Title:	**Mobile Computing and Remote Working Policy**
Version:	**1.1**
Date:	**March 2018**
Reviewed:	**March 2018**
To be reviewed:	**December 2020**
Classification:	**Public**

1. Introduction

This Mobile Computing and Remote Working Policy is a sub-policy of the Information Security Policy and sets out the additional principles, expectations and requirements relating to the use of mobile computing devices and other computing devices which are used to access DMT information assets.

While recognising the benefits to the DMT of permitting the use of mobile devices and working away from the designated place of work, the DMT also needs to consider the information security challenges and risks which will necessarily result from adopting these permissive approaches. In particular, the DMT must ensure that any processing of personal data remains compliant with the principles of the Data Protection Act (see also Privacy Notice) and its successor legislation.

2. Definition

A mobile computing device is defined to be a portable computing or telecommunications device which can be used to store or process information. Examples include laptops, netbooks, smartphones, tablets, USB sticks, external or removable disc drives, flash/memory cards and wearable devices (such as Google Glass).

3. Scope

This policy applies to all DMT staff, Trustees and Committee members and covers all mobile computing devices whether personally owned, supplied by the DMT or provided by a third party. Personally owned, DMT owned or third party provided non-mobile computers (for example desktops) which are used outside of DMT designated place(s) of work are also within scope.

4. Personally owned devices

Whilst the DMT does not require its staff to use their own personal devices for work purposes, it is recognised that this is often practical and convenient and such use is permitted subject to the following requirements and guidelines. It also expects its Trustees and Committee members to use personal devices for Trust business. Users must at all times give due consideration to the risks of using personal devices to access DMT information and in particular, information classified as confidential.

- The device must run a current version of its operating system. A current version is defined to be one for which security updates continue to be produced and made available to the device.

- Mobile devices must be encrypted.
- An appropriate passcode/password must be set for all accounts which give access to the device.
- A password protected screen saver/screen lock must be configured.
- The device must be configured to “autolock” after a period of inactivity (no more than 10 minutes).
- Devices must remain up to date with security patches both for the device’s operating system and its applications.
- Devices which are at risk of malware infection must run anti-virus software.
- All devices must be disposed of securely.
- The loss or theft of a device must be reported to the Executive Director.
- Any use of personal devices by others (family or friends) must be controlled in such a way as to ensure that these others do not have access to restricted DMT information assets.

In addition to the above requirements, the following recommendations will help further reduce risk:

- Consider configuring the device to “auto-wipe” to protect against brute force password attacks where this facility is available.
- Consider implementing remote lock/erase/locate features where these facilities are available.
- Do not undermine the security of the device (e.g. by “jail breaking” or “rooting” a smartphone).
- Do not leave mobile devices unattended where there is a significant risk of theft.
- Be aware of your surroundings and protect yourself against “shoulder surfing”.
- Minimise the amount of restricted data stored on the device and avoid storing any data classified as strictly confidential.
- Be mindful of the risks of using open (unsecured) wireless networks. Consider configuring your device not to connect automatically to unknown networks.
- If a personally owned device needs to be repaired, ensure that the company you use is subject to a contractual agreement which guarantees the secure handling of any data stored on the device.
- Reduce the risk of inadvertently breaching the Data Protection Act (and successor legislation) by ensuring that all data subject to the Act which is stored on the device is removed before taking the device to a country outside of the European Economic Area (or the few other countries deemed to have adequate levels of protection).

5. DMT owned devices

The DMT may at times provide computing devices to some its staff. When it does, it will supply devices which are appropriately configured so as to ensure that they are as effectively managed as devices which remain within the office environment.

In addition, the following are required:

- Non-staff of the DMT (including family and friends) must not make any use of the supplied devices.

- No unauthorised changes may be made to the supplied devices.
- All devices supplied must be returned to the DMT when they are no longer required or prior to the recipient leaving the DMT, irrespective of how they were purchased (for example, grant funding).
- Staff should also follow the additional recommendations listed above for personally owned devices.

6. Third party devices

In general, members should not use third party devices to access restricted DMT information assets. This includes devices in public libraries, hotels and cyber cafes.

7. Reporting losses

DMT staff have a duty to report the loss, suspected loss, unauthorised disclosure or suspected unauthorised disclosure of any DMT information asset to the Executive Director.