

Removable media includes but is not limited to: Tapes, floppy discs, removable or external hard disc drives, optical disc DVD or CD ROMs solid state memory devices including memory cards, mobile phones and SIM cards, USB Pen drives.

2. PURPOSE

This policy sets out procedures to prevent unauthorised disclosure, modification, removal or destruction of Trust information assets, which may cause disruption to Trust's business activities.

3. RESPONSIBILITIES, ACCOUNTABILITIES & DUTIES

Line Managers

- Line managers in collaboration with the Health Informatics Service Delivery team are responsible for day to day management and oversight of removable media used within their work areas to ensure this policy is followed.
- Line managers are responsible for the secure storage of all unallocated removable media and its related control documentation as required by this policy. Trust approved pen drives should not be shared. Individuals issued the device will be held responsible for its security and integrity.
- Notification in change of device ownership should be sent to the ICT Service Desk to ensure the device is asset tracked to the correct individual. This should be completed by the individual and / or the individuals Line manager.

All Staff

- Staff and contractors are not permitted to save any information to any removable media other than provided or explicitly approved for use by the Trust.
- Transfer of confidential or sensitive data must be undertaken under the terms of the Trust's Electronic Transfer of Person Identifiable Data (Policy CO051)
- The Health Informatics Service Delivery Team is responsible for identifying and implementing any device configuration requirements that the Trust may require in order to comply with NHS Information Governance security policy and standards. This includes data encryption capabilities.
- Staff who have been authorised to use removable media for the purposes of their job roles are responsible for the secure use of those removable media as required by this policy. Failure to comply with this Removable Media Policy may endanger the information services of the Trust and may result in disciplinary or criminal action
- Staff involved in data extraction and data file creation must have completed the required Information Governance Training.

External Partners and Contractors

- Introducing removable media to the Trust network must ensure that a virus check is completed before any removable media is read.

4. SECURITY PROCEDURES

- The Trust deploys end point security on its network with USB ports and writable CD and DVD drives disabled by default.
- Before information can be transferred to removable media, authorisation must be obtained by completing the “Request to use removable media” form (TAD_HI001_01). The form must be completed, signed by a line manager and returned to the IT department for approval.
- Anyone requesting to transfer sensitive or person identifiable data on removable media must be authorised to do so in line with the Trust’s Electronic Transfer of Person Identifiable Data Policy – CO51. Procedures for authorisation are set out in that policy.
- A list of removable media that have been approved for use within the Trust can be found on the IT pages of the intranet or by contacting the IT Service Desk on 0161 716 1234.
- Removable media may only be used to store and share NHS information that is required for a specific business purpose. When the business purpose has been satisfied, the contents of removable media must be removed immediately.
- Redundant removable media must be returned to the Trust’s IT Department for disposal in line with the Trust’s Disposal and Destruction of Removable Media Policy – CO052.
- Removable media should not be taken or sent outside the Trust unless a prior written agreement or instruction exists. A record must be maintained of all removable media taken or sent outside the Trust, or brought into or received by the Trust. This record should also identify the data files involved. The Trust security software will audit filenames that are copied onto removable media, therefore only the information for which authorisation has been received should be transferred. Should there be any changes to the type of information / data being transferred, a further request to sue writable media form must be completed and submitted (TAD_HI001_01).
- Removable media containing sensitive or person identifiable data should only be taken or sent off site in accordance with the Trust’s Electronic Transfer of Person Identifiable Data Policy – CO051.
- Removable media must be physically protected against loss, damage, abuse or misuse when used, stored or in transit.
- Under no circumstances must passwords be kept with Trust approved devices; any such incidents will be fully investigated and may result in disciplinary action being taken.
- No staff other than Trust IT personnel should try to change or modify any security settings on the approved devices; any such incidents will be fully investigated and may result in disciplinary action being taken.
- Staff should not try to bypass the formal route to gain authorisation to use removable media.
- Data archives or backups taken and stored on removable media, either short term or long term, must take account of any manufacturers specification or guarantee and any limitations therein.
- A minimum of two audits will be carried out within any year to ensure adherence to this Policy. Details of these checks will be recorded on the IT Service Desk. The audits will be undertaken by the Information Governance Manager or nominated representative.

The results of the audits will be reported to the Information Governance Steering Group.

- All incidents involving the use or loss of removable media must be reported to the Trust Information Governance Manager and the IT Service desk immediately and an incident form completed. Any such incidents will be fully investigated and may result in disciplinary action being taken.
- The ICT department reserves the right to remove a device or remove access to a device if usage of the device is deemed inappropriate. Details will then be sent to the individuals Line Manager.

5. EQUALITY IMPACT ANALYSIS

As part of its development, this document was analysed to consider / challenge and address any detrimental impact the policy may have on individuals and or groups protected by the Equality Act 2010. This analysis has been undertaken and recorded using the Trust's analysis tool, and appropriate measures will be taken to remove barriers and advance equality of opportunity in the delivery of this policy / procedure

6. FREEDOM OF INFORMATION EXEMPTION ASSESSMENT

Under the Freedom of Information Act (2000) we are obliged to publish our policies on the Trust's website, unless an exemption from disclosure applies. As part of its development, this policy was assessed to establish if it was suitable for publication under this legislation. The assessment aims to establish if disclosure of the policy could cause prejudice or harm to the Trust, or its staff, patients, or partners. This assessment has been undertaken using the Trust's Freedom of Information Exemption Guide, and will be reviewed upon each policy review.

7. INFORMATION GOVERNANCE ASSESSMENT

This Policy has been analysed to ensure it is compliant with relevant information law and standards as in place at the time of approval, and are consistent with the Trust's interpretation and implementation of information governance components such as data protection, confidentiality, consent, information risk, and records management.

Compliance will be reviewed against any changes to legislation / standards or at the next review of this document.

8. SAFEGUARDING

All staff have a responsibility to promote the welfare of any child, young person or vulnerable adult they come into come into contact with and in cases where there are safeguarding concerns, to act upon them and protect the individual from harm.

All staff should refer any safeguarding issues to their manager and escalate accordingly in line with the Trust Safeguarding Families Policy and Local Safeguarding Children/Adult Board processes.

9. MONITORING

The effective application of this policy / guideline, including adherence to any standards identified within will be subject to monitoring using an appropriate methodology and design, such as clinical audit.

Monitoring will take place on a biannual basis and will be reportable to the Quality Group via the Clinical Effectiveness and Quality Improvement Team.

10. REVIEW

This policy / guideline will be reviewed three-yearly unless there is a need to do so prior to this; e.g. change in national guidance.