

Business Computing Standard

1. Purpose

The Business Computing Standard is a combination of a University provided user computing device (a PC for example) and set of systems, services and processes that together provide a cyber-safe and secure operating environment for accessing corporate information systems. The environment has been specifically configured to adhere to the technical requirements of all 3rd party corporate information system suppliers (Finance, Student Admin, Timetabling etc.)

The Business Computing Standard directly supports the University's Information Security Policy (<http://url.tees.ac.uk/isp>) and, as embodied as a staff desktop, has helped the University to achieve Cyber-Essentials Plus external accreditation.

Accessing corporate information systems from devices not aligned to the Business Computing Standard generates potentially serious risks to the organisation.

A list of current information systems and services in use by the University is available here:

<https://unity3.tees.ac.uk/departments/ict/Systems/default.aspx>

2. The Business Computing Standard

The Business Computing Standard, for newly configured personal computers, comprises:

- Windows 10 Enterprise Operating System (or later)
- Microsoft Office 2016 (or later)
- Outlook as the e-mail client and Exchange as the mail store

One advantage of having a defined standard for business computing devices is that other needs can be layered on top of the basic standard.

3. Remote Working

Remote working, within the context of the business computing standard, is defined to be the ability to have full office desktop experience at a remote location (home, hotel, meeting room, abroad etc).

The provision of remote working brings many productivity benefits and serious operational difficulties nearly all of which relate to cyber-security. It is vitally important that remote (mobile) working is facilitated within a highly controlled and managed environment to ensure, as far as possible, there are no options for data loss (at rest or in transit over 3rd party Wi-Fi or networks). To that end following extensions to the Business Computing Standard apply:

- Full disk bit-locker encryption (to protect data should a device be lost or stolen)
- Bit-locker encryption for memory sticks – ensuring compatibility with BCS compliant devices.
- Direct-Access technology (to allow secure remote access to University facilities whilst offsite and allow world-wide updating of the device). For further information please see the IT Remote Working Policy (<http://url.tees.ac.uk/rwp>).

For a personal computer to comply with the Business Computing Standard it must be owned and managed by the University and be joined to University's configuration management system (Active Directory).

4. Ownership

The Director, IT and Communications Services (IT Department) has direct responsibility for maintaining this policy and providing guidance and advice on its implementation.