Healthier Communities, Outstanding Care

NHS
Sherwood Forest Hospitals
NHS Foundation Trust

# REMOVABLE MEDIA POLICY

<table>
<tr><td colspan="2"></td><td colspan="3"><b>POLICY</b></td></tr>
<tr><td><b>Reference</b></td><td colspan="4">IG/005</td></tr>
<tr><td><b>Approving Body</b></td><td colspan="4">Cyber Security Assurance Programme Board</td></tr>
<tr><td><b>Date Approved</b></td><td colspan="4">29th September 2022</td></tr>
<tr><td rowspan="3"><b>For publication to external SFH website</b></td><td colspan="4"><b>Positive confirmation received from the approving body that the content does not risk the safety of patients or the public:</b></td></tr>
<tr><td><b>YES</b></td><td colspan="2"><b>NO</b></td><td><b>N/A</b></td></tr>
<tr><td>x</td><td colspan="2"></td><td></td></tr>
<tr><td><b>Issue Date</b></td><td colspan="4">October 2022</td></tr>
<tr><td><b>Version</b></td><td colspan="4">3</td></tr>
<tr><td><b>Summary of Changes from Previous Version</b></td><td colspan="4">Review – minor changes to formatting<br>References added on approvals process and references to Cyber Security Assurance Programme Board</td></tr>
<tr><td><b>Supersedes</b></td><td colspan="4">Version 2</td></tr>
<tr><td><b>Document Category</b></td><td colspan="4">Information Governance</td></tr>
<tr><td><b>Consultation Undertaken</b></td><td colspan="4">The Policy has been reviewed and developed by the Cyber Security Assurance Delivery Group and approved by the Programme Board with representation from:<br>• Nottingham and Nottinghamshire Clinical Commissioning Group<br>• Sherwood Forest Hospitals NHS Foundation Trust<br>• Nottingham CityCare Partnership<br>• Nottinghamshire Health Informatics Service</td></tr>
<tr><td><b>Date of Completion of Equality Impact Assessment</b></td><td colspan="4">13th April 2022</td></tr>
<tr><td><b>Date of Environmental Impact Assessment (if applicable)</b></td><td colspan="4">13th April 2022</td></tr>
<tr><td><b>Legal and/or Accreditation Implications</b></td><td colspan="4">Data Protection Legislation</td></tr>
<tr><td><b>Target Audience</b></td><td colspan="4">All staff and visitors</td></tr>
<tr><td><b>Review Date</b></td><td colspan="4">29th September 2024</td></tr>
<tr><td><b>Sponsor (Position)</b></td><td colspan="4">Cyber Security Assurance Programme</td></tr>
<tr><td><b>Author (Position &amp; Name)</b></td><td colspan="4">Cyber Security Assurance Delivery Group</td></tr>
<tr><td><b>Lead Division/ Directorate</b></td><td colspan="4">Corporate</td></tr>
<tr><td><b>Lead Specialty/ Service/ Department</b></td><td colspan="4">Information Governance/ Information Security</td></tr>
</table>

| | |
|---|---|
| **Position of Person able to provide Further Guidance/Information** | Cyber Security Assurance Programme<br>Local Information Governance Lead |
| **Associated Documents/ Information** | **Date Associated Documents/ Information was reviewed** |
| 1. Data Protection, Confidentiality and Disclosure Policy | 11th March 2020 |
| 2. Remote Working Policy | 11th March 2020 |
| 3. Email and Internet Policy | 30th July 2021 |
| 4. Information Security Policy | 11th March 2020 |
| Template control | June 2020 |

## CONTENTS

## APPENDICIES

## 1.0 INTRODUCTION

The 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.

This policy aims to ensure that the use of removable media devices is controlled 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 computer 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.

## 2.0 POLICY STATEMENT

This document has been developed as part of the Nottinghamshire Health Informatics Service (NHIS) and partner commitments to maintaining a secure network as part of the Cyber Security Assurance Programme.

The Policy has been reviewed and developed by:

- Nottingham and Nottinghamshire Integrated Care Board
- Sherwood Forest Hospitals NHS Foundation Trust
- Nottingham CityCare Partnership

All partners are committing to the principles of the policy and protection of the shared network through management of removable media. The Trust will ensure the controlled use of removable media devices to store and transfer information by all users who have access to information, information systems and IT equipment for the purposes of conducting official business.

## 3.0 DEFINITIONS/ ABBREVIATIONS

This policy should be adhered to at all times, but specifically whenever any user intends to store any information used by the Trust to conduct official business on removable media devices.

Removable media devices include, but are not restricted to the following [this list is not exhaustive and further advice can be obtained from the NHIS cyber security team] :

- 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).

## 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 and then approved by the CSA Programme Board**.**

### Trust Board

The Board has the Individual Officer arrangements in place to ensure that requirements are carried out effectively.

### Information Governance (IGC) Committee

The Committee is responsible for ensuring that this policy is implemented, including:

- Providing management direction and support for removable media activities in accordance with business requirements

- Ensuring additional guidance and training deemed necessary to support removable media activities are implemented

- It will monitor and provide Board assurance in this respect.

The Committee reports to the Risk Committee.

### Individual Officers

The Director of Corporate Affairs, in their role as Senior Information Risk Owner (SIRO) is to take ownership of the organisation's information risk and act as an advocate for information risk on the Board, assisted by the Information Governance department.

Line Managers will be responsible for implementing and maintaining the policy in their area of management, including ensuring that procedures are in place and staff have adequate access to information security training.

Information Asset Administrators (IAAs) have day to day responsibility for managing security aspects of their particular assets.

Information Asset Owners will review the security of information systems and removable media on a regular basis, and this will be subject to internal audit as set out in organisational IAO framework.

All members of staff should read and note the contents of this policy and must have access to and conscientiously follow the guidance outlined in their local policies and procedures.

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). An outline of the Caldicott Principles can be found in Appendix 3.

All staff are responsible for minimising the risk that an actual or potential security breache occurs as a direct result of their actions.

The Trust will investigate all suspected/actual security breaches and report through their incident reporting procedures.

## 5.0 APPROVAL

Approval of the Policy will be through the Cyber Security Assurance Programme Board, with appropriate consultation through relevant Trust officers and the Information Governance Working Group. The Information Governance Committee will formally accept the Policy for the Trust and ensure that Trust Staff are aware of the principles of the Policy.

## 6.0 DOCUMENT REQUIREMENTS

### Risks

The Trust recognises that there are risks associated with users accessing and handling information in order to conduct official Trust business. Information is used throughout Trust and sometimes shared with external organisations and applicants.

Securing personal confidential or sensitive data is of paramount importance – particularly in relation to the Trusts need to protect data in line with the requirements of the Data Protection Legislation (Data Protection, Confidentiality & Disclosure Policy).Any loss of the ability to access information or interference with its integrity could have a significant effect on the efficient operation of Trust. It is therefore essential for the continued operation of Trust that the confidentiality, integrity and availability of all information recording systems are maintained at a level, which is appropriate to the Trust's needs.

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 be stored on corporate systems and exchanged using appropriately protected and approved information exchange connections

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 Trust 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 Trust or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the Trust or individuals as a result of information loss or misuse.
- Trust reputational damage as a result of information loss or misuse.

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

## Applying the Policy

### Restricted Access to Removable Media

It is Trust policy to prohibit the use of all removable media devices. The use of removable media devices will only be approved if a valid business case for its use is developed. There are large risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks must be demonstrated before approval is given.

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 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 Trust **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.

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.

**Where 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 usedto access their systems.

### Procurement of Removable Media

All removable media devices and any associated equipment and software must only be purchased and installed by NHIS.

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

The only equipment and media that should be used to connect to Trust equipment or the NHIS network is equipment and media that has been purchased by NHIS or approved Trust procurement routes and approved by the IAO or has been sanctioned for use by Information Governance.

### Security of Data

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 Trust 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.  For further information please see Remote Working Policy.

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.

**Incident Management**

It is the duty of all users to immediately report any actual or suspected breaches in information security via the Datix system or via the information governance team. All incidents will be investigated as outlined in the Incident Reporting 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.

**Third Party Access to Trust Information**

No third party (external contractors, partners, agents, and the public or non-employee parties) may receive data or extract information from the Trust'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 Trust 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.

**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 Trust, other organisations or individuals from the data being lost whilst in transit or storage.

## 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 Servicedesk on 4040.

## User Responsibility

All considerations of this policy must be adhered to at all times when using all types of removable media devices. 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 Trust equipment or the network or to hold information used to conduct official Trust 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.

## 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 prosecution of the offender(s).

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

## Review and Revision

This policy will be reviewed biannually. Policy review will be undertaken by the Cyber Security Assurance Delivery Group

## 7.0 MONITORING COMPLIANCE AND EFFECTIVENESS

| **Minimum Requirement to be Monitored**<br>**(WHAT – element of compliance or effectiveness within the document will be monitored)** | **Responsible Individual**<br>**(WHO – is going to monitor this element)** | **Process for Monitoring e.g. Audit**<br>**(HOW – will this element be monitored (method used))** | **Frequency of Monitoring**<br>**(WHEN – will this element be monitored (frequency/ how often))** | **Responsible Individual or Committee/ Group for Review of Results**<br>**(WHERE – Which individual/ committee or group will this be reported to, in what format (eg verbal, formal report etc) and by who)** |
|---|---|---|---|---|
| Removable media | IG Team | Report from NHIS | Quarterly | IG Committee |

## 8.0 TRAINING AND IMPLEMENTATION

The policy will be circulated via the staff bulletin and will be uploaded to the Trust's website and intranet.

There is no specific training associated with this policy, however all staff should complete mandatory Information Governance and Security training.

## 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 Legislation
- Caldicott Principles

**Related SFHFT Documents:**

- Data Protection Confidentiality and Disclosure Policy
- Remote Working Policy
- Risk Management Policy
- Email and Internet Policy
- Information Security Policy
- 3rd Party device connection agreement

## 11.0 KEYWORDS

Memory stick, flash drive, ports.

## 12.0 APPENDICES

- Equality Impact Assessment
- Environmental Impact Assessment
- Caldicott Principles
- Approval Form for Removable Media

## APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

| | | | |
|---|---|---|---|
| **Name of service/policy/procedure being reviewed: Removable Media Policy** | | | |
| **New or existing service/policy/procedure: Existing** | | | |
| **Date of Assessment: 13th April 2022** | | | |
| **For the service/policy/procedure and its implementation answer the questions a – c below against each characteristic (if relevant consider breaking the policy or implementation down into areas)** | | | |
| **Protected Characteristic** | **a) Using data and supporting information, what issues, needs or barriers could the protected characteristic groups' experience? For example, are there any known health inequality or access issues to consider?** | **b) What is already in place in the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening?** | **c) Please state any barriers that still need to be addressed and any proposed actions to eliminate inequality** |
| **The area of policy or its implementation being assessed:** | | | |
| **Race and Ethnicity** | None | Not applicable | None |
| **Gender** | None | Not applicable | None |
| **Age** | None | Not applicable | None |
| **Religion** | 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 be available in alternative languages, upon request | None |
| **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?**<br>• None | | | |
| **What data or information did you use in support of this EqIA?**<br>• 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?**<br>• No | | | |
| **Level of impact**<br>Low Level of Impact | | | |
| **Name of Responsible Person undertaking this assessment: Information Security Officer** | | | |
| **Signature: Information Security Officer** | | | |
| **Date: 13th April 2022** | | | |

## 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?<br>• Is the policy likely to increase the waste produced?<br>• 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)<br>• 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)<br>• Is the policy likely to result in water being polluted? (e.g. dangerous chemicals being introduced in the water)<br>• 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.)<br>• Does the policy fail to include a procedure to mitigate the effects?<br>• 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 – Caldicott Principles

**Principle 1 - Justify the purpose(s) for using confidential information**
Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

**Principle 2 - Don't use personal confidential data unless it is absolutely necessary**
Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

**Principle 3 - Use the minimum necessary personal confidential data**
Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

**Principle 4 - Access to personal confidential data should be on a strict need-to-know basis**
Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

**Principle 5 - Everyone with access to personal confidential data should be aware of their responsibilities**
Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

**Principle 6 - Comply with the law**
Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

**Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality**
Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

**Principle 8** - A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

## APPENDIX 4 - 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.