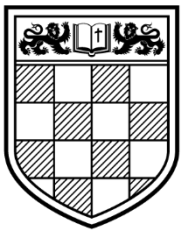

UNIVERSITY OF WINCHESTER

Home and Mobile Working (IT Elements) Policy (01.08.2024)

Document Title:	Home and Mobile Working (IT elements) Policy
Responsible Role and Department:	Director of KDS Knowledge & Digital Services
Approving Body:	University Leadership Team (ULT)
Date of Approval:	24 July 2024
Date Effective From:	01 August 2024
Review Date:	31 July 2025
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

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

1. Scope

1.1. The University understands that flexible and mobile working is a necessary, and often advantageous, mode of working. Flexible working is achieved by using a range of devices with the capability to connect to, and access resources from University systems and data sources.

1.2. This increases the level of risk of undertaking the University business including data loss or inadvertent access, compromised accounts, cyber criminality (including ransomware deployment), loss, theft and inappropriate use of physical or digital assets.

1.3. This policy applies to all University staff and all other authorised users including visiting lecturers, external examiners, and anyone one else providing support or services to the University.

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. Note this registration is required where your activities (work or research) may trigger concerns around safeguarding, legality or ethical questions, 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 required that all devices are continuously updated.

2.2. To support enhanced cyber security requirements the University will 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.

2.3. You must not access University resources or services from any mobile device which is shared with anyone.

2.4. You must not access University resources or services from any device where "biometrics" are the only option to unlock the device/account.

2.5. On your device you must create a separate Work account, separating your personal activities from your work activities.

2.6. You must not save passwords or access details on the device.

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

2.7.1. You only use the OneDrive or Teams tools for encrypted and secure storage. You must use this exclusively for all University related work, including drafts, sharing with teammates etc. If you are working on a shared external research project, committee or other such activities, and they require you to access other collaborative spaces, you must have suitable encryption software loaded on the device you are using. You

should also be aware of who else has access permissions and ensure they have legitimate reasons. You must also have permission of any document or shared file owner approves you sharing the link with others. You must do this before connecting any device to University wireless or other available networks.

2.7.2. 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. If you do need to have files on such a drive each file must be password protected. Files should be retained only for that specific purpose and then immediately deleted including a full reformatting of the device used.

2.7.3. If the device is to be used to handle or store 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.

2.7.4. Before any device can be reassigned to another user it must be completely wiped with all data removed and the device reformatted back to its original settings. Where the device was provisioned by the University it must be returned to Knowledge & Digital Services to perform this task.

2.7.5. If you lose any device that contains University information you must report this immediately to ServiceDesk with as much information as possible.

2.8. Users must ensure they mitigate the risks associated with the locations they are accessing University resources and services from. Advice and guidance should be sought from Knowledge & Digital Services on the risks of using networks away from the University (off campus or international locations). Where you may be unsure of the risks you may be facing, email ServiceDesk for assistance.

2.9. Be aware that public wi-fi hotspots, including in places like hotels are inherently unsafe and should not be used without additional protections. Again contact ServiceDesk for assistance.

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 manage devices to ensure patching and updates are applied appropriately, and to provide licenced and approved software. KDS also lock down access to limit activities that increase risk to the network (including installation of apps and services).

3.3. University provided devices are continuously monitored to ensure that they are not used in a way that presents a risk to the device, university network and data, regardless of location.

3.3.1. Knowledge and Digital Services will provide access to monitoring outputs as required and approved to support University disciplinary processes, concerns for safety, or criminal investigations.

3.4. There are a number of devices previously distributed which will be recalled to bring them in line with this policy and 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.

3.5. During this process Knowledge & Digital Services reserve the right to wipe and reformat the device. 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.

4.1.2. No University 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 devices such as USB sticks, external hard drives, flash card or 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 made 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 required 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.

5.1.4. If you lose any removable device or media that contains University information you must report this immediately to ServiceDesk with as much information as possible.