Endpoint Device Purchasing, Deployment and Management Policy

Responsible Office	Department of IT Services
Responsible Officer	Director of IT Services
Approving Authority	VCAG
Date of Approval	15 July 2019
Effective Date	15 July 2019
Related Procedures	None
Related University Policies	Regulations for the Use of Computer Facilities
Amended (if applicable)	N/A
Supersedes	N/A
Next review due	July 2020

1 Purpose

This policy covers the selection, purchase, deployment and disposal of endpoint desktop and laptop computers by the University on behalf of its staff and students. Its function is to minimise the costs and risks associated with purchasing and supporting a large estate of IT equipment used for a wide variety of purposes. The initial cost of purchasing computers for staff across the University is significant, but accounts for only around a third of the overall cost of a device. The remaining costs are made up of support, licensing, underlying infrastructure and disposal. All of these cost components can only be controlled by adopting a standardised approach to the purchase of computers, although flexibility is still required to accommodate specialist activities such as research.

2 Definitions

Scope

This policy applies to all PC (Wintel) and Apple devices (either in desktop or laptop/tablet format) purchased using University funds for the use of permanent and temporary staff in their normal duties. The policy excludes the procurement of mobile phones, which is covered in the Mobile Telephony Purchasing and Usage Policy. It does however include the management of Apple iPhones.

Any equipment purchased as an exception to this policy will receive only the third tier of support as set out in *Table 1* on page 9.

Other exclusions include:
● Equipment required for specialist teaching or research where specific requirements cannot be met by approved suppliers; 1
● Specialised servers, storage and core infrastructure purchased by IT Services, which are subject to separate procurement policies and technical requirements;
● Servers or storage purchased by academic departments for specialist teaching or research, which should be procured in accordance with the procurement policies and technical requirements that govern core infrastructure products purchased by IT Services;
● Hardware purchased for deployment in student labs, although many of the same principles will apply.

Device Procurement

Due to the total volume of computer equipment purchased across the University, all such purchases are subject to EU procurement legislation. The only means of purchasing computer equipment that is fully compliant with this legislation is via the University's approved suppliers. The University's suppliers have been selected with the support of the University's Procurement team following a tendering process using the National Desktop and Notebook Agreement (NDNA) for Higher Education for Wintel devices, and the Higher Education Purchasing Consortium, Wales for Apple devices, ensuring that prices and service levels are optimised for the University.

IT Services will maintain a small stock of recommended devices, ensuring that new requests can be actioned quickly.

Device Standards

The use of equipment standards is an important tool in the delivery of value for money to the University and a consistent user experience for staff and students. The University offers a standard selection of desktop and laptop computers designed to meet the vast majority of staff requirements, and allows for other equipment and variations to be purchased at preferential rates with guaranteed levels of support. The standard models are kept under review with the supplier to ensure suitability. There are currently two desktop and two laptop models from each platform available for selection. All standard models are designed to be supportable by the staff and infrastructure of the University.

3 Policy

Desktop and Laptop Devices			
Principle	Details	Rationale	Exceptions
One device per person.	Users can select a desktop device, OR a laptop device, but not both. Docking stations and external monitor, keyboard and mouse will be made available for laptop users, along with appropriate guidance and support on the safe use of portable computers. Further guidance may need to be issued for securing or locking away laptops overnight.	A laptop with a docking station is equivalent in power and performance to a desktop device for most purposes. BSU laptops are now encrypted. Lightweight laptops are available for regular travellers and “power users”.	Where users have a need for multiple devices as a result of a disability, medical condition or other need under the Equality Act.
Device appropriate to user needs.	Users should select the most appropriate and cost-effective device based solely on business need. Detailed guidance on appropriate technology will be produced by IT Services in consultation with colleagues across BSU.	Historically, there has been little preventing users from purchasing high-end equipment without demonstrating a viable business justification.	Where a business justification can be demonstrated.
Standard devices are Wintel with Apple as an exception.	Unless there is a software-driven need for an Apple device, a Wintel device should be procured.	Wintel devices are cheaper to procure than their Apple equivalent. Some business applications (e.g. Dream, SITS client) only have Windows versions available.	Where a business justification can be demonstrated.
Standard device lifetime is four years for portable and desktop	Users are not able to purchase a new device until their current device is at least four years old. Devices can be periodically re-imaged by the Service Desk to improve performance.	Most standard software is able to run on hardware of up to four years of age with an acceptable level of performance.	Equipment which is deemed “beyond economic repair” or where performance has dropped below

devices.			reasonably expected standards.
Devices which are still functioning will be “sweated” beyond this four year term.	If there is no good reason to refresh a device, it will be kept in service.	Sweating assets maximises the value derived from them (up to the point – at the discretion of IT Services – that they are no longer economically viable to support).	Equipment which is deemed beyond “economic repair”, where performance has dropped below reasonably expected standards or where the device is no longer able to run a supported operating system.
Devices to come from the standard product catalogue maintained by IT Services.	Users must select the most appropriate model from the available catalogue. Exceptions to this process to be approved by the Head of School and Director of IT Services or their nominated representatives.	By maintaining a fleet of standard devices, hidden costs of support and bespoke configuration can be reduced. Technical standards promote a consistent user experience and more effective, responsive, therefore cost-effective support.	Devices for specific approved purposes, generally aligned to part of the BSU academic proposition (e.g. Creative Computing, Music Production, etc.).
Devices to be repurposed and cascaded from leaver to joiner.	Where a member of staff is leaving the University, their IT asset will be re-imaged by the IT Service Desk to bring it back to an as-new status to be issued to their successor.	Re-use of devices ensures expected ROI from their initial cost and avoids unnecessary expenditure on new devices for new staff.	Where a device is more than four years old, a new device will be offered. Where the nature of the role dictates a change of form factor (e.g.

			laptop over desktop) a new device can be considered.
Where practicable, assets will be repurposed.	When a member of staff leaves the University or a department, their computer will be re-allocated to another member of staff if it is less than four years old. Where a serviceable laptop or desktop asset is available, this will be provided to a requesting department rather than a new one.	If the IT Service Desk has recovered and reconditioned a device and proved that it is still useable, this will be provided instead of a new device (at no cost to the requesting department).	Where a reconditioned device is not suitable for a more demanding role, a new device may be purchased.
Devices will be configured with the relevant supported build and security profiles.	Devices will be named, built and installed with licensed, supported software according to their intended purpose. All devices will be installed with management software for the purposes of hardware and software asset management and to facilitate remote technical support.	In order to meet its legal and regulatory commitments and to achieve the expected return on investment in its hardware and software estate, the University needs to ensure compliance of endpoint devices with current policies.	In the event that device management is transferred to an individual, that individual assumes responsibility for compliance.

Mobile Phones, tablets and data contracts			
Principle	Details	Rationale	Exceptions
Tablet devices (e.g. iPads, etc.) available only where there is a valid business case.	Generally, these will be available as companion devices for desktop users with particular requirements. Full guidelines and use cases are to be developed.	For mobile users, a laptop typically represents the most effective and best value option.	Full use cases are to be developed.
Data contracts	Provision of data contracts will be for		Demonstrable

for tablets will be provided only where there is a valid business case.	exceptional use cases. Alternatives such as Wi-Fi should be the default.		business justification.
Standard smartphones will be offered.	A standard smartphone will be available on the BSU catalogue. More advanced and costly models will not be offered.	Many staff now need smartphone functionality such as email, calendaring, and web access on the move. The advanced functionality offered by high-end models is rarely justified.	Demonstrable business justification with appropriate approval at a senior level (VCAG member).

General			
Principle	Details	Rationale	
All devices to be procured from the approved sources.	Generally, this will be via the IT Services catalogue pages on Apollo.	By maintaining a fleet of standard devices, hidden costs of support and bespoke configuration can be avoided.	
All staff are expected to look after all items of technology equipment carefully and guard against damage or	Care must be taken not to leave items unattended, particularly in public places, nor to drop items or spill fluids on them. Deliberate damage to or abuse of equipment will be treated as a disciplinary manner.	Lost or stolen items constitute a potential data security risk. Technology items are typically valuable assets which can be easily damage and are costly to replace. There is the additional risk of data loss to items which are severely damaged.	

loss.			
Computers purchased by the University from its operating budgets remain the property of the University for their lifetime.	Without exception, no devices are to be gifted or sold to members of staff. Historically, members of staff have occasionally been gifted devices or had the opportunity to purchase them when they leave.	Gifting or selling an asset will generally necessitate the purchase of a replacement device for their successor. There is greater value in repurposing a device. There are software licencing, data protection, disposal legislation and health and safety reasons that preclude gifting or selling a BSU asset.	
Access to University computers is subject to all the relevant policies.	Any individual using the University's IT facilities is bound by the Regulations for the use of Computer Facilities.	Use of IT facilities is governed by general as well as IT-specific laws and regulations.	
No spend permitted on BSU credit cards, nor through expenses routes.	Other purchasing channels are not permitted for these items.	There have been examples of purchases made through these channels.	
Due consideration must be given to physical security of computers.	Particular care should be taken in computer labs and open plan offices and fitted with anti-theft devices where necessary. Computers should not be left unattended when unlocked at any time.	Computer theft poses a threat to the University both in terms of asset and data loss. While computers are encrypted, there is a risk of data loss through theft when devices are left unlocked.	

Computers must be disposed of correctly.	In accordance with the EU Waste Electrical and Electronic Equipment Directive (WEEE) regulations and the University's IT Asset Recycling and Disposal Policy via the University's approved contractor.	To comply with legal requirements.	

Exceptions

The normal process for any computer procurement or management requirement deviating from the principles above is to gain approval as follows:
● Exceptions must be approved by the DVC (for Schools and Admin & Tech Services), relevant PVC, HR Director and University Secretary. This will be reviewed after one year's operating experience.
● The approval of an exceptional purchase should be logged with the IT Service Desk.
● Commonly approved exceptions will be incorporated into future versions of the standard specifications.

Service Levels

The service available is in three, distinct tiers as per the table below. Support for anything beyond what is listed here is provided, where possible, on a 'best endeavours' basis.
Additional licensed software may be installed by arrangement with local IT support staff (subject to appropriate licenses being available) – in these cases, installation and ongoing support of that software will only be available from local staff at their discretion.

Windows on approved hardware	Apple on approved hardware	All others
• Normally procured, configured and delivered in 5 days. • 5-day warranty repair or replace service and a temporary replacement within 4 hours. • Anti-virus installed and updated daily. • Web filtering enabled. • Security patches applied frequently and where possible without user intervention. • Over 20 software tools pre-installed. • Suitable for accessing all University systems. • Pre-configured printing, network storage and wireless access (laptops). • Remote technical support. • Software for secure access to University network installed (VPN).	• Delivery subject to availability. • Faulty hardware replaced as per Apple's consumer warranty terms. • Anti-virus installed and updated daily. • Web filtering enabled. • Security patches applied frequently and where possible without user intervention. • Remote technical support. • Self-service software portal. • Self-service printing configuration. • Pre-configured network storage. • Some University systems may not be compatible. • Out of Box configuration (iOS devices).	• Wired and wireless connection available but not automatically configured. • Email access via web browser. • Some University systems may not be available.

Table 1