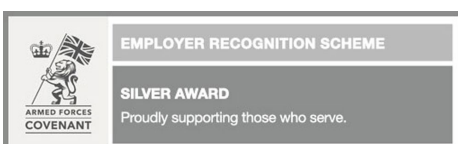




MADE TO MEASURE MENTORING LTD
LAPTOPS AND REMOVABLE MEDIA POLICY

1. CONTENTS

1. INTRODUCTION	1
2. CONTACTS	1
3. PURPOSE	1
4. SCOPE	1
5. PORTABLE DEVICES POLICY	3
6. REMOVABLE MEDIA POLICY	4
7. LOST AND FOUND PORTABLE AND REMOVABLE MEDIA DEVICES	5
8. LEAVING THE COMPANY	5
9. POLICY INFORMATION	5
10. SIGNATURES	6



1. INTRODUCTION

- 1.1. Made to Measure Mentoring Limited (M2M2[®]) is a company registered in England and Wales (Number: 10653662). This procedure also covers all subsidiary companies in M2M2's ownership.

2. CONTACTS

Name	Role		Telephone
Sibbald, Duncan (DS)	Data Protection Officer	duncansibbald@m2m2co.uk	07776 092 806
Miles, Andy (AM)	MD (Academic)	andymiles@m2m2.co.uk	07730 119958
Robinson, Tony (APR)	MD (Commercial)	tonyrobinson@m2m2.co.uk	07495 006485
Robinson, Peter (PR)	Chairman	peterrobinson@m2m2.co.uk	07831 161523

3. PURPOSE

- 3.1. This policy has been written to establish the principles, procedures and working practice with regard to laptops and removable data and all data stored on removable media.
- 3.2. The purpose is to minimise the loss, unauthorised disclosure, modification or removal of sensitive information maintained by M2M2.
- 3.3. It also outlines users' responsibilities around the use of portable and removable media devices, including what actions to take if such items are misplaced.

4. SCOPE

- 4.1. This Laptops and Removable Media Policy sets out how Made to Measure Mentoring Limited ("M2M2", "we", "our", "us", "the Company") handle the laptops and removable media of our customers, suppliers, employees, workers, sub-contractors and other third parties.

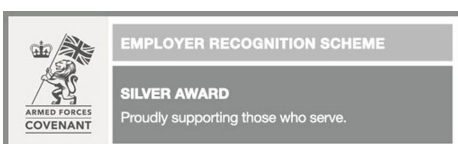
- 4.2. This Laptops and Removable Media Policy applies to all Company Personnel (“you”, “your”). You must read, understand and comply with this Data Protection Policy when using laptops and/or removable media on our behalf and attend training on its requirements if asked.
- 4.3. This Laptops and Removable Media Policy sets out what we expect from you for the Company to comply with applicable law. Your compliance with this Laptops and Removable media policy is mandatory. Any breach of this Laptops and Removable media policy may result in disciplinary action.
- 4.4. When referred to within this policy, portable devices and removable mediums include:
- 4.4.1. Laptop computer, notebook computer, netbook, etc.
 - 4.4.2. PDA
 - 4.4.3. Tablet
 - 4.4.4. Smart Watches
 - 4.4.5. Phone, smartphone, MP3 player or other communications / audio / video device with data storage or data access capability
 - 4.4.6. All portable computer devices typically running one or more of Windows, MacOS, Unix / Linux, or other source codes
 - 4.4.7. CD, DVD, floppy disk, tape, zip disk, etc.
 - 4.4.8. External hard disk
 - 4.4.9. USB memory stick
 - 4.4.10. Solid-state or other storage card (e.g. CompactFlash, SD, other new digital storage, etc.).

5. PORTABLE DEVICES POLICY

- 5.1. Portable devices should only be used where there is no other alternative method of storing data. Unless absolutely essential to M2M2 business, personal devices must not hold any information that is sensitive, personal, confidential or of commercial value.
- 5.2. In the event that you are transferring data internally, a full anti-virus sweep should be conducted.
- 5.3. All devices used for M2M2 business must have full disk encryption unless cleared by the DPO.
- 5.4. Ideally, M2M2 supplied devices should not be used for personal use as this increases the risk of introducing malware into M2M2 systems.
- 5.5. All devices must be kept securely by the employee, sub-contractor, etc. responsible for them. When unattended, devices should be kept in a locked area (e.g. a locked room or cabinet). All personnel should strive to minimise the time that devices are left unattended.
- 5.6. Portable devices are particular targets for theft. 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. Ensure that it is locked away in the boot or hidden and it is recommended that you do not leave it for periods longer than 15 minutes.
- 5.7. All devices should be updated with the latest upgrades and security updates and personnel should ensure that firewalls are updated and that anti-virus and anti-malware programs are enabled and all upgrades routinely applied.
- 5.8. No passwords should be written down and stored with devices.
- 5.9. All devices should be locked manually when the user leaves them and should be configured to lock if inactive for a period no longer than five minutes.
- 5.10. If your portable device (M2M2 supplied or personal device) is stolen you must report it to the DPO without delay so they 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-M2M2 supplied removable media devices, except as explicitly provided for in contracts with third parties providing goods or services to M2M2.
- 6.2. As with laptops, M2M2 supplied removable media 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:
 - 6.3.1. The storage medium is encrypted to relevant industry standards, for example, Advanced Encryption Standard (AES) 256.
 - 6.3.2. Unencrypted portable media is used only in a single location, not transported and is 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.)
 - 6.3.3. 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.



7. LOST AND FOUND PORTABLE AND REMOVABLE MEDIA DEVICES

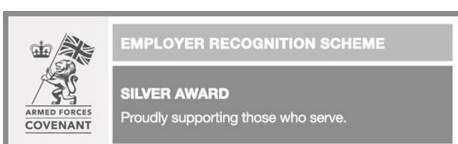
- 7.1. The GDPR specifies that any data breaches must be reported to the DPO within 48 hours once discovered or reported. It is, therefore, important that you report any lost devices or compromises to personal data as soon as possible.
- 7.2. In the first instance this should be reported by phone or in person and not by email.
 - 7.2.1. Lost Items: If you have lost any items as detailed above, please contact the DPO with as much information as possible, such as time of loss, place of loss, last sitting, etc.
 - 7.2.2. Found Items: Any items that are found also need to be reported to the DPO and you should also give as much information as possible, such as locality, time, etc.

8. LEAVING THE COMPANY


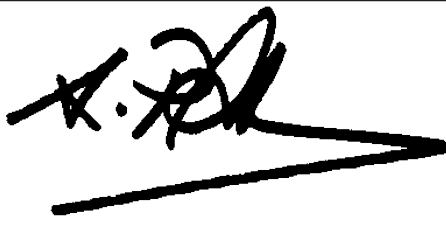

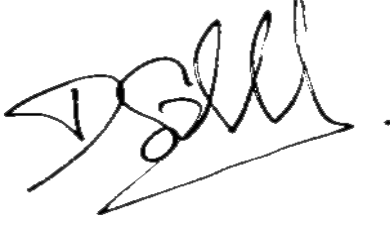
- 8.1. Upon leaving the company or the cessation of contract, all M2M2 owned laptops and equipment must be returned and all removable data wiped.

9. POLICY INFORMATION

- 9.1. All queries on this policy should be submitted to either the Data Protection Officer or the Managing Director (Commercial).
- 9.2. This policy is kept under regular review. The latest review date is published on our website at <https://m2m2.co.uk/company-policies..>



10. SIGNATURES

Name	Signed	Role
Miles, Andy (AM)		Director
Robinson, Tony (TR)		Director
Robinson, Peter (PR)		Director
Sibbald, Duncan (DS)		Director
Made to Measure Mentoring Limited		