DATA LEAKAGE PREVENTION AND REMOVABLE MEDIA POLICY

	POLICY

Reference	IG/005		
Approving Body	Data Protection and Cyber Security Committee		
Date Approved	3rd August 2026		
For publication to external SFH website	**Positive confirmation received from the approving body that the content does not risk the safety of patients or the public:**		
	YES	**NO**	
	x		
Issue Date	September 2026		
Version	5		
Summary of Changes from Previous Version	Full policy review undertaken. Scope broadened from removable media to data leakage prevention and removable media controls. Title, definitions, policy statement, approval requirements, incident reporting, monitoring arrangements, evidence base, related documents, keywords and staff guidance updated to reflect current information governance, cyber security and ISO/IEC 27001:2022 storage media requirements.		
Supersedes	Version 4		
Document Category	Information Governance		
Consultation Undertaken	The policy has been reviewed and developed through the Cyber Security Assurance Delivery Group (CSADG), with consultation through the Information Governance Working Group (IGWG). It will be shared with the Cyber Security Assurance Programme Board (CSAPB) for partner awareness, alignment and local adoption.		
Date of Completion of Equality Impact Assessment	3rd July 2026		
Date of Environmental Impact Assessment (if applicable)	Not applicable		
Legal and/or Accreditation Implications	Data Protection Act 2018; UK GDPR; Common Law Duty of Confidentiality; Caldicott Principles; NHS Data Security and Protection Toolkit; ISO/IEC 27001:2022; NIS Regulations 2018 where applicable.		
Target Audience	All staff and visitors		
Review Date	3rd August 2028		
Sponsor (Position)	Director of Corporate Affairs		
Author (Position & Name)	Ruth Lloyd, Head of Corporate and Business Support and Jacquie Widdowson, Head of Data Security and Privacy		

Lead Division/ Directorate	Corporate
Lead Specialty/ Service/ Department	Information Governance
Position of Person able to provide Further Guidance/Information	NHIS Cyber Security Information Governance

Associated Documents/ Information	**Date Associated Documents/ Information was reviewed**
1. Data Protection, Confidentiality and Disclosure Policy	July 2026
2. Remote Working Policy	January 2026
3. Email and Internet Policy	March 2026
4. Information Security Policy	June 2025
Template control	April 2024

CONTENTS

APPENDICIES

1.0 INTRODUCTION

The policy establishes the principles and working practices that must be followed by all users to ensure that information is stored, handled and transferred securely. Information must remain within approved, corporately controlled systems wherever possible and, where transfer is authorised, must be protected by appropriate security controls, including encryption in transit and at rest where required.

For the purposes of this policy, data leakage prevention refers to the controls and behaviours required to prevent Trust information from being removed, copied, transferred, disclosed or stored outside approved corporate systems without authorisation. Removable media is one specific high-risk method by which data leakage may occur and is therefore subject to specific controls within this policy.

The scope of this policy includes the use of removable media and other activities that may result in information being removed from approved corporate systems, including copying, downloading, printing, photographing, recording, uploading to non-approved cloud storage, use of personal devices and use of non-approved digital tools. Removable media remains a specific high-risk area covered by this policy, but the wider principle is that Trust information must not be moved, stored or processed outside approved environments unless this has been formally authorised.

2.0 POLICY STATEMENT

Data leakage prevention is a fundamental component of information governance and cyber security within NHS organisations. It ensures that confidential, personal, and sensitive organisational data is protected from unauthorised access, disclosure, or loss. In an increasingly digital and mobile working environment, where staff have access to personal devices and multiple communication channels, the risk of inadvertent or deliberate data leakage has significantly increased.

Effective controls are therefore essential to safeguard patient confidentiality, maintain public trust, and meet statutory and regulatory requirements.

This policy has been developed as part of Nottinghamshire Health Informatics Service and partner organisation commitments to maintaining a secure shared network through the Cyber Security Assurance Programme.

All partners are committed to the principles of this policy and to the protection of the shared network through data leakage prevention controls, including the controlled use of removable media.

The Trust will ensure that information is stored, handled and transferred using approved systems and that any exception involving removable media is authorised, justified, encrypted where required and subject to appropriate technical controls.

Removable media must only be used where there is a documented business need, appropriate approval and approved technical controls in place. Under normal circumstances, information should be stored on corporate systems and exchanged using appropriately protected and approved information exchange routes.

This policy supports alignment with ISO/IEC 27001:2022 control A.7.10 Storage media and relevant information security policies and procedures.

3.0 DEFINITIONS/ ABBREVIATIONS

Data leakage means the unauthorised or inappropriate removal, disclosure, transfer, copying, storage, photographing, recording or sharing of Trust information outside approved corporate systems or processes.

Data leakage prevention means the policies, technical controls, governance arrangements and staff behaviours used to reduce the risk of information being removed, disclosed, copied, transferred or stored outside approved systems without authorisation.
Removable media means any portable storage device or medium that can be connected to and removed from a system and is used to store or transfer data. Examples include USB drives, external hard drives, solid-state drives, optical discs and memory cards.

Removable media means any portable storage device or medium that can be connected to and removed from a system and is used to store or transfer data. Examples include USB drives, external hard drives, solid-state drives, optical discs and memory cards.

Encrypted removable media means removable media that has been approved for use and protected using encryption or equivalent technical controls proportionate to the sensitivity of the information.

USB-connected peripheral equipment that does not store or transfer data, such as keyboards, mice, webcams and similar input or output devices, is outside the scope of the removable media controls unless it includes storage capability or creates another information security risk.

4.0 ROLES AND RESPONSIBILITIES

Groups & Committees

The Cyber Security Assurance Programme (CSA) has developed these documents to further ensure the security of the shared network and infrastructure. They have been developed by the CSA Delivery Group, consulted on by each partner by their internal governance.

Trust Board

The Trust Board is ultimately responsible for Information Governance within the organisation and is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

Information Governance Committee

The Committee is responsible for ensuring that this policy is effectively implemented, including any supporting guidance and training deemed necessary to support the implementation, and for monitoring and providing Board assurance in this respect.

Chief Executive

The Chief Executive has overall responsibility for this policy within the Trust. Implementation of, and compliance with this policy is delegated to the Senior Information Risk Owner, Caldicott Guardian, Data Protection Officer, and members of the Information Governance Committee.

Senior Information Risk Owner (SIRO)

The SIRO is responsible to the Chief Executive for Information Governance, who takes ownership of the Trust's information risk policy, acts as an advocate for information risk on the Board and provides written advice to the Chief Executive on the content of the Statement of Internal Control in regard to information risk. The SIRO also reports annually to the Trust Board on Information Governance performance.

Caldicott Guardian

The Caldicott Guardian[1] is the 'conscience' of the organisation, providing a focal point for patient confidentiality, information sharing and advising on the options for lawful and ethical processing of information as required.

Data Protection Officer (DPO)

As a public authority the Trust is required to have a Data Protection Officer. The Head of Data Security and Privacy is the Trusts designated Data Protection Officer and reports to the Senior Information Risk Owner and works with the Caldicott Guardian. The Data Protection Officer is tasked with monitoring compliance with Data Protection legislation, our data protection policies, awareness-raising, training, and audits. Our Data Protection Officer acts as a contact point for the Information Commissioner's Office. When performing their tasks, our Data Protection Officer has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purposes of processing.

Information Asset Owners (IAOs)

[1] https://www.sfh-tr.nhs.uk/about-us/regulatory-information/your-medical-record-privacy-policy/caldicott-guardians/

Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result, they are able to understand and address risks to the information and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process. When carrying out a Data Protection Impact Assessment, they seek the advice from the Information Governance Team and of our Data Protection Officer who also monitors the process.

Information Asset Administrators (IAAs)
Information Asset Administrators ensure that IG policies and procedures are followed, recognise actual or potential IG security incidents and take steps to mitigate those risks, consult their Information Asset Owners on incident management, and ensure that information asset registers are accurate and up to date. When carrying out a Data Protection Impact Assessment, they seek the advice from the Information Governance Team and of our Data Protection Officer who also monitors the process.

All Staff
All staff (including Medirest, Skanska, agency and contractor colleagues) who use and have access to Trust personal information must understand their responsibilities for data protection and confidentiality.

Contractors and agency staff and other third parties' staff are under instructions to report all incidents, their causes and resolving actions to their own line managers. The Trust reserves the right to audit the supplier's contractual responsibilities or to have those audits carried out by a third party.

The Trust will expect an escalation process for problem resolution relating to any breaches of IG security and/or confidentiality of personal information by the Contractor's employee and/or any agents and/or sub-contractors. Any IG security breaches made by the Contractor's employees, agents or sub-contractors will immediately be reported to the Trust's Information Governance Team.

Third parties contracting services to the Trust must sign a confidentiality agreement, countersigned by the Information Asset Owner. This ensures that their employees undertake annual data security awareness training, have read and understood our data protection and confidentiality policy and accept their personal responsibility to maintain confidentiality at all times.

Managers or health professionals who are responsible for any seconded / work experience placement should ensure that all students have read and understood our data protection and confidentiality policy and accept their personal responsibility to maintain confidentiality at all times.

5.0 APPROVAL

Approval of this policy for Sherwood Forest Hospitals NHS Foundation Trust will be through the Data Protection and Cyber Security Committee, following consultation through the Information Governance Working Group. The policy will be shared with the Cyber Security Assurance Programme Board for partner awareness, alignment and adoption through each partner organisation's own governance arrangements.

6.0 DOCUMENT REQUIREMENTS

This policy should be read alongside the Trust's Data Protection, Confidentiality and Disclosure Policy, Data Protection Impact Assessment Policy and Information Security Policy. Those documents set out the wider requirements for lawful information sharing, DPIA completion, confidentiality, access controls and information security. This policy focuses specifically on preventing data leakage and controlling the use of removable media and other routes by which Trust information may be removed, copied, stored, transferred or disclosed outside approved corporate systems.

Access to, use of and transfer of information must be limited to what is necessary, proportionate and justified for an authorised operational or clinical purpose. Staff must follow the need-to-know principle and must not access, copy, transfer or share information unless there is a legitimate business need and an approved route for doing so.

The Trust recognises that there are risks associated with users accessing, handling, storing and transferring information in order to conduct official Trust business. Information is used throughout the Trust and may be shared with external organisations, partner organisations, applicants and other authorised recipients where there is a lawful and legitimate business need.

Information sharing must be undertaken in line with the Trust's Data Protection, Confidentiality and Disclosure Policy. This policy does not replace the wider requirements for lawful information sharing, confidentiality, Caldicott considerations or disclosure governance.

Securing personal confidential, sensitive and business critical information is of paramount importance, particularly in relation to the Trusts obligations under data protection legislation and the Trust's Data Protection, Confidentiality and Disclosure Policy. Any loss of confidentiality, integrity or availability of all information could have a significant impact on the efficient operation of the Trust, the delivery of services, patient care, staff, partner organisations and public confidence.

Failure to control or manage the use of removable media and other routes by which information may be removed from approved corporate systems can result in significant financial loss, theft or inappropriate disclosure of information, introduction of malware, regulatory action and

serious reputational damage.. Removable media must only be used to store, access 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 routes.

Examples of data leakage risks include copying information to personal cloud storage, uploading information to non-approved online accounts, photographing information on a mobile phone, using personal artificial intelligence tools for clinical or corporate work, leaving paper records accessible outside secure working environments, or using personal devices or messaging platforms to store, copy or share Trust information.

This policy aims to reduce the following risks:

- disclosure of sensitive, personal confidential or business critical information as a result of loss, theft, unauthorised disclosure, inappropriate transfer or careless use of removable media or other non-approved methods of storage or transfer.
- contamination of Trust networks, systems or equipment through the introduction of viruses or malware, including through the transfer of data from one form of IT equipment to another.
- unauthorised removal, copying, photographing, recording, uploading or storage of Trust information outside approved corporate systems;
- potential regulatory action against the Trust or individuals, including action by the Information Commissioner's Office, as a result of information loss, misuse or inappropriate disclosure.
- potential legal action against the Trust or individuals as a result of information loss, misuse or inappropriate disclosure.
- financial loss, operational disruption or inability to provide necessary services, and
- reputational damage to the Trust or partner organisations as a result of information loss, misuse or inappropriate disclosure.

Non-compliance with this policy could have a significant effect on the efficient operation of the Trust and may result in financial loss, operational disruption, regulatory action, reputational damage and an inability to provide necessary services.

Restricted Access to Removable Media

The use of removable media is prohibited by default. Removable media must only be used where there is a documented and proportionate business need, where approved corporate systems or approved information exchange routes are not suitable, and where the risks have been assessed and accepted through the appropriate governance route.

Any exception must be approved before access is enabled. Approval must include authorisation from the relevant line manager, review by Information Governance, and confirmation from NHIS that appropriate technical and cyber security controls can be applied. Where removable media

will be used to store, transfer or access information owned by a specific system, service or information asset, approval must also be obtained from the relevant Information Asset Owner.

Requests for access to, and use of, removable media must be submitted through the approved NHIS service request process. http://customerportal.notts-his.nhs.uk/

Each request must include:

- the business justification;
- the type of information to be stored, accessed or transferred;
- the proposed device or media type;
- the intended recipient, destination or receiving system;
- the period for which access is required;
- confirmation that approved alternative transfer methods have been considered;
- line manager approval;
- Information Governance approval;
- Information Asset Owner approval, where applicable; and
- the associated approval record.

Where an exception is approved, access must be limited to the minimum number of users, devices and media types necessary to meet the approved business need. Permitted devices and/or approved user access must be recorded on the relevant organisation-specific whitelist or technical control register before use is enabled.

By default, desktops and other Trust-controlled devices must have removable media access disabled or restricted through technical controls. Any requirement to deviate from the approved secure baseline must be supported by a documented business justification and approved before implementation.

Where data is required to be copied to CD, DVD or other removable media, the relevant Information Asset Owner must approve the transfer. The Information Asset Owner must ensure that only approved encrypted removable media is used, unless a specific and documented exception has been approved through Information Governance and NHIS cyber security review.

The approval record must be retained for audit purposes and reviewed when the business requirement changes, the approved period expires, the user changes role, or the device is no longer required.

Technical controls support compliance with this policy but do not remove individual responsibility. Users must not attempt to bypass, disable or circumvent security controls. Any business process that cannot comply with this policy must be documented, risk assessed and approved by the relevant Information Asset Owner and Information Governance before it is implemented or used.

Should access to, and use of, removable media be approved, the following requirements apply and must be adhered to at all times.

Procurement of Removable Media

All removable media devices, associated equipment and software must only be purchased, approved and installed through NHIS or approved Trust procurement routes..

Non-Trust owned removable media devices **must not** be used to store, access or transfer any information used to conduct official Trust business, and **must not** be used with any Trust owned, leased or managed IT equipment.

The only equipment or media that may be connected to Trust equipment or the NHIS network is equipment or media that has been purchased through NHIS or approved Trust procurement routes and has been approved by the relevant Information Asset Owner or sanctioned for use by Information Governance.

Security of Data

Data that is only held in one place and in one format is at higher risk of being unavailable, lost or corrupted through loss, destruction or malfunction or compromise of equipment than data that is stored and backed up within approved corporate systems.

Removable media must not be the only place where data obtained or used for Trust purposes is held.

Copies of any data stored on removable media must also remain on the source system or approved networked location until the data has been successfully transferred to another approved networked computer, system or storage location. For further information please refer to the Remote Working Policy.

To minimise physical risk, loss, theft, unauthorised access or corruption, all removable 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 ensuring that removable media devices, and the information stored on them, are not compromised in any way whilst in their care or under their control.

Incident Management

All users must immediately report any actual or suspected breach of information security involving removable media, data leakage, unauthorised transfer, inappropriate disclosure or

loss of information via the Datix system and the information governance team. All incidents will be investigated in accordance with the Incident Reporting Policy.

Any misuse, irresponsible action, attempted circumvention of technical controls, loss of data or activity that may affect the confidentiality, integrity or availability of business or personal confidential information must be reported as an information security incident to the information governance team.

Third Party Access to Trust Information

No third party, including external contractors, partners, agents, members of the public or other non-employee parties, may receive, remove, extract, copy, store or transfer information from the Trust's network, information stores or IT equipment without explicit agreement and approval from the Information Governance Team and the relevant Information Asset Owner.

Technical access by third parties must be managed through the Information Security Policy and relevant NHIS third-party access processes. This section applies specifically to preventing data leakage where third parties access, remove, copy, store or transfer Trust information.

Where third parties are approved to access Trust information, all relevant requirements of this policy apply to their handling, storage and transfer of the information. Robust controls must be in place for the management of third parties and contractors who require connection to the network or access to Trust information. The relevant connection agreement or authorised process must be completed and approved through information governance and NHIS Third Party Access processes must also be followed where applicable.

Preventing Information Security Incidents

Damaged or faulty removable media devices must not be used. Users must contact NHIS immediately if removable media is damaged, faulty, lost or suspected to be compromised.

Wider technical security controls, including malware protection, device monitoring and security configuration, are set out in the Trust's Information Security Policy and relevant NHIS technical control processes. Staff must not bypass or attempt to disable those controls.

Virus and malware checking software approved by the Nottinghamshire Health Informatics Service (NHIS) must be operational on both the machine from which data is taken and the machine on to which data is loaded. Data must be scanned using approved virus and malware checking software before removable media is loaded onto the receiving machine. Remote assurance of this capability is provided through overall estate monitoring by NHIS.

Whilst in transit or storage, information held on removable media must be protected according to the type of information and its sensitivity. Encryption or equivalent approved technical controls must be applied unless there is a documented and approved justification confirming

that there is no risk to the Trust, partner organisations or individuals from the information being lost, accessed or disclosed.

Disposing of Removable Media Devices

Secure disposal requirements in this section apply specifically to removable media. Wider records management, information security and equipment disposal requirements must be followed in line with Trust policies and NHIS secure disposal processes.

Any removable media intended for reuse must have its contents securely erased to the recognised NHS standard. This must involve thorough removal of all data from the media using appropriate specialist software or tools to prevent potential data leakage

All removable media devices that are no longer required, have become damaged, or are suspected to be compromised 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 ServiceDesk on 4040 or 01623 410310.

User Responsibility

All requirements of this policy must be adhered to at all times when using removable media or when handling, storing or transferring Trust information. devices.

Particular care must be taken when using USB memory sticks (also known as pen drives or flash drives), external hard drives, recordable CDs, DVDs, memory cards, disks or any other removable media

Users must ensure that:

- any removable media device used in connection with Trust equipment, the NHIS network or information used to conduct official Trust business has been purchased, approved and installed through NHIS. Or approved Trust procurement routes removable media that has not been supplied or approved through NHIS or approved Trust procurement routes is not used.
- approved virus and malware checking software is used when removable media is connected to a machine.
- only authorised and necessary data is saved to removable media
- removable media is not for archiving or storing records as an alternative to approved corporate systems.
- removable media is physically protected from loss, theft, damage, unauthorised access or disclosure, and

- anyone using removable media to transfer data can demonstrate that reasonable care has been taken to avoid damage, loss, theft, compromise or unauthorised disclosure.

Where a new or changed system, digital tool, transfer method, artificial intelligence tool, cloud service or data flow is proposed, staff must consider whether a Data Protection Impact Assessment is required in line with the Trust's Data Protection Impact Assessment Policy before implementation.

In addition to removable media, the Trust acknowledges the availability of cloud storage, personal device storage and online resources that may enable data to be stored, copied, uploaded or transferred outside approved corporate systems. These methods are not permitted unless expressly authorised, documented and approved by the Trust's Data Protection Officer or authorised Information Governance route.

The use of cameras, mobile devices, or recording equipment within NHIS or client environments is strictly controlled to protect the confidentiality, dignity, and safety of patients, staff and visitors.

Photography, filming, or audio recording is prohibited unless there is a clearly defined and authorised purpose, appropriate consent has been obtained where required, and the activity has been approved in line with NHIS and Trust governance processes.

Unauthorised recording of any individual, including incidental capture in the background, is strictly prohibited and will be treated as a breach of confidentiality and managed in accordance with incident management and disciplinary procedures.

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

Policy Compliance

If any user is found to have breached this policy, they may be subject to Trust disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the investigation or prosecution of the offender or offenders.

If you do not understand the implications of this policy or how it applies to you, you must seek advice from the Information Governance Team.

Review and Revision

This policy will be reviewed every 2 years or sooner if required. Policy review will be undertaken by the Cyber Security Assurance Delivery Group

7.0 MONITORING COMPLIANCE AND EFFECTIVENESS

Minimum Requirement to be Monitored **(WHAT – element of compliance or effectiveness within the document will be monitored)**	**Responsible Individual** **(WHO – is going to monitor this element)**	**Process for Monitoring e.g. Audit** **(HOW – will this element be monitored (method used))**	**Frequency of Monitoring** **(WHEN – will this element be monitored (frequency/ how often))**	**Responsible Individual or Committee/ Group for Review of Results** **(WHERE – Which individual/ committee or group will this be reported to, in what format (e.g verbal, formal report etc) and by who)**
Compliance with data leakage prevention controls, including approved exceptions, use of authorised removable media, incident trends and any attempted circumvention of technical controls	Data Protection and Cyber Security Committee	NHIS reporting, Information Governance review, incident reporting trends, exception records and review of approved whitelisted removable media devices.	Quarterly, or more frequently where incident trends or risk indicators require escalation.	Information Governance Working Group and Data Protection and Cyber Security Committee, with onward escalation in line with Trust governance arrangements where required

8.0 TRAINING AND IMPLEMENTATION

Annual data security awareness level 1 (formally known as Information Governance) training is mandatory for all new starters as part of the induction process. In addition all existing staff must undertake data security awareness level 1 training on an annual basis. Staff can undertake this either face-to-face[2] or online. Provision is available online (or face to face for staff who do not have routine access to personal data) and includes Data Protection and confidentiality issues.

Data security awareness level 1 session meets the statutory and mandatory training requirements and learning outcomes for Information Governance in the UK Core Skills Training Framework (UK CSTF) as updated in May 2018 to include General Data Protection Regulations (GDPR).

Our Senior Information Risk Owner, Information Asset Owners and Information Asset Administrators must attend regular information risk awareness training which is available from the Information Governance team.

Implementation of this policy will be supported through staff communications, mandatory Information Governance and Security training, local management oversight and clear expectations for staff behaviour. Staff must understand the risks associated with removable media, personal devices, cloud services, messaging platforms, photography and recording, and must seek advice before moving, copying, storing or sharing Trust information outside approved systems.

9.0 IMPACT ASSESSMENTS

- This document has been subject to an Equality Impact Assessment, see completed form at Appendix 1
- This document has been subject to an Environmental Impact Assessment, see completed form at Appendix 2.

10.0 EVIDENCE BASE (Relevant Legislation/ National Guidance) AND RELATED SFHFT DOCUMENTS

Evidence Base:

- Data Protection Act 2018
- UK General Data Protection Regulation, including the integrity and confidentiality security principle and security of processing requirements
- Common Law Duty of Confidentiality
- Caldicott Principles
- NHS Data Security and Protection Toolkit requirements, including the National Data Guardian's Data Security Standards
- Network and Information Systems Regulations 2018, where applicable to essential services and supporting network and information systems
- ISO/IEC 27001:2022, including control A.7.10 Storage media

[2] https://sfhcoursebooking.nnotts.nhs.uk/default.aspx (internal web link)

- NHS and national cyber security guidance relevant to information security, incident reporting, secure handling of information and protection of network and information systems

Related SFHFT Documents:

- Data Protection, Confidentiality and Disclosure Policy
- Information Security Policy
- Information Governance Policy
- Information Risk Management Policy
- Remote Working Policy
- Email and Internet Acceptable Use Policy
- Incident Reporting Policy
- Risk Management Policy
- Records Management Policy
- Third Party Access Procedure or third party device connection agreement
- Relevant NHIS cyber security, service request and technical control processes for removable media access, whitelisting and secure disposal.

11.0 KEYWORDS

Data leakage prevention, data loss prevention, removable media, USB, memory stick, flash drive, external hard drive, encrypted removable media, cloud storage, personal devices, mobile devices, photography, recording, artificial intelligence tools, data transfer, information sharing, unauthorised disclosure, information security, cyber security, confidentiality, whitelisting, secure disposal, malware.

12.0 APPENDICES

- Equality Impact Assessment
- Environmental Impact Assessment
- Staff guidance: Data leakage prevention and removable media

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

EIA Form Stage One:

Name EIA Assessor: Gina Robinson		**Date of EIA completion:** 3rd July 2026	
Department: IG		**Division:** Corporate	
Name of service/policy/procedure being reviewed or created: Data Leakage Prevention and Removable Media Policy			
Name of person responsible for service/policy/procedure: Existing			
Brief summary of policy, procedure or service being assessed: This policy sets out requirements for preventing data leakage and controlling the use of removable media to protect Trust information and support compliance with information governance and cyber security standards.			
Please state who this policy will affect: Patients or Service Users, Carers or families, Commissioned Services, Communities in placed based settings, Staff, Stakeholder organisations.			
Protected Characteristic	**Considering data and supporting information, could protected characteristic groups' face negative impact, barriers, or discrimination? For example, are there any known health inequality or access issues to consider? (Yes or No)**	**Please describe what is contained within the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening. Please also provide a brief summary of what data or supporting information was considered to measure/decipher any impact.**	
Race and Ethnicity	None	Not applicable	None
Sex **Gender**	None	Not applicable	None
Age	None	Not applicable	None
Religion and Belief	None	Not applicable	None
Disability	Visual accessibility of this policy	Already in Arial font size 12. Use of technology by end user. This policy can be made available in alternative formats, such as easy read or large print, and may	None

		be available in alternative languages, upon request	
Sexuality	None	Not applicable	None
Pregnancy and Maternity	None	Not applicable	None
Gender Reassignment	None	Not applicable	None
Marriage and Civil Partnership	None	Not applicable	None
Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation)	None	Not applicable	None

What consultation with protected characteristic groups including patient groups have you carried out?

- None

What data or information did you use in support of this EqIA?

- Trust guidance for completion of the Equality Impact Assessments.

As far as you are aware are there any Human Rights issues be taken into account such as arising from surveys, questionnaires, comments, concerns, complaints or compliments?

- No

Level of impact

Low Level of Impact

Name of Responsible Person undertaking this assessment: G Robinson

Signature: G Robinson

Date: 3rd July 2026

Marriage and Civil Partnership	None	Not applicable
Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation)	None	

If you have answered 'yes' to any of the above, please complete Stage 2 of the EIA.

What consultation with protected characteristic groups including patient groups have you carried out?

Information Governance Working Group

As far as you are aware are there any Human Rights issues be taken into account such as arising from surveys, questionnaires, comments, concerns, complaints or compliments? Yes

On the basis of the information/evidence/consideration so far, do you believe that the policy / practice / service / other will have a positive or negative adverse impact on equality? (delete as appropriate)

Positive			Negative			
		Low				

If you identified positive impact, please outline the details here: This policy is expected to have a low positive impact on equality by supporting consistent protection of patient, staff and organisational information, including personal and confidential information. No adverse impact on protected characteristic groups has been identified. The policy is available in an accessible format and can be provided in alternative formats or languages on request.

Protected Characteristic	Please explain, using examples of evidence and data, what the impact of the Policy, Procedure or Service/Clinical Guideline will be on the protected characteristic group.	Please outline any further actions to be taken to address and mitigate or remove any in barriers that have been identified.
Race and Ethnicity	No specific adverse impact identified. The policy applies consistently to all staff and supports protection of confidential information for all patients, staff and service users.	No further action required. Policy can be made available in alternative languages on request.
Gender	No specific adverse impact identified. The policy applies equally to all staff and service users.	No further action required
Age	No specific adverse impact identified. The policy supports consistent handling and protection of information for all age groups.	No further action required.
Religion	No specific adverse impact identified. The policy does not affect access to services or treatment on the basis of religion or belief.	No further action required.
Disability	A potential accessibility consideration has been identified in relation to access to the policy document. This is mitigated by the use of Arial 12 font and availability in alternative formats on request.	Ensure alternative formats, such as large print or easy read, are provided on request.
Sexuality	No specific adverse impact identified. The policy applies consistently and supports confidentiality for all individuals.	No further action required.
Pregnancy and Maternity	No specific adverse impact identified. The policy does not create different requirements for staff or service users on the basis of pregnancy or maternity.	No further action required.
Gender Reassignment	No specific adverse impact identified. The policy supports confidentiality and secure handling of personal information for all individuals.	No further action required.
Marriage and Civil Partnership	No specific adverse impact identified. The policy applies consistently to all individuals regardless of marital or civil partnership status.	No further action required.
Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation)	No specific adverse impact identified. The policy does not create barriers linked to deprivation or socio-economic status.	No further action required.

EIA Form Stage Two:

Signature: G Robinson *I can confirm I have read the Trust's Guidance document on Equality Impact Assessments prior to completing this form*
Date: 3rd July 2026

Please send the complete EIA form to the People EDI Team for review. **Please send the form to: sfh-tr.edisupport@nhs.net**

APPENDIX 2 – ENVIRONMENTAL IMPACT ASSESSMENT

The purpose of an environmental impact assessment is to identify the environmental impact, assess the significance of the consequences and, if required, reduce and mitigate the effect by either, a) amend the policy b) implement mitigating actions.

Area of impact	Environmental Risk/Impacts to consider	Yes/No	Action Taken (where necessary)
Waste and materials	• Is the policy encouraging using more materials/supplies? • Is the policy likely to increase the waste produced? • Does the policy fail to utilise opportunities for introduction/replacement of materials that can be recycled?	No	
Soil/Land	• Is the policy likely to promote the use of substances dangerous to the land if released? (e.g. lubricants, liquid chemicals) • Does the policy fail to consider the need to provide adequate containment for these substances? (For example bunded containers, etc.)	No	
Water	• Is the policy likely to result in an increase of water usage? (estimate quantities) • Is the policy likely to result in water being polluted? (e.g. dangerous chemicals being introduced in the water) • Does the policy fail to include a mitigating procedure? (e.g. modify procedure to prevent water from being polluted; polluted water containment for adequate disposal)	No	
Air	• Is the policy likely to result in the introduction of procedures and equipment with resulting emissions to air? (For example use of a furnaces; combustion of fuels, emission or particles to the atmosphere, etc.) • Does the policy fail to include a procedure to mitigate the effects? • Does the policy fail to require compliance with the limits of emission imposed by the relevant regulations?	No	
Energy	• Does the policy result in an increase in energy consumption levels in the Trust? (estimate quantities)	No	
Nuisances	• Would the policy result in the creation of nuisances such as noise or odour (for staff, patients, visitors, neighbours and other relevant stakeholders)?	No	

APPENDIX 3 - STAFF GUIDANCE: DATA LEAKAGE PREVENTION AND REMOVABLE MEDIA

Why this guidance matters

Protecting patient, staff and organisational information is everyone's responsibility. Data leakage, whether accidental or deliberate, can result in harm to patients, loss of public trust, regulatory action, legal consequences and reputational damage.

This guidance explains the practical steps staff must take to keep Trust information within approved systems and to prevent unauthorised removal, copying, transfer, disclosure or storage of information.

What is data leakage?

Data leakage means information being removed, disclosed, copied, transferred, photographed, recorded, uploaded, stored or shared outside approved corporate systems or processes without authorisation.

Examples include:

- copying information to a personal device;
- saving information to personal or non-approved cloud storage;
- emailing information to a personal email account;
- sharing information through non-approved messaging apps;
- photographing screens, documents or records;
- recording conversations or meetings without approval;
- uploading information to non-approved artificial intelligence tools;
- printing or leaving paper records where they can be accessed by unauthorised people; and
- storing or transferring information on removable media without approval.

Why this guidance matters

Protecting patient, staff and organisational information is everyone's responsibility. Data leakage, whether accidental or deliberate, can result in harm to patients, loss of public trust, regulatory action, legal consequences and reputational damage.

This guidance explains the practical steps staff must take to keep Trust information within approved systems and to prevent unauthorised removal, copying, transfer, disclosure or storage of information.

What is data leakage?

Data leakage means information being removed, disclosed, copied, transferred, photographed, recorded, uploaded, stored or shared outside approved corporate systems or processes without authorisation.

Examples include:

- copying information to a personal device;
- saving information to personal or non-approved cloud storage;
- emailing information to a personal email account;

- sharing information through non-approved messaging apps;
- photographing screens, documents or records;
- recording conversations or meetings without approval;
- uploading information to non-approved artificial intelligence tools;

printing or leaving paper records where they can be accessed by unauthorised people; and storing or transferring information on removable media without approval.

Key rule: keep information in approved systems

Staff must keep Trust information within approved corporate systems wherever possible. Information must not be moved, copied, stored, photographed, recorded, uploaded or shared outside approved systems unless this has been formally authorised.

If in doubt, do not move, copy, photograph, record, upload or share the information. Seek advice first.

What staff must do

Staff must:

- access only the information they need for an authorised purpose;
- use approved Trust or NHIS systems for storing, accessing and sharing information;
- use approved information exchange routes wherever possible;
- seek approval before using removable media;
- ensure any approved removable media is encrypted and technically authorised;
- protect any approved removable media from loss, theft, damage or unauthorised access;
- report damaged, lost, stolen or suspected compromised removable media immediately;
- report any actual or suspected data leakage incident immediately through Datix and to the Information Governance team; and
- seek advice from their line manager, Information Governance or NHIS where they are unsure.

What staff must not do

Staff must not:

- use personal devices to store, copy or transfer Trust information;
- copy information to personal cloud storage or non-approved online accounts;
- email Trust information to personal email accounts;
- use personal messaging apps to share Trust information;
- upload Trust information to non-approved artificial intelligence tools;
- photograph or record screens, documents, systems, patients, staff or visitors without authorisation;
- use removable media unless it has been approved;
- use non-Trust owned removable media for Trust information;
- attempt to bypass or disable technical security controls;
- leave paper records or removable media unattended or insecure; or
- try to access files on removable media that they have found or that has not been approved.

Removable media approvals

The use of removable media is prohibited by default. It may only be used where:

- there is a documented and proportionate business need;
- approved corporate systems or approved information exchange routes are not suitable;
- approval has been obtained from the relevant line manager;
- Information Governance has reviewed and approved the request;
- NHIS has confirmed that appropriate technical and cyber security controls can be applied;
- Information Asset Owner approval has been obtained where applicable; and
- the device or access has been recorded on the relevant approved whitelist or technical control register**.**

Only approved encrypted removable media may be used unless a specific documented exception has been approved.

If something goes wrong

Staff must report any actual or suspected incident immediately.

This includes:

- loss or theft of removable media;
- use of unauthorised removable media;
- information sent to the wrong recipient;
- information copied or uploaded to a non-approved system;
- photographs or recordings taken without approval;
- suspected malware or virus infection;
- attempts to bypass technical controls; or
- any unauthorised access, disclosure, transfer or loss of information.

Incidents must be reported through Datix and to the Information Governance team. Staff must not attempt to conceal, delete or resolve the issue without advice.

Consequences of non-compliance

Failure to follow this policy may result in investigation under incident management procedures, disciplinary action, regulatory consequences, legal action or professional consequences where applicable.

Where to go for advice

If staff are unsure what to do, they must seek advice before taking action.

Advice is available from:

- line managers;
- the Information Governance team;
- NHIS ServiceDesk; and
- the relevant Information Asset Owner, where applicable.

Simple reminder

Use approved systems only.
Access only what you need.
Do not move, copy, photograph, record, upload or share information without approval.
Do not use personal devices or personal cloud storage for Trust information.
Ask before acting if you are unsure.