NHS
Nottingham and Nottinghamshire
Integrated Care Board

Removable Media Policy

July 2022 – July 2025

CONTROL RECORD			
Reference Number GOV-013	**Version** 1.0	**Status** Final	**Author** Cyber Security Assurance Programme Board **Sponsor** Information Governance Steering Group **Team** Information Governance Team
Title	Removable Media Policy		
Amendments	None		
Purpose	To set out the principles and working practices that are to be adopted by all users of devices or applications supplied to them by Nottingham and Nottinghamshire Integrated Care Board to support its health and social care business functions in order for data to be safely stored and transferred on removable media to ensure that the use of removable media devices is controlled and managed appropriately.		
Superseded Documents	None		
Audience	All staff, third parties, contractors and partners of systems, that are users of devices or applications supplied to them by Nottingham and Nottinghamshire Integrated Care Board to support its health and social care business functions.		
Consulted with	The Policy has been reviewed and developed by the Cyber Security Assurance (CSA) Delivery Group and approved by the CSA Programme Board.		
Equality Impact Assessment	June 2022		
Approving Body	ICB Board	Date Approved:	1 July 2022
Date of Issue	July 2022		
Review Date	July 2025		
This is a controlled document and whilst this policy may be printed, the electronic version available on the ’s document management system is the only true copy. As a controlled document, this document should not be saved onto local or network drives.			

NHS Nottingham and Nottinghamshire Integrated Care Board (ICB)’s policies can be made available on request in a range of languages, large print, Braille, audio, electronic and other accessible formats from the Engagement and Communications Team at nnicb-nn.comms@nhs.net.

Contents

1. Introduction

1.1. This policy been reviewed and developed as part of the Nottingham and Nottinghamshire Integrated Care Board ('the ICB') and partner commitments to maintaining a secure network as part of the Cyber Security Assurance Programme partners as follows:

- Nottingham and Nottinghamshire Integrated Care Board
- Sherwood Forest Hospitals NHS Foundation Trust
- Nottingham CityCare Partnership
- Nottinghamshire Health Informatics Service (NHIS).

1.2. Failure to control or manage the use of removable media can lead to significant financial loss, the theft of information, the introduction of malware and severe loss of reputation to the organisation. Removable media should only be used to store or transfer information as a last resort. Under normal circumstances information should only be stored on corporate systems and exchanged using appropriately protected and approved information exchange connections.

1.3. This policy aims to ensure that the use of removable media devices is controlled in and managed in order to:

- Enable the correct data to be made available where it is required
- Maintain the integrity of the data
- Prevent unintended or deliberate consequences to the stability of the IT Network
- Avoid contravention of any legislation, policies or good practice requirements
- Build confidence and trust in the data that is being shared between systems
- Maintain high standards of care in ensuring the security of protected and restricted information
- Prohibit the disclosure of information as may be necessary by law.

1.4. All partners are committed to the principles of the policy and protection of the shared network through management of removable media. They will ensure the controlled and managed use of removable media devices to store and transfer information by all users who have access to information, information systems and software, IT equipment and devices for the purposes of conducting Nottingham and Nottinghamshire Integrated Care Board official business.

2. Purpose

2.1. This policy establishes the principles and working practices that are to be adopted by all users in order for data to be safely stored and transferred on removable media.

2.2. Users are required to adhere to this policy at all times, but specifically whenever any user intends to store any information used by the ICB to conduct official business on removable media devices.

2.3. Adherence to this policy aims to reduce the following risks

- Disclosure of sensitive or personal confidential information as a consequence of loss, theft or careless use of removable media devices.
- Contamination of networks or equipment through the introduction of viruses or malware through the transfer of data from one form of IT equipment to another.
- Potential sanctions against the ICB or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the ICB or individuals as a result of information loss or misuse.
- reputational damage as a result of information loss or misuse.

2.4. Non-compliance with this policy could have a significant effect on the efficient operation of the ICB and may result in financial loss and an inability to provide necessary services to our customers.

3. Scope

3.1. This Removable Media Policy applies to:

- All employees who work for or on behalf of the ICB including those on temporary or honorary contracts, secondments, volunteers, Integrated Care Board members, students and any staff working on an individual contractor basis or who are employees for an organisation contracted to provide services to the ICB.
- All Nottingham and Nottinghamshire ICB Directors, Heads of Departments, Senior Managers nominated Information Asset Owners and Information Asset Managers are responsible for the security of their systems, devices or applications supplied to their business area by Nottingham and Nottinghamshire Integrated Care Board to support its health and social care business functions.

4. Definitions

4.1. Removable media devices include, but are not restricted to the following:

Term	Definition
Removeable Media Devices	Removable media devices include, but are not restricted to the following: • CDs • DVDs • Optical Disks • External Hard Drives • USB Memory Sticks (also known as pen drives or flash drives) • Media Card Readers • Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards) • MP3 Players • Digital Cameras • Backup Cassettes • Audio Tapes (including Dictaphones and Answering Machines).

5. Roles and Responsibilities

5.1. This table sets out Removable Media Policy key responsibilities for specific roles and staff groups in relation to delivering the objectives of this policy.

Role	Responsibilities
ICB Board	The Board must have Individual Officer arrangements in place to ensure that requirements of this policy are carried out effectively.
Senior Information Risk Owner (SIRO)	The Chief Financial Officer, in their role as Senior Information Risk Owner (SIRO) takes ownership of the organisation's information risk and act as an advocate for information risk on the Board.
Information Governance Steering Group (IGSG)	IGSG reports to the Audit and Risk Committee and is responsible for ensuring that this policy is implemented, including: • Providing direction and support for removable media activities in accordance with business requirements • It will monitor and provide Board assurance in this respect.

Role	Responsibilities
Information Asset Owner's (IAOs) / Directors	Are responsible for implementing and maintaining this policy in their area of management of Nottingham & Nottinghamshire ICB systems, devices or applications, ensuring that procedures are in place and staff have adequate access to information management and security training.
Designate Heads of Department and Senior Managers	Are responsible for implementing and maintaining this policy in their area of management of Nottingham & Nottinghamshire ICB systems, devices or applications ensuring that procedures are in place and staff have adequate access to information management and security training.
Information Asset Managers (IAMs) and line managers	Information Asset Managers (IAMs) have day to day responsibility for managing their information assets and associated records management, confidentiality, integrity and availability to include information security.
All Staff	All members of staff should read and note and fully adhere to the requirements of this policy and must have access to and follow the guidance outlined in local SOPs/Processes and procedures. The ICB will investigate all suspected/actual security breaches and report through their incident reporting procedures.
Caldicott Guardian	The Caldicott Guardian will be central to the framework for handling personal confidential data in the NHS and will be fully aware of their responsibilities specified in the Caldicott Guardian Manual (Department of Health, 2017 Manual).

6. Removable Media Management and Controls

6.1. Securing business confidential, personal confidential or sensitive data is of paramount importance – particularly in relation to Nottingham and Nottinghamshire Integrated Care Board (the ICB) statutory requirements to protect data in line with the requirements of the data protection legislation.

6.2. Any loss of the ability to access information or interference with its integrity could have a significant effect on the efficient operation of the ICB. It is therefore essential for the continued operation of the ICB that the confidentiality, integrity and availability of all information systems are maintained at a level, which is appropriate to the ICB's business needs.

6.3. The ICB recognises that there are risks associated with users accessing and handling information in order to conduct official ICB business. Information is used throughout the organisation and sometimes shared with external bodies, organisations and individuals. To mitigate this risk, it is ICB policy to prohibit the use of all removable media devices.

6.4. The use of removable media devices will only be approved if a valid business case for its use is developed. As there are large risks associated with the use of removable media, and clear business benefits that outweigh the risks must be demonstrated before approval is given.

6.5. Restricted Access to Removable Media

Where the use of removable media is required to support the business need, it should be limited to the minimum media types and users needed. The secure baseline build should deny access to media ports by default, only allowing access to approved users.

- Requests for access to, and use of, removable media devices must be made to the employee's relevant line manager, Approval for their use must be given by the Information Asset Owner (IAO) and information governance. Requests should be directed to the NHIS Customer Portal Internal Customer Portal: http://customerportal.notts-his.nhs.uk/
- Should access to, and use of, removable media devices be approved the following sections apply and must be adhered to at all times.
- By default, all desktops under the control of the ICB shall have USB ports disabled and read access only via DVD drive. Any requirement to deviate from this shall require formal authorisation and business justification with line manager approval prior to submission to Information Governance and the NHIS cyber security team.
- If there is a requirement for data to be burned to CD/DVD or copied to other removable media, this shall have approval of the relevant Information Asset Owner (IAO) for the data. The IAO shall ensure that only encrypted removable media is used in their area.

6.6. Procurement of Removable Media

- All removable media devices and any associated equipment and software must only be purchased and installed by NHIS.
- Non-ICB owned removable media devices **must not** be used to store any information used to conduct official ICB business and **must not** be used with any ICB owned or leased IT equipment.
- The only equipment and media that should be used to connect to ICB equipment or the NHIS network is equipment and media that has been

purchased by NHIS or approved ICB procurement routes and approved by the IAO or has been sanctioned for use by Information Governance.

6.7. Security of Data when using Removable Media

- Data that is only held in one place and in one format is at much higher risk of being unavailable or corrupted through loss, destruction or malfunction of equipment than data which is frequently backed up.
- Therefore, removable media should not be the only place where data obtained for ICB purposes is held.
- Copies of any data stored on removable media must also remain on the source system or networked computer until the data is successfully transferred to another networked computer or system.
- In order to minimise physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment.
- Each user is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way whilst in their care or under their control.

6.8. Incident Management for Removal Media

- It is the duty of all users to immediately report any actual or suspected breaches in information security via the Information Governance Team and all incidents will be required to be investigated as outlined in the Risk Management Policy.
- Any misuse or irresponsible actions that affect business data, or any loss of data, should be reported as a security incident to the Information Governance Team**.**

6.9. Third Party Access to ICB Information

- No third party (external contractors, partners, agents, and the public or non-employee third parties) may receive data or extract information from the ICB’s network, information stores or IT equipment without explicit agreement and approval from the Information Governance Team and IAO for the system/equipment.
- Should third parties be allowed access to ICB information then all the considerations of this policy apply to their storing and transferring of the data. There should be robust controls in place for management of third parties and contractors who require connection to the network. Completion and approval

of the relevant connection agreement or authorised process is available from the information governance team.

6.10. Preventing Information Security Incidents

- Damaged or faulty removable media devices must not be used. It is the duty of all users to contact NHIS should removable media be damaged.
- Virus and malware checking software approved by the [Nottinghamshire Health Informatics Service (NHIS)] must be operational on both the machine from which the data is taken and the machine on to which the data is to be loaded. The data must be scanned by virus checking software products, before the media is loaded on to the receiving machine
- Whilst in transit or storage the data held on any removable media devices must be given appropriate security according to the type of data and its sensitivity. Encryption or password control must be applied to the data files unless there is no risk to the ICB, other organisations or individuals from the data being lost whilst in transit or storage.

6.11. Disposing of Removable Media Devices

- Any devices for reuse must have their contents erased to the recognised NHS standard. This must be a thorough removal of all data from the media to avoid potential data leakage using specialist software and tools. All removable media devices that are no longer required, or have become damaged, must be returned to NHIS for secure disposal

- For advice or assistance on how to thoroughly remove all data, including deleted files, from removable media, contact the NHIS Service Desk on 01623 410310 or internally dial 4040.

6.12. User Responsibility

All considerations of this policy must be adhered to at all times when using all types of removable media devices and user guidance is available at **Appendix A**. However, special attention must be paid to the following when using USB memory sticks (also known as pen drives or flash drives), external hard drives, recordable CDs, DVDs and diskettes:

- Any removable media device used in connection with ICB equipment or the network or to hold information used to conduct official ICB business **must** only be purchased and installed by NHIS. Any removable media device that has not been supplied by NHIS **must not** be used.

- Virus and malware checking software **must** be used when the removable media device is connected to a machine.
- Only data that is authorised and necessary to be transferred should be saved on to the removable media device. Data that has been deleted can still be retrieved.

- Removable media devices **must not** be used for archiving or storing records as an alternative to other storage equipment.

- Special care **must** be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

- For advice or assistance on how to securely use removable media devices, please contact the Information Governance team.

6.13. Non-Compliance with Removable Media Management and Controls

If any user is found to have breached this policy, they may be subject to ICB disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s). If you do not understand the implications of this policy or how it may apply to you, please seek advice from the Information Governance Team.

7. Communication, Monitoring and Review

7.1. Managers are required to make staff aware of information governance responsibilities with ICB policies to include this Removable Media Policy during their induction period. This policy is included in the ICB suite of policies available on-line.

7.2. The Information Governance Steering Group are responsible for monitoring compliance and the effectiveness of this policy though the reporting of incidents, use of audits and staff surveys.

7.3. Any individual who has queries regarding the content of this policy, or has difficulty understanding how this policy relates to their role, should contact the Information Governance Team.

8. Staff Training

8.1. Nottingham and Nottinghamshire ICB is required to ensure organisational compliance with legislation and Department of Health and Social Care guidelines relating to data security and data protection. This requires knowledge and awareness of data security and data protection to be at the core of the ICB's objectives and embedded amongst other governance initiatives.

8.2. Annual Data Security Awareness (DSA) Level 1 training, as developed by NHS Digital, is mandatory for all staff members, including new starters, locums, temporary staff, lay members, student and contract staff at induction and on an annual basis as refresher training for staff.

8.3. This training is mandated for corporate induction and thereafter annually with a minimum target of 95% completion across the ICB. At Induction managers must provide staff with the Information Governance Staff Handbook that provides awareness of information security concepts & principles to ensure compliance with this policy but should more training be required please contact the Information Governance Team.

9. Equality and Diversity Statement

9.1. Nottingham and Nottinghamshire ICB pays due regard to the requirements of the Public Sector Equality Duty (PSED) of the Equality Act 2010 in policy development and implementation as a commissioner and provider of services, as well as an employer.

9.2. The ICB is committed to ensuring that the way we provide services to the public and the experiences of our staff does not discriminate against any individuals or groups on the basis of their age, disability, gender identity (trans, non-binary), marriage or civil partnership status, pregnancy or maternity, race, religion or belief, gender or sexual orientation.

9.3. We are committed to ensuring that our activities also consider the disadvantages that some people in our diverse population experience when accessing health services. Such disadvantaged groups include people experiencing economic and social deprivation, carers, refugees and asylum seekers, people who are homeless, workers in stigmatised occupations, people who are geographically isolated, gypsies, roma and travellers.

9.4. As an employer, we are committed to promoting equality of opportunity in recruitment, training and career progression and to valuing and increasing diversity within our workforce.

9.5. To help ensure that these commitments are embedded in our day-to-day working practices, an Equality Impact Assessment has been completed for, and is attached to, this policy.

10. Interaction with other Policies

10.1. This policy document should be read in conjunction with:

- Confidentiality and Data Protection Policy;
- Information Security Policy;
- Internet and Email Policy;
- Account Management and Access Policy;
- Acceptable Use of the Network Policy;
- Risk Management Policy;
- Incident Reporting and Management Policy;
- Information Governance Staff Handbook.

11. References

11.1. This policy takes into account reviews of the following as part of the development of this policy document:

- Access to Health Records Act 1990;
- Caldicott Guidance as updated 2013;
- Common Law Duty of Confidentiality;
- Computer Misuse Act 1990;
- Coroners and Justice Act 2009;
- Crime and Disorder Act 1998;
- Data Protection Act 2018;
- General Data Protection Regulation 2016;
- Electronic Communications Act 2000;
- Environmental Information Regulations 2004;
- Equality Act 2010;
- Fraud Act 2006;
- Freedom of Information Act 2000;
- Health and Social Care Act 2012;
- NHS Digital Guidance;
- Human Rights Act 1998;
- ISO/IEC 27001:2005 Specification for an Information Security Management system & ISO/IEC27002:2005 Code of Practice for Information Security Management;
- NHS Act 2006;

- Privacy and Electronic Communications Regulations 2003;
- Protection of Freedoms Act 2012;
- Public Interest Disclosure Act 1998;
- Public Records Act 1958;
- 2004 Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992.

12. Equality Impact Assessment for this Policy

Date of assessment:	**June 2022**			
For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups:	Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity?	If yes, are there any mechanisms already in place to mitigate the adverse impacts identified?	Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned.	Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe.
Age[1]	None identified	N/A	None	None
Disability[2]	Visual accessibility of this policy	Use of technology by end user. This policy can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request.	None	None
Gender identity (trans, non-binary)[3]	None identified	N/A	None	None
Marriage or civil partnership status[4]	None identified	N/A	None	None

[1] A person belonging to a particular age (for example 32 year olds) or range of ages (for example 18 to 30 year olds).

[2] A person has a disability if she or he has a physical or mental impairment which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities.

[3] The process of transitioning from one gender to another.

Date of assessment:	**June 2022**			
For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups:	Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity?	If yes, are there any mechanisms already in place to mitigate the adverse impacts identified?	Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned.	Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe.
Pregnancy or maternity[5]	None identified	N/A	None	None
Race[6]	None identified	N/A	None	None
Religion or belief[7]	None identified	N/A	None	None
Gender[8]	None identified	N/A	None	None
Sexual orientation[9]	None identified	N/A	None	None
Carers[10]	None identified	N/A	None	None

[4] Marriage is a union between a man and a woman or between a same-sex couple. Same-sex couples can also have their relationships legally recognised as 'civil partnerships'.

[5] Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth, and is linked to maternity leave in the employment context. In the non-work context, protection against maternity discrimination is for 26 weeks after giving birth, and this includes treating a woman unfavourably because she is breastfeeding.

[6] Refers to the protected characteristic of race. It refers to a group of people defined by their race, colour, and nationality (including citizenship) ethnic or national origins.

[7] Religion refers to any religion, including a lack of religion. Belief refers to any religious or philosophical belief and includes a lack of belief. Generally, a belief should affect your life choices or the way you live for it to be included in the definition.

[8] A man or a woman.

[9] Whether a person's sexual attraction is towards their own sex, the opposite sex, to both sexes or none. https://www.equalityhumanrights.com/en/equality-act/protected-characteristics

[10] Individuals within the which may have carer responsibilities.

APPENDIX A:

REMOVABLE MEDIA USER GUIDANCE

What is removable media?

Removable media is the term used to describe any kind of portable data storage device that can be connected to and removed from your computer. Typical examples are:

- CDs.
- DVDs.
- External Hard Drives.
- USB Memory Sticks (also known as pen drives or flash drives).
- MP3 Players and iPods.
- Digital Cameras.

What is the risk?

The NHS creates and uses a vast amount of confidential and sensitive information and it is critical that this information is well protected against unauthorised access, misuse or tampering.

Failure to control or manage the use of removable media can lead to significant financial loss, the theft of information, the introduction of malware and severe loss of reputation to our organisation.

Removable media should only be used to store or transfer information as a last resort. Under normal circumstances, information should be stored on corporate systems and exchanged using appropriately protected and approved information exchange connections.

The use of removable media to store or transfer personal and sensitive information is an everyday business process. However, we fail to adequately protect and manage removable media the organisation could be exposed to the following risks:

- Loss of information. The small physical size of removable media can result in it being easily misplaced or stolen, potentially compromising the confidentiality and availability of the information stored on it.
- Reputational damage. A loss of personal or sensitive data often attracts media attention which is likely to cause a lack of public confidence in the organisation.
- Financial loss. If personal or sensitive information is lost or compromised you and the organisation could be subjected to financial penalties and fines.
- Introduction of malware. The uncontrolled use of removable media on multiple systems will increase the risk from malware.
- Information leakage. Some media types retain information after user deletion; this could lead to an unauthorised transfer of information between systems.

How do I protect removable media?

You can protect removable media, the information held on it and your organisation by:

- Limiting the use of removable media. The use of removable media should be authorised by the organisation and limited to encrypted devices. The type of encryption should be proportionate (and in accordance with NHS requirements) to the value of the information and the risks posed to it.
- Scanning all media for malware. Ensure that all removable media is scanned with the organisation’s anti-virus solution before it is brought in to use or when received from any other organisation.
- Formally accounting for all removable media. All removable media should be formally issued by the organisation to individuals who will be accountable for its secure use and return for destruction or reuse.
- Applying password protection. Passwords protect the information or the media itself in order to restrict access. Remember that the password will also need to be protected to the level of the data it gives access to.

Do

- Make sure that you understand your organisation’s information security policy for removable media.
- Use encryption or passwords to protect security classified, personal or sensitive information held on removable media.
- Ask for help from your IT department or line manager if you’re not sure what to do with removable media.
- Special care **must** be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

Don’t

- Copy files to removable media unless you really need to and it is authorised by your organisation.
- Leave removable media lying around. Lock it away when not in use even if you believe it contains no information.
- Attempt to access files from any removable media that you may have found, not even to determine to whom it might belong - it could contain a computer virus; instead you should pass it on to your IT department or line manager.