UNIVERSITY OF HULL

Removable Media Policy

Classification:	Policy
Version Number:	1-00
Status:	Published
Approved by (Board):	University Leadership Team
Approval Date:	30 January 2018
Effective from:	30 January 2018
Next Review Date:	30 January 2019
Document Authors:	Service Assurance, ICT (D. Chambers, S. Doyle, S. Jones)
Document Owner:	Head of Service Assurance, ICT (Stewart Doyle)
Department/Contact:	help@hull.ac.uk
Summary:	This policy outlines the organisational responsibilities and controls around the use of removable media within the University.
Scope:	This policy applies to all University members
Collaborative provision:	Not mandatory
Assessment: (where relevant)	Not applicable
Consultation: (where relevant)	Not applicable
Relevant legal frameworks:	See relevant section of overarching Information Governance and Assurance Policy
Related documents:	Information Governance and Assurance Policy
Published locations:	Public website (www.hull.ac.uk) and SharePoint (share.hull.ac.uk)
Document Communication and Implementation Plan:	Available upon request.

All printed versions of this document are classified as uncontrolled.
A controlled version is available from the university website.

This policy outlines the organisational responsibilities and controls around the use of removable media within the University

Removable Media Policy

1. Introduction

1.1. Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. In the normal course of business, it should not be necessary to use removable media, and the risk of doing so usually outweighs any perceived benefit.

1.2. Removable media is very easily lost, which can, and does, result in the compromise of large volumes of information. The loss of media can result in significant reputational damage, even if there is no evidence of what exactly has been lost.

1.3. Removable media that is used to transfer information from one machine to another, for example a University PC to one at home, can be utilised by attackers to transport malicious software from one environment to the other.

2. Purpose

2.1. This policy is intended to outline organisational responsibilities and controls around the use of removable media. Removable media refers to any type of computer storage that is not physically fixed inside a computer. This includes, but is not limited to:

- USB flash drives (aka USB sticks, USB pens, memory sticks)
- External hard disk drives, including “internal” drives used via a “dock”
- Mobile devices used as external storage (e.g. smartphones)
- Optical media (e.g. DVD, CD)

2.2. This policy supports the objectives of the overarching Information Security Controls policy and sub-policies, as well as the Data Protection and Information Governance and Assurance policies.

3. Scope

3.1. This policy covers all devices used to conduct University related business, and any removable media used with those devices.

3.2. This policy applies to all University members, third parties and visitors using University computer equipment.

3.3. For the purposes of this policy, “University data” refers to any data owned or licensed by the University that if disclosed publicly without authorisation, could result in financial, commercial or reputational damage and/or legal proceedings.

4. Policy

4.1. The use of removable media within the University is not prohibited, but should only be used in cases where no suitable alternative exists (e.g. sanctioned network shares/cloud storage).

4.2. Managers and information asset owners shall ensure that use of removable media is suitably controlled within their area of responsibility in line with the objectives of this policy.

4.3. Managers and information asset owners reserve the right to request that technical controls be implemented to prevent the use of removable media in certain circumstances.

4.4. University staff members within professional services electing to use removable media, shall be responsible for ensuring they are authorised to do so within their area.

4.5. Any removable media used to transport or store any University data should be purchased via approved channels.

4.6. Personally owned removable media shall not be used for the purposes of transporting or storing University data.

4.7. Removable media used for storage of University data should be either hardware encrypted or employ the use of encrypted containers.

4.8. Guidance on encryption including recommended hardware and software should be available to colleagues.

4.9. Researchers are responsible for ensuring that use of removable media and the encryption of any such media meets the requirements imposed upon them by their research (e.g. by funders, or data sharing agreements).

4.10. When the removable media has reached the end of its useful life it should be submitted for secure destruction via the corresponding ICT processes.

4.11. Use of removable media by a third party or sub-contractor should be risk-assessed and authorised, and in accordance with University Data Protection Policy governing third-party access to data.