Computer Procurement & Deployment Policy

Document Control

|  |  |
| --- | --- |
| Title | Computer Procurement & Deployment Policy |
| Abstract | This document sets out the University’s policy on the procurement & deployment of computers and laptops for work purposes |
| Version | 1.0 |
| Date Issued | 21/03/23 |
| Status | Draft |
| Document owner | Information Services |
| Creator name | Dr David Telford |
| Creator organisation name | The University of Stirling |
| Subject category | Centralised procurement & deployment |
| Access constraints | Internal |
| Overarching Policy | Information Security Policy |

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Summary of changes |
| 0.1 | 26 April 2022 | Dr David Telford | First draft |
| 0.2 | 27/10/22 | Trish Davey | Comments from 1st draft incorporated |
| 0.3 | 27/10/22 | Richard Aird | Further edits to the text |
| 0.4 | 21/11/22 | Richard Aird | Further edits to the text |
| 0.5 | 17/01/23 | Dr David Telford | Edits to text |
| 1.0 | 20/03/23 | Richard Aird | Final edits to text, conversion to 1.0 status |
| 1.1 | 01/09/2023 | Dr David Telford | Update following SMT feedback |
| 1.2 | 09/04/24 | Richard Aird | Removal of comments, minor typo edits (Note – Unidesk Links to be added in yellow sections below at next revision) |

Table of Contents

[Document Control 2](#_Toc144647996)

[Purpose 4](#_Toc144647997)

[Background 4](#_Toc144647998)

[Scope 5](#_Toc144647999)

[Key Principles 5](#_Toc144648000)

[Centralised purchasing model 6](#_Toc144648001)

[Loss or theft of a device 7](#_Toc144648002)

# Purpose

1. This document sets out the strategy and policy for the centralised procurement and deployment of staff computers, laptops and peripherals.

# Background

1. A modern agile organisation requires its workforce to be equipped with the best digital equipment it can afford. It is vital for the future success of the University of Stirling not only that it adopts emerging technologies but has the devices necessary to operate successfully online with modern software and digital services. This includes the need to remain secure and to operate safely in a digital environment.
2. The Scottish government expects that organisations will protect their information, systems and services from the ever-evolving cyber threat landscape. Universities must adhere to the Cyber Essentials and other security compliance measures and regulations and where appropriate, research-based universities should go further by aligning with ISO27001 best practice in information security.
3. In order to meet our security accreditation, all University procured devices must be registered with our Mobile Device Management (MDM) system which ensures these devices are registered, secured, regularly updated, and able to be remotely traced and erased in event of theft or malicious attack.
4. The purchase of standard devices delivers opportunities for centralised management of software upgrades and security patches whilst also supporting remote tracking and wiping of lost or stolen devices. Additionally, for many staff the use of laptops rather than desktop PCs will enable them to work anywhere anytime allowing for more efficient use of space across our campus and a reduction in the use of paper.
5. Centralised procurement and deployment will deliver a device replacement scheme which ensures equipment is replaced at the end of an agreed lifecycle; thus removing old hardware which presents a security risk as firmware and software updates are withdrawn due to the age of the equipment. The scheme will ensure that the devices are configured, maintained, and secured properly; and the standardisation of equipment enables a safer and more efficient support service.
6. Importantly, economies of scale are achieved through the use of framework purchases ensuring a good standard of device while minimising cost.

# Scope

1. This policy applies to all laptops and desktop PCs running either Microsoft Windows or Apple macOS operating systems, purchased using University funds for the use of university employees in their normal duties.
2. The policy excludes mobile phones and tablets, and also excludes any devices running other operating systems, including iOS, Android, linux and ChromeOS. Such devices must be registered with the University’s mobile device management system, otherwise access to corporate and academic systems will be denied. These exclusions require local budget – please contact the Information Centre for advice before purchasing these types of devices, or see the links below for further information:  
   9.1 Purchasing tablets: <http://stir.ac.uk/1tp>9.2 Purchasing mobile phones: TO FOLLOW  
   9.3 Purchasing non-standard devices (e.g. linux, ChromeOS, etc.): TO FOLLOW
3. Exceptions to this policy must be approved by Information Services prior to the purchase of any equipment. Examples of reasons for valid exceptions to this policy are outlined below:
   1. IT devices necessary for specialist teaching or research where the business requirement cannot be met by the specifications of centrally provided laptop or desktop PCs.
   2. IT hardware purchased for deployment in computing labs, although many of the same principles will apply.
   3. Specialised servers, storage and core infrastructure purchased by Information Services, which are subject to separate procurement policies and technical requirements.

# Key Principles

1. Where the university has purchased computer equipment as defined within this policy the following principles apply:
   1. Deans and Executive Directors are required to confirm the role necessitates the use of a university laptop or desktop PC.
   2. The devices purchased by the University are the property of the University for the lifetime of the device.
   3. Where the staff role requires a computer, the standard provision will be a laptop device suitable for the activity (with redistribution of the device should the employee leave).
   4. Where a desktop PC is required, the business rationale must be endorsed by the Dean or Executive Director and will be assessed by Information Services for suitability.
2. The device will be purchased by Information Services from an approved supplier, using the list of standard models available at that time, and installed with the University configured operating system and desktop build, and registered with our Mobile Device Management (MDM) security solution,
3. Device information will be registered on delivery of the device from our suppliers and held in an asset register of all University-owned devices, maintained by Information Services. Devices will be linked to their primary user (staff member) in Unidesk, our IT Service Management (ITSM) platform.
4. The purchase of Apple macOS-based computers incurs significantly higher costs compared to equivalent Windows-based computers. Apple macOS-based computers do not receive the same level of support as standard Microsoft Windows-based computers due to their design and enterprise limitations; and some University services cannot be guaranteed to work on macOS devices. It is recognised however, that certain specialist requirements necessitate the use of macOS or Apple-specific software for teaching and research. Therefore, requests for macOS devices are permissible within the scope of the centralised procurement scheme, with requests to be made by the Faculty Operations Manager or Directors of professional services and approved by the Executive Director of Information Services. Approved devices purchased through these requests will be registered with an Apple-specific MDM and subject to the same security and software licencing controls as the Windows-based devices.
5. The computer equipment defined and purchased within the scope of this policy will be subject to an anticipated lifecycle of five years, subject to budgets made available in support of the scheme. Devices will be replaced at the end of their lifecycle, and disposed of through approved routes which minimise electronic waste and seek to repurpose redundant hardware.
6. In some instances, staff leaving the University may be allowed to retain their device, with permission granted by the University Secretary, via requests made by the Dean or Executive Director to the Executive Director of Information Services. If approved, the device must be first returned to Information Services where all University information or data will be securely deleted, and the device returned to its ‘factory designated’ condition (which may require a personal operating system licence to be purchased by the recipient).Centralised purchasing model
7. Devices will be prioritised for replacement based on age and condition. Each year of the scheme will concentrate on the replacement of our oldest devices at that time.
8. In addition to targeting the oldest devices, a limited pool of standard Windows-based laptops will be kept in stock for new staff, strictly for use where existing devices cannot be redistributed (e.g. devices should transfer from a member of staff who leaves employment, to their replacement; but this may not be possible where the overall staff headcount increases within a department). Requests for these devices under exceptional circumstances shall be made by contacting the Information Centre, and the request will need validation by the Faculty Operations Manager or Director of professional services.
9. Where necessary, devices (laptop and desktop) will initially be provided with a monitor, keyboard, mouse, headset and webcam. Laptops will also be provided with a dock where required. If additional quantities of these peripherals are required, perhaps for remote working for example, faculties and directorates are required to provide a fund code to purchase these.
10. Peripherals will not be replaced at the same lifecycle as the device and will only be replaced at the end of their functional working life.

# Loss or theft of a device

1. Should a device be lost or stolen Information Services must be immediately notified whereupon the tracing and/or wiping of the device will be initiated. Where the device cannot be found or otherwise retrieved, a replacement device will be issued.