Cambridgeshire and Peterborough
Clinical Commissioning Group

Cambridgeshire and Peterborough Clinical Commissioning Group (CCG)

REMOVABLE MEDIA POLICY 2017 - 2019

Approval Process

Lead Author(s):	Information Governance Manager Senior ICT Service Development Manager
Reviewed / Developed by:	Information Governance (IG), Business Intelligence (BI) and IM&T Steering Group members
Approved by:	IG, BI and IM&T Group
Ratified by:	Clinical Executive Committee
Date ratified:	April 2017
Version:	3.0
Review date:	April 2019
Valid on:	April 2017

Document Control Sheet

Development and Consultation:	Policy developed in consultation with the Information Governance, Business Intelligence and IM&T Steering Group.
Dissemination	This policy will be promoted within the CCG and uploaded to the website
Implementation	The Senior Information Risk Owner is responsible for monitoring the application of the policy by ensuring that:- • The policy is brought to the attention of all employees and building users • Assistant Directors and Line Managers are aware of their responsibilities for ensuring that staff under their control implement the policy • Staff are informed and consulted as appropriate • Any appropriate training and guidance is provided to staff • Corporate business processes support the implementation of the policy.
Training	Training will be undertaken if required as part of the CCG's ongoing processes.
Audit	Implementation of the Policy will be monitored in line with the data security assurance section of the Information Governance Toolkit.
Review	This policy will be reviewed bi-annually or earlier if there are changes in procedures or legislation.
Care Quality Commission	This policy supports the CCG in its compliance with the Care Quality Commission Registration Requirements.
Links with other Policy and Guidance	The Policy should be read in conjunction with: • Information Security for Staff Policy • Information Governance Policy • Disciplinary Policy and Procedure
Equality and Diversity	The Governance team have carried out a Rapid Equality & Diversity Impact assessment and concluded the policy is compliant with the CCG Equality and Diversity Policy. No negative impacts were found.

Revisions

Version	Page/ Para No	Description of change	Date approved
V1		Adaptation from NHS Cambridgeshire policy into CCG Policy	April 2013
V 1.1	Links with other Policy and Guidance	Updated list of policies	Nov 2013
V2.0		Reviewed and ratified by CMET	July 2015
V3	Whole document review	Bi-annual review and update	April 2017

CONTENTS

1. Introduction

1.1. All staff working in the NHS have a personal responsibility to keep person identifiable information and business sensitive information secure and confidential.

1.2. Recent security incidents have highlighted several important issues to bear in mind when transferring such information, particularly in electronic format (ie email; CD; DVD; USB memory sticks) for example:

- Does the recipient have the right to access the information?
- Does the recipient need to see all the information - can it be anonymised?
- Is the recipient clearly identified and do they know that the information is being transferred to them?
- Is the information secure or securely packaged when in transit?
- Are arrangements in place for a confirmation of receipt to be sent?

1.3. This policy aims to prevent unauthorised disclosure, modification, removal or destruction of CCG information assets, and disruption to business activities.

1.4. Under the powers granted to the Information Commissioners Office since April 2010 a financial penalty of up to £500,000 can be raised against an individual or organisation that does not comply with information security requirements and loses personal identifiable data.

1.5. This policy should be adhered to for all types of data used on removable media regardless whether or not the data is Person Identifiable. This ensures that if the removable media is lost or stolen no information governance or security breaches could occur.

2. Scope

2.1. Removable media refers to computer storage devices that are not fixed inside a computer and includes:

- Tapes
- Removable or external hard disk drives
- Optical disks i.e. DVD and CD
- Solid state memory devices including memory cards, pen drives, memory sticks (USB) etc.

2.2. All removable media for use on information systems owned or operated by the CCG are covered by this procedure.

2.3. Only CCG provided encrypted USB memory sticks are used by staff independently. Other removable media are only used with agreement and in conjunction with CCG ICT staff.

3. Responsibilities

3.1. Staff and contractors are not permitted to introduce or use any removable media other than those provided, or explicitly approved for use, by the Senior ICT Service Development Manager on behalf of the CCG.

3.2. Any bulk data extracts (over 50 records) of person identifiable information or business sensitive information must be authorised by the responsible Director for the work area and a log/register kept of such transactions (see Appendix A).

3.3. The Senior ICT Service Development Manager is responsible for ensuring that the CCG has adequate supplies of all removable media that has been approved for use.

3.4. The Senior ICT Service Development Manager is responsible for identifying and arranging the implementation of any device configuration requirements that the CCG may need. This will enable compliance with NHS Information Governance standards and IT security policy and procedures, for example, the restriction of write permission to hard drives, USB port restrictions etc.

3.5. Assistant Directors are responsible for authorising the use of removable media by staff and must record the authorisation in the format outlined in Appendix A.

3.6. Assistant Directors should assure themselves that there is a real business requirement to use removable media.

3.7. Assistant Directors, in collaboration with the Senior ICT Service Development 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.

3.8. Assistant Directors are responsible for the secure storage of all unallocated or returned removable media and any related control documentation required by this procedure.

3.9. Assistant Directors are responsible for ensuring that staff authorised to use removable media receive appropriate Information Governance training.

3.10. 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 CCG and may result in disciplinary or criminal action.

3.11. Staff must not use removable media to store the primary record. The primary record must always be stored on a secure network drive.

3.12. Staff must keep a record of the data that is stored on removable media. In the case of media lost or stolen a copy of this record must be included in the incident report.

3.13. Staff must be aware of policy and procedure governing the work area, including consequences of breach of policy.

3.14. Staff have a responsibility to ensure all individuals with which they work do not use non-approved removable media when working on NHS related activities.

4. Security Procedures

4.1. Removable media shall only be used by staff and contractors who have an identified and agreed business need for them.

4.2. The use of removable media by sub-contractors or temporary workers must be subject to the same risk assessment and authorisation process.

4.3. Removable media that have been approved for use within the CCG are to be identified by the Senior ICT Service Development Manager.

4.4. Removable media may only be used to store and share NHS information that is required for a specific business purpose.

4.5. Where person identifiable information or business sensitive information is being sent or received, a process must be in place to record the safe receipt. Note: Only very limited and controlled use of Patient identifiable data (PID) / Personal Confidential Data (PCD) is allowed within the CCG. For any processing of PID / PCD under the General Data Protection Regulations a legal basis to do so must be identified. The CCG has very few approved reasons for the use of PID/PCD.

4.6. 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.

4.7. Spot check audits and questionnaires will be conducted by the CCG to ensure this policy is complied with. Any compliance issues will be reported to the Assistant Director concerned and may be handled through staff disciplinary processes or contractual arrangements.

4.8. All incidents involving the use of removable media must be reported to the Senior ICT Service Development Manager and Information Governance Lead immediately and in accordance with the CCG's Incident and near miss reporting guidance.

4.9. Removable media should not be taken or sent off-site unless a prior agreement or instruction exists. A record must be maintained of all removable media taken or sent off-site, or brought into or received by the organisation. This record should also identify the data files involved. (Appendix A).

4.10. Removable media must be physically protected against their loss, damage, abuse or misuse when used, where stored and in transit.

4.11. When the business purpose has been satisfied, the contents of removable media must be removed from that media through a destruction method that makes recovery of the data impossible. Alternatively the removable media

and its data should be destroyed and disposed of beyond its potential reuse. In all cases, a record of the action to remove data from or to destroy data should be recorded in an auditable log file.

5. Unacceptable Use

5.1. The following activities are, in general, prohibited. The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

5.2. The unauthorised storage of patient identifiable or business sensitive information on any form of removable media (including memory pens, generic MP3 players, digital cameras etc).

5.3. The use of any removable media, such as digital cameras, generic MP3 players, external hard drives, USB memory sticks etc to the CCG network without prior authorisation from the Senior ICT Service Development Manager.

5.4. Attempting to install applications / or programs from removable media onto any CCG computer assets.

5.5. The saving of non-operational documents, files or folders from any removable media to any CCG network drive or computer asset.

5.6. Use of USB drives or other mechanisms to subvert Cambridgeshire and Peterborough CCG security controls is expressly forbidden. Any failure to comply with this requirement will be reported to the Assistant Director concerned and may be handled through staff disciplinary processes or contractual arrangements.

NHS
Cambridgeshire and Peterborough
Clinical Commissioning Group

AUTHORISATION REQUEST FORM FOR THE USE OF REMOVABLE MEDIA
(NB Only one application per form)

Name of User (Block Capitals): _____

Job Title: _____ Base: _____

Contact Number: _____ Date: _____

I request authorisation to use the following removable media (please tick):

Media Type		**Asset No/ Serial No** *(if approved)*	**Media Type**		**Asset No/ Serial No** *(if approved)*
Blackberry/PDA			Memory Card		
USB Pen drive			External Hard drive		
CD/DVD			ZIP/DAT drive		

Other: (please specify)…….

The removable media will be used for the following purposes:

PC Asset No. *(If applicable)*	Specific details of data to be transferred	Purpose/Location

I have read and agree to abide by the CCG's Removable Media Policy and Information Security Staff Policy.

I understand that any breach will result in my access being terminated and may lead to disciplinary action being taken by the CCG.

The issued USB memory key remains the property of the Trust and must be returned to the IT Dept. when leaving the organisation or when it is no longer required to fulfil the job role.

Failure to do so will incur a replacement charge for the Unit. This is a nominal £10 for a 1GB USB Stick.

Signature of User……..
(Cambridgeshire and Peterborough CCG retains ownership of any data that is held on removable media issued)

ASSISTANT DIRECTOR AUTHORISATION

I authorise the purchase of the above removable media for the use specified.

I confirm that I understand my responsibility for the day to day management and oversight of this device in accordance with the Removable Media and Information Security Policies.

Signed .....

Name (Block capitals):.....

Job Title:..... Date:.....

Base: ..... Contact no: .....

AUTHORISED / REJECTED BY INFORMATION GOVERNANCE MANAGER

Date: _____

Authorised (Yes/No): _____

If no, reason for rejection .....

.....

Signed .....

Name (Block capitals) .....

ISSUE/RETURN

Date of issue: _____

Signed (Senior ICT Service Development Manager/Assistant Director)

.....

Name (Block capitals).....

Signed (Member of staff for receipt) .....

Name (Block capitals).....

Date of return: _____

Signed (Senior ICT Service Development Manager/Assistant Director)

.....

Name (Block capitals).....

Signed (Member of staff for return).....

Name (Block capitals).....

Appendix B

Process for Requesting Removable Media