Pennine Care NHS
NHS Foundation Trust

Policy Document Control Page

Title

Title ***Policy for the Permitted use of removable media - harmonised***

Version: 4

Reference Number: CO50

Supersedes

Supersedes: 3

Description of Amendment(s):

- **No changes made**

Originator

Originated By: Jiten Patel

Designation: Head of ICT Service Delivery

Equality Impact Assessment (EIA) Process

Equality Relevance Assessment Undertaken by: Barbara Hoyle

ERA undertaken on: 20th April 2009

ERA approved by EIA Work group on: 4th June 2009

Where policy deemed relevant to equality-

EIA undertaken by

EIA undertaken on

EIA approved by EIA work group on

Integrated Governance Group **Referred for approval by: Barbara Hoyle** **Date of Referral: 24th June 2013** **Approved by: Information Governance Steering Group** **Approval Date: 26th July 2013** **Executive Director Lead: Director of Planning Performance & Information**
Circulation **Issue Date: 02 October 2013** **Circulated by: Performance and Information** **Issued to: An e-copy of this policy is sent to all wards and departments**
Review **Review Date: July 2016** **Responsibility of: Head of ICT Service Delivery**
An e-copy of this policy is sent to all wards and departments (Trust Policy Pack Holders) who are responsible for updating their policy packs as required. **This policy is to be disseminated to all relevant staff.** **Date Posted: 02 October 2013**

1. Introduction

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.

2. Scope

All removable media for use on information systems owned or operated by Pennine Care NHS FoundationTrust 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 phone simm cards, USB pen drives.

3. Responsibilities

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.

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.

Transfer of confidential or sensitive data must be undertaken under the terms of the Trust's Electronic Transfer of Person Identifiable Data. Policy CO51.

The Technical Support Manager 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.

Line managers, in collaboration with the Technical Support Manager are responsible for the 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.

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 receive appropriate Information Governance training.

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 at Appendix 1. The form must be completed, signed by a line manager, and returned to the IT Department for approval.

- Anyone requiring 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 – CO52.

- Removable media should not be taken or sent outside the Trust unless a prior 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 use writable media form must be completed and submitted. (Appendix 2.)

- 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 – CO51.

- 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 back ups taken and stored on removable media, either short term or long term, must take account of any manufacturer's 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.