Information Security for Portable and Removable Media Devices Policy

Version:	**4.0**
Dated:	**26 June 2020**
Document Owner:	**Head of IT Security and Compliance**

Document History and Reviews

Version	Date	Revision Author	Summary of Changes
0.1	May 2018	Ali Mitchell	Change of policy title and transferred to a new template. Added in process for lost and found removable devices.
0.2	May 2018	Ali Mitchell	Added in Lost and Found report form
0.3	May 2018	Ali Mitchell	Minor changes made from peer feedback
1	May 2018	Ali Mitchell	Approved Version
1.1	July 2019	Ali Mitchell	Amendment to paragraphs 1.1, 2.3 and 6.2 Removed paragraph 3.2
2	Sept 2019	Ali Mitchell	Version 2 sent for IGSSG approval
3	Sept 2019	Ali Mitchell	Added in bullet point 5.3
3.1	March 2020	Ali Mitchell	Removed related policies from para 2.3 and created new section 8. Added Encryption policy to the list. Changed list of reviewers
3.2	June 2020	Ali Mitchell	Added in paragraph 9. Para 5.2 updated to reflect comments raised at ISG.

Review Distribution

Name	Title
Brenda Waterman	Information Governance Manager and DPO
Ira Goel	IT Risk and Compliance Manager
Martyn Goldsborough	Information Security Manager
Mike Maling	Operations and Security Manager
Simon Hallett	Security Architect

Approval

Versions	Position	Approval Date
1	Members of the IGSSG	May 2018
2	Members of the IGSSG	Sept 2019
3	Members of the IGSSG	Oct 2019
4	ISG members	1 July 2020

Contents

1. Introduction

1.1 On 25 May 2018, the Data Protection Act was replaced with the General Data Protection Regulations (GDPR) which saw the biggest shake up on Data Protection legislation for some time. The GDPR gives individual's more say about how their data is collected, used, protected and controlled as well the right to being forgotten. Any non-compliance with the GDPR could result in significant fines being imposed, damage to University's reputation and the potential for great distress to individual's should their personal data be compromised.

1.2 The University takes data protection extremely seriously and is mandated to conform to the controls required to protect individual's data. Additionally, the University also has other important and valuable data; sometimes collectively referred to as Intellectual Property (IP). It is therefore important that measures are taken to protect the University's and individual's data.

1.3 Due to the nature of portable and removable media devices and the way they are used; they are susceptible to being lost. This means there is a danger of the loss of sensitive data, compromise of the University's IP and the delivery and propagation of malware; including ransomware, viruses etc. Whilst impacts around these risks can vary widely it worth highlighting that malware attacks have significantly increased with ransomware becoming a preferred tool for hacktivists.

2. Purpose

2.1 This policy has been produced to help the University mitigate the risks associated with the use of portable and removable media devices. As such, this policy defines the standards, procedures, and restrictions for users who have legitimate business requirements to connect portable and removable media devices to any infrastructure within the University's internal network(s) or related technology resources. It also outlines users' responsibilities around the use of portable and removable media devices including what actions to take if such items are misplaced.

2.2 This policy is intended to ensure that any information used or accessed by staff is protected against unauthorised access or modification when stored or accessed on any portable device or medium. There can be no absolute guarantees where security is concerned but overall the standard required is that such information must not be 'readily accessible' by any unauthorised person or persons.

2.3 Staff must take personal responsibility for adhering to this policy and should treat University information with (at least) the same care that they would expect to be applied to any personal or confidential information held about them.

3. Scope

3.1 This policy applies to all staff working for, or on behalf of, the University and includes direct employees, contractors, agency workers, associates or other third parties with legitimate access to University data. It includes both University supplied portable and removable devices and personal items used for University business.

3.2 Note that this policy is designed to provide an adequate level of confidentiality of data for most users. If 'military grade' security is required for specific projects or activities then

users for whom this is a requirement may need to implement additional security to the standard required by the parties with whom they are working. In such cases, please log the details with the SID.

3.3 When referred to within this policy, portable devices and removable mediums include:

- Laptop computer, notebook computer, netbook, etc.
- PDA
- Tablet
- Smart Watches
- Phone, smartphone, MP3 player or other communications / audio / video device with data storage or data access capability
- All portable computer devices typically running one or more of Windows, MacOS, Unix / Linux. Other types of mobile device will be covered by other policies available from the IT webpages
- CD, DVD, floppy disk, tape, zip disk, etc.
- External hard disk
- USB memory stick
- Solid-state or other storage card (e.g. CompactFlash, SD, other new digital storage, etc.)

4. Risks to the University

4.1 As briefly highlighted in paragraph 1.3, the use of portable and removable media devices can expose the University to many risks. Whilst it is recognised that there are many benefits of using these devices; there needs to be an element of caution and control, to prevent risks such as:

- **Loss of information**

  The physical design of removable media can result in it being misplaced or stolen, potentially compromising the confidentiality and availability of the information stored on it. Which could lead to a risk to the safety, dignity and wellbeing of data subjects.

- **Introduction of malware**

  The uncontrolled use of removable media will increase the risk from malware if the media can be used on multiple ICT systems.

- **Information leakage**

  Some media types retain information after user deletion; this could lead to an unauthorised transfer of information between systems or an undesired recovery of the information by a third party.

- **Reputational damage**

  A loss of sensitive information often attracts media attention which could erode customer confidence in the business and impact upon the University's reputation.

- **Financial loss**

  If sensitive information is lost or compromised the organisation would be subjected to considerable financial penalties.

5. Portable Devices Policy

5.1 Unless absolutely critical, personal devices must not hold any information that is sensitive, personal, confidential or of commercial value.

5.2 Where possible, all devices used for University business must have full disk encryption and in line with the University's specification.

5.3 Ideally University supplied devices should not be used for personal use as this increases the risk of introducing malware onto the IT network.

5.4 All devices must be kept secure by the employee, contractor etc. responsible for them. When unattended, devices should be kept in a locked area (e.g. a locked room or cabinet).

5.5 Portable devices such as laptops or tablets etc. are highly desirable items with many being stolen from vehicles or by being left in places.

5.6 When travelling with a laptop it is better to use a rucksack instead of a conventional laptop bag. You should never leave your laptop or portable device in view in a vehicle, it is better to keep it in the boot or hidden and it is recommended that you do not leave it for periods longer than 15 minutes.

5.7 Please ensure that you do not have any passwords for the devices written down and/or stored with it.

5.8 If your portable device (University supplied or personal device) is stolen you must report it to the SID without delay so we can assess whether a data breach has occurred.

6. Removable Media Policy

6.1 No personal, sensitive or confidential information shall be stored on any non-University supplied removable media devices except as explicitly provided for in contracts with third parties providing goods or services to the University.

6.2 University supplied devices should not be used to store personal items as this increases the risk of introducing malware onto the IT network.

6.3 Removable media devices can only store personal, sensitive or confidential information when at least one of the following conditions is met:

- The storage medium is encrypted to relevant industry standards, for example, Advanced Encryption Standard (AES) 256.

- Unencrypted portable medium are used only in a single location, not transported and are kept securely locked away at all times when not in use. (Note that such activity carries some inherent risk of loss or breach of confidentiality of the data so anyone working in this way must be made aware of the dangers.)

- An alternative stronger level of protection is in place if required by other agencies. Note that, owing to the risk of user error, we do not recommend the use of an unencrypted storage medium where confidential, personal or sensitive information is stored in encrypted folders or files.

7. Lost and Found Portable and Removable Media Devices

7.1 The GDPR specifies that any data breaches must be reported to the Information Commissioners Office (ICO) within 72 hours once discovered or reported. It is therefore important, that you report any lost devices or compromises to personal data as soon as possible. In the first instance this should be reported through the SID by phone or in person and not by email.

Lost Items

7.2 If you have lost any items as detailed in paragraph 3.3, SID will ask you to either complete a form if you are visiting them in person, or they will complete the form (see Annex A below) for you if you are phoning the issue through. It will be more helpful if you could give as much information as possible in order for the issue to be assessed.

Found Items

7.3 Any items that are found, also need to be reported to SID and you will also be asked to complete a form (Annex A).

8. Related Policies

8.1 Staff are also asked to abide by the following related policies below:

- Overarching Information Governance and Security Policy
- Data Breach Management Policy
- Privacy and Personal Data Protection Policy

- Regulations Relating to the Use of Information Technology Facilities
- Anti-malware Policy
- Bring Your Own Device
- Encryption Policy

9. Policy Review and Maintenance

9.1 This policy will be reviewed and updated, annually, or as needed, to ensure that the policy remains aligned with changes to relevant laws, contractually obligations and best practice.

10. Help and Advice

10.1 If you need any further advice, please contact the SID, Information Governance team dataprotection@exeter.ac.uk or IT Security and Compliance itsecurityandcopliance@exeter.uk