Bring Your Own Device (BYOD) Policy

1. Purpose

Thispolicy applies to all University staff that process University data on personally owned devices and covers computers and mobile devices (phones and tablets)

1.1 This document sets out the University’s policy on the use of personally owned devices to

Personally owned devices	Includes - but is not limited to –laptops, personal computers, netbooks, tablets and smartphones that are used to collect, store, access, transmit, carry, use or hold any University data. It applies to the use of the Personally Owned Device both during and outside of normal working hours and whether or not it is used at your normal

University requirements to ensure data securityand the protectionof University owned intellectual property and confidential information.

- Ensuring that no unauthorised persons are able to access University owned data on their personally owned devices.
- Ensuring that University data is removed from the device before disposing of the device or selling it or

the functionality of the locally installed versions if these functions are required and the Microsoft 365 applications are installed locally then Office documents can be opened from the web portal (https://www.office.com/) using the “Open in Desktop App” option. This keeps the document in

- Do not process or view High Risk Data in public places.
- When data is encrypted by the user, a procedure for the management of electronic encryption keys must be established to ensure the adoption of best practice guidelines and compliance with both legal and contractual requirements and to ensure information can be accessed by authorised users when needed
-

you bear in mind the requirements of this policy when purchasing a device you wish to use for work purposes

- Keep your device's software up to date. This includes operating systems, applications, and anti-virus and malware protections
- Personally owned devices can only be connected to the University's Guest Network (e.g. the Eduroam WiFi service) when used on campus. DTS will not register personally owned devices for connection to the wired campus network.
- Do not use public WiFi spots if you are using a personally owned device for High Risk Data. Disable Bluetooth and WiFi if they are not needed
- On leaving the University, ensure all University data is deleted securely from your device. Ensure that master copies of documents that are required by the University are transferred to other University staff before you leave.
- Remove University data from the device before disposing of the device or selling it or passing onto another individual. Ideally, the device should be reset to factory defaulcab[(d)5.4 (ev)-34.2 (2,)0.8 ([(d)5.452 o (c)s)0.8 (ab)2-0.7 (o)2e.6 (o)7.2 (i3d)5.452 o]T
enurei(t)-4.8 you3dehesh