



# Home and mobile working (IT elements) policy

January 2022



UNIVERSITY OF  
**WINCHESTER**

|  |   |
|--|---|
| Document Title:  | Home and Mobile working policy (IT)   |
| Document Author:   | Fiona Greig   |
| Responsible Person and Department:   | Fiona Greig Knowledge & Digital Services  |
| Approving Body:  | UMG<br>Senate   |
| Date of Approval:  |   |
| Date Effective From:   | <i>1<sup>st</sup> January 2022</i>  |
| Review Date:   | <b>31 July 2023</b>   |
| Indicate whether the document is for public access or internal access only<br><br>Indicate whether the document applies to collaborative provision?<br><i>(Strikethrough text, as appropriate)</i> | <b>Public Access</b><br><del><b>Internal Access Only</b></del><br><del><b>Applies to Collaborative Provision</b></del>  |
| 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

|                                       |   |
|---------------------------------------|---|
| 1. Scope                              | 3 |
| 2. Use of personal devices            | 3 |
| 3. University provided mobile devices | 4 |
| 4. Storage                            | 4 |
| 5. Removable devices and media        | 4 |

## 1. Scope

- 1.1. It is recognised by the University that flexible and mobile working is a necessary and often advantageous mode of working. However, flexible working is achieved by using 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 compromised accounts, cyber criminality (including ransomware deployment), loss, theft and inappropriate use.
- 1.3. This policy applies to all University staff and all 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. For more information about these visit the National Cyber Security Centre's [advice page](#).
  - 2.1.2. You have read and adhered to all relevant policies and, where required, registered your device with Knowledge & Digital Services. This registration is where your work or research is into areas which may trigger concerns from legal, criminal or ethical challenge. Registration should happen before any websites or data is accessed or created.
  - 2.1.3. Your device is running the most up to date version of the operating system and key software. It is expected you will always update your device.
  - 2.1.4. To support enhanced cyber security requirements the University may have to automatically capture information about your devices (operating system, update status, IP location) and may block access to our services if these are not in line with our operational and security requirements.
- 2.2. Before connecting any device to University wireless or other available networks you must ensure:
  - 2.2.1. We have provided you a OneDrive space for encrypted and secure storage. You should use this exclusively for all University related work, including drafts, sharing with teammates etc. If you choose not to use OneDrive you must ensure you have installed suitable encryption software for the storage and access to University provided information. You must do this before connecting any device to University wireless or other available networks.
  - 2.2.2. University information should not be stored or transported using a mobile device (including USB flash drives etc.) unless there is a clear business need to do so and this copy should be retained only for the specific purpose and then immediately deleted including a full reformatting of the device used.
  - 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, 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 Knowledge & Digital 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. Knowledge & Digital Services are responsible for sourcing, building and maintaining University devices to support staff to undertake their full range of activities.

3.2. Knowledge & Digital Services 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 be recalled to have the management tool installed. All staff will be expected to comply with the request to return devices for updating. Withholding devices may lead to disciplinary action.

3.4. During this process Knowledge & Digital 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 required to utilise 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 Knowledge & Digital Services on behalf of the University. This includes but is not limited to:

- iCloud
- 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. You can purchase USB devices with built-in encryption – these are expected to be used. Members of ELT, Deans and Directors should contact Director of Knowledge and Digital Services if they have a requirement to utilise mobile storage devices.