Home and mobile working (IT elements) policy

February 2020

UNIVERSITY OF
WINCHESTER

Document Title:	Home and Mobile working policy
Document Author:	Fiona Greig
Responsible Person and Department:	Fiona Greig Library & IT Services
Approving Body:	SMT
Date of Approval:	17 Feb 2020
Date Effective From:	*17 Feb 2020*
Review Date:	***31 July 2021***
Indicate whether the document is for public access or internal access only Indicate whether the document applies to collaborative provision? *(Strikethrough text, as appropriate)*	**Public Access** ~~**Internal Access Only**~~ ~~**Applies to Collaborative Provision**~~

Summary:

This policy sets out clearly what is required when using a University supplied or privately owned mobile computing device. Effective implementation of this policy will minimise the risk of data loss and/or inappropriate use or access to University electronic resources and information.

TABLE OF CONTENTS *(right-click table below and select 'Update Field' and, if given option, 'Update entire table').*

1. Scope

1.1. It is recognised by the University that mobile working is a necessary and often advantageous mode of working. However, mobile working today is now supported by a range of devices designed for ease of use and with the capability to connect and access resources such as email, online storage, and University business systems and data sources.

1.2. This increases the level of risk of data loss, theft and inappropriate use.

1.3. This policy applies to all University staff and other authorised users.

2. Use of personal devices

2.1. Before connecting any device to University wireless or other available networks you must ensure:.

2.1.1. You have installed a suitable anti-virus and malware protection software.

2.1.2. You have read and adhered to all relevant policies and where required, registered your device with Library & IT Services.

2.2. Before connecting any device to University wireless or other available networks you must ensure:.

2.2.1. You have installed suitable encryption software for the storage and transportation of University information.

2.2.2. University information should not be stored or transported using a mobile device unless there is a clear business need to do so and should be retained only long enough to fulfil that need. As soon as the requirement is completed the information should be fully deleted and unrecoverable from that device.

2.2.3. If the device is to be used to handle data provided by a third party it is the device owner's responsibility to ensure any security or data handling requirements by that organisation are met.

2.2.4. University information and critically any stored account, identity or access details must be removed before the device can be reassigned to another user.

2.3. Users must ensure they mitigate the risks associated with the environment in which they may be working. Advice and guidance should be sought from Library & IT Services on environments, off campus or international locations where you may be unsure of the risks you may be facing.

3. University provided mobile devices

3.1. Library and IT Services are responsible for sourcing, building and maintaining University mobile devices to support staff to undertake their full range of activities.

3.2. Library & IT Services are reviewing new mobile device management solutions and will have the responsibility and authority to lock-down devices to ensure patching and updates are applied appropriately and to lock down access to install unapproved apps and services.

3.3. There are a number of devices previously distributed which will need to be brought into this new approach. All staff will be expected to comply with the request to return the device for updating.

3.4. During this process Library & IT Services reserve the right to clean down the device and do a fresh install of the University build. Any non-official software, documentation or services on the device will be removed.

4. Storage

4.1. Devices with synchronised online storage present considerable opportunities for data loss or inappropriate use or access to information. Users therefore must ensure the following:

4.1.1. Where the University has provisioned cloud storage (e.g. OneDrive or Board Papers) all staff are expected to utilize these services in favour of any other storage option.

4.1.2. No University confidential information should be synchronised to or stored on cloud based storage that has ***not*** been agreed contractually by Library & IT Services on behalf of the University. This includes but is not limited to:

- GoogleDocs
- Drop box
- Skydrive
- SugarSync

5. Removable devices and media

5.1. Storage mediums and devices such as USB sticks, external hard drives, flash card and any other portable drives carry considerable risks in transporting, storing or transferring University confidential information and so :

5.1.1. Should not be used unless absolutely necessary to temporarily store University information.

5.1.2. Information on such devices should be retained only long enough to fulfil the specific need. As soon as the requirement is completed the information should be fully deleted and unrecoverable from that device.

5.1.3. Encryption should be applied to all such devices.