Version number:	3.0
Policy owner:	Director of Students, Support and Information Services & Director of Information and Learning Technology
Effective date:	01/03/2026
Review date:	28/02/2029

ICT Equipment (Hardware and Software) Provisioning Policy

1. Policy Statement

It is the policy of the University of Chichester ("The University") to ensure that its staff, students and other stakeholders have equipment suitable to the fulfilment of their role and to enable them to participate in and innovate in the University's learning communities.

Equipment is provided for the purposes of your employment at the University. The equipment may not be altered, have unauthorised software added, or used in a way that is inconsistent with the Electronic Information Security Policy (link to policy).

This provisioning policy is shaped by the principles of standardisation, simplification, supportability and device sharing, environmental sustainability, value for money and maintaining security against cyber-threats. The provisioning policy considers the role and context of individuals in what equipment is provided.

The integrity of the devices sourced for the University are permitted to access University information and technology services, as defined by the University's compliance with internationally recognised standards, (e.g. ISO27001), conditions set out in our partnership contracts and in accordance with our financial regulations and procurement policies.

Personal devices, and those provided by (for example) another employer may not satisfy the integrity necessary for the University's commitments to privacy, copyrights, safeguarding and cyber security. If a device fails the connection tests applied at every requested log-in, it will be excluded from accessing University systems, resources and services.

A central inventory of all University IT assets (hardware and software) is maintained. Security and functional updates are centrally deployed to provided devices from within the University's approved software inventory. Equipment will be maintained and, unless there are performance or reliability issues, the workable lifecycle of equipment will vary.

2. The purpose of this policy is to:

- Guide expectations of what equipment can be provided (PC/Laptop/Telephony)
- Raise awareness of how provisioning is shaped by;
    - statutory obligations to avoid loss or exposure of information, and other cyber threats,
    - contractual obligations to the University's partners,
    - privacy, particularly for other people's information you may have access to,
    - the needs of safeguarding,
    - supportability, and value for money,

- the code of conduct as set out in the Electronic Information Security Policy (link to policy),
- arrangements for when someone leaves the University, and;
- environmentally sustainable, and secure disposals.

Summary of Provisioning

- The University provides equipment to achieve the aims of the University. Whilst reasonable personal use is permitted, the devices and services are not to be used for anything that is not aligned to the University's purpose and values, or that elevates risks.
- Staff of 0.4fte and above are provided with a University PC or Laptop. For working patterns of below 0.4fte, equipment maybe shared, unless this is operationally impossible.
- Peripherals to enable telephone and video conferencing etc are included
- Printing and telephone services are included, but usage costs are recharged
- Each Department Head (budget holder) is expected to anticipate additional posts and equipment during each years preceding Operational Planning, and,
  - Where there is an in-year leaver, or departmental reorganisation their equipment should be returned to Service Delivery for redeployment or disposal.
  - Where a member of staff is on sabbatical, equipment may be required to be returned to Service Delivery for redeployment.
  - Where there is an in-year joiner, equipment should be identified to Service Delivery in sufficient time for this to be sourced from stock or suppliers.
- The configuration of equipment is role based, and needs for the role's PC/Laptop/mobile phone, and system and software should be set out in the Staffing Request Form
- The University buys only business class equipment from verified suppliers
  - Higher performance equipment can be proposed, provided it does not compromise security
  - Any nonstandard equipment requires a business case
  - Nonstandard equipment that is unsecured or costly to support will be rejected
- Personal devices (including those belonging to other institutions / employers etc) will only be enabled if they meet the minimum-security standard, as assessed at each login.
- The University provides an extensive range of software:
  - Any software for which there is no Data Protection Impact Assessment (DPIA) will not be approved
  - 'Software' in this context, includes cloud subscriptions, and freeware
  - Any Software, that requires excessive costs to support and maintain to meet the Minimum-Security Standard, or advice from the Data Protection Office may not be approved.
  - Any additional software for which there is an existing solution available, will not be approved
  - AI software that cannot meet the Minimum-Security Standard and the Supply Chain Risk Management Strategy (SCRMS) will not be approved
  - Accessibility Software is not treated differently
  - All new software requires a business case and a Data Protection Impact Assessment and cannot be deployed until IT has assessed that it meets the Minimum-Security Standard.

- Excess, redundant or old devices are not to be gifted, or sold.

3. Staff Computer Packages

Standard IT provision is a registered[1], high performance business class PC or laptop. This will meet almost all needs whilst also enabling a high standard of security, robustness, service and support. Commonly, this is provided with a keyboard, mouse and a monitor, and where it is a laptop, a docking station.

PCs and Laptops are fitted with a head-phone socket and are either supplied with, or have, an integral web camera. Laptops are Wi-Fi enabled. Whilst equipment can be sourced in-year where there is an urgent need, the case for additional equipment will usually be anticipated in each department's annual operational plan, or within the Staffing Request Form.

To ensure the best connectivity, interoperability and security, as well as value from our purchasing, skills and support, University systems are primarily designed to work with the Microsoft enterprise architecture. This is the connectivity that organises and links information together with systems and facilities (such as firewalls and Virtual Private Networks) to repel unauthorised access to university systems and data.

All University devices are bought from verified providers and have anti-tamper mechanisms[2] to reduce the risks of a lost or stolen device being used to gain access to university data and private intellectual property.

Specialised requirements for medical reasons will involve a review and approval through the appropriate Health and Safety officer, or HR Officer. A users' preferences or familiarity with an additional or enabling software does not override its cyber security, or the principles of where an existing alternative exists that has already been approved. This includes AI, screen-readers, speech to text software, and additional grammatical assistance tools, some of which despite their good intentions, are not adequately secure.

4. Additional access to computing resources

All staff and students can use the University log-in credentials provided to them to access other University equipment, such as in teaching rooms, libraries and the equipment in staff hubs. For staff, this also includes the ability to log in to a colleague's laptop, and vice versa. Additional, flexible facilities enable remote access to ultra-high-performance computing and specialised software. In addition, there is a range of loanable equipment available through the Support & Information Zone (SIZ).

Each user's unique log-in configures the computer to the user's email account, print facility, network and cloud-storage. Some teaching and open access PCs may also have access to additional specialised software.

[1] The University must account for all equipment to ensure it is not in the hands of someone who may steal data

[2] Local administrator rights are therefore not enabled, as this invalidates essential Cyber-certification

5. *Bring Your Own Device (BYOD)*[3]

It is important to reflect that staff and students at a university are targeted by cyber-criminals to gain access to sensitive and personal information. The University's provided devices are secured to a validated standard to prevent this and to ensure the University can meet statutory obligations and the conditions required by auditors, and our contract partners such as the Degree Apprentice employers, and the Ministry of Defence.

Only a central University computer, with a university configuration is suitable for accessing sensitive personal information.

Provided a user does not have access to personal sensitive information[3] most other services are web-based (e.g. email, staff intranet, Moodle, web printing) and can be accessed using suitably configured non-university equipment, either on or off campus. However, technologies are deployed to ensure that any device that is infected with malware, or that appears to have unlicenced software, will be excluded.

To connect a personal device to any University infrastructure, or any University information system, the device must be protected with a suitable, up-to-date anti-virus services, user segmentation with a strong password, and must employ cyber-security such as hard disk encryption. All personal devices must be set to not cache University ID and passwords.

As set out in the Electronic Information Security Policy, and its associated guidance, University IDs and password must not be used in 3rd party (non-University) systems and services. If these standards are not met and maintained the device will be excluded.

The SIZ, Service Delivery and Central IT Service will try to help if you have issues, but cannot deploy education software to your device, cannot change the configuration of, or repair personally owned equipment.

6. *Premium and Non-standard Devices*

The University provides high performance, business class equipment as standard. If a specialised device is needed, for example to undertake graphics intensive work, then other devices are available that meet these standards. The devices sourced by Service Delivery operate within the University's enterprise environment to ensure interoperability and that they maintain security. These are bought through reputable supply chains with assured environmental and anti-slavery policies.

Whilst other equipment may be proposed, it must maintain the same level of integrity, whilst also passing the tests of value for money, and must be supportable without unreasonable additional cost. Any premium equipment will require an individual business case to be reviewed by the Corporate Project Monitoring Group, or by a member of the Senior Leadership team, and then for funding to be arranged. Requests based on personal preference is not adequate justification.

Equipment sourced by departments is treated as a 'Bring Your Own Device' (BYOD) and is subjected to the same connection tests as any other device. If it cannot meet the integrity test, it will be excluded from accessing University information, and resources.

[3] For information on BYOD, and Non-University Devices, please see https://help.chi.ac.uk/personal-devices

7. Telephony[4]

The University's primary telephony mechanism is Microsoft Teams which operates in conjunction with a Staff Laptop, PC or mobile telephone. The telephony service automatically 'follows' the user from device to device and includes additional features, such as the usual range of 'do-not-disturb' and 'out-of-office' presence functions. MS Teams Telephony will operate anywhere (worldwide) where there is internet access and is very cost effective.

MS Teams telephony also works via an App. The App is freely available to either University or non-University mobile telephones, and some staff may choose to use this method of answering or making a telephone call.

Where a member of staff is expected to make and receive telephone calls, a Teams compatible stereo headset will be provided. Where necessary, an MS Teams compatible handset (which emulates a traditional telephone) can be provided, however this would be charged to the requesting department's cost centre. Similarly, where the business case justifies it, traditional (telephones can be provided into common areas, office locations etc.

Specialised audio requirements required for medical reasons such as alternative, speakers and microphones will involve review and approval through the Health and Safety Office who can be contacted at the following email address: healthandsafety@chi.ac.uk.

8. Mobile Telephones

The University's high-performance mobile telephones are centrally provided to enable cost-effective commercial rates for data and calls, but also to enable essential security mechanisms to be applied.

Whilst equipment can be sourced in-year where there is an urgent need, the case for additional equipment should be anticipated in each department's annual operational plan, or within the Staffing Request Form.

It is important to recognise that telephony is supplied for the purposes of the work of the University. Calls, SMS texts and data usage charges are recharged to the respective department.

University provided mobile phones are assigned with a managed profile to ensure the security of the device and the member of staff using it. This means the mobile phone has enforced controls, such as automatic screen lock and remote device wipe. The mobile phone is provisioned with university-approved apps (MS Teams, for example). Requests for additional applications will be reviewed on an individual basis where consideration will be made for the business need, and for its prevailing security.

9. Eligibility

University staff with at least a 0.4 FTE permanent contract will usually be provided with dedicated equipment. Job sharing staff, and those on less than a 0.4FTE contract are normally expected to share[5] office equipment, unless there are reasons such as remote and homeworking that make this not possible.

[4] It is important to recognise that telephony is supplied for the purposes of the work of the University. Call charges are disaggregated and recharged to the respective department.

[5] The design of IT network accounts readily supports and enables equipment sharing

Associate lecturers are **not** provided with a university device (e.g. laptop) although short term loans can be arranged. Associate Lecturers can of course use open access facilities or share other staff equipment to access all relevant software and services.

Where there is extended leave of absence (and with appropriate consultation) accounts, and therefore access, may be suspended, and the equipment assigned to such individuals is expected to be returned to the University.

10. Software

It is an integral pillar of the University's security and licensing policies that legitimate software is centrally deployed and that this is therefore incorporated within cyber-security mechanisms. All software enabled or endorsed by university staff must be compatible with the University's security and connectivity mechanisms and policies.

Software that increases risks of cyber-threats or whose purpose is achievable with existing software[6] will not be installed. The IT Service will source and install all software[7].

Software for non-University owned equipment, and for specialised equipment sourced by department, may not be suitable for use within the University's licensing and network environment.

No software can be deployed, accessed or used without it first being formally reviewed for its cyber integrity and safeguarding facilities through a Data Protection Impact Assessment (DPIA). Subscription and cloud-based software that operates through a local client or a web browser may also be unsuitable and must be reviewed through a DPIA. In addition to the oversight of DPIAs through the Data Protection Officer (DPO) all DPIAs are reviewed by IT to assess that they meet the 'Minimum Security Standard'.

The recent developments of AI software require careful analysis of their entire supply chain as often these products comprise of several components sourced by other suppliers, risking data privacy as data could be lost or harvested. External security software is catching up, and the situation will become more manageable, however some AI does not protect against the risks of stalking or radicalism or personal sensitive data from being compromised.

11. In-year developments

Equipping learning spaces or large-scale refurbishments identified in annual operational plans will likely be undertaken as a project.

Where the business case[8] for an in-year need for new hardware of software is approved, this can be sourced from within the University's approved suppliers and installed quickly, provided there are no unmanageable security or safeguarding issues.

Ordinarily, a request for a simple commodity item such as a laptop will be processed in 2-3 weeks. Specialised and premium equipment may take longer and is treated in a case-by-case basis.

---

[6] Unless there is an approval of the business case for a new, or essential software package.

[7] Administrator rights are therefore not enabled, including for the reason that this invalidates Cyber-certification.

[8] This should be co-written with IT/Service Delivery

Most software can be made available quickly, in hours and days as opposed to weeks. It is important to provide ample notice of these requests to ensure reasonable integrity reviews and timescales can be met.

12. Ordering process

The equipment set out in each annual Operational Plan will be collated into a summary report and will be reviewed by the Capital Projects Monitoring Group. Subject to approvals, and the budget approval cycle, the plan for each year's new, and renewed equipment will be set out, including its associated purchasing, equipment preparation and delivery arrangements.

The business case for equipment and software not set out during operational planning (e.g. urgent, premium, etc.) must be identified in a Staffing Request Form, or, if not related to a specific new staffing request can be submitted as an equipment request though the University's Support-Me on-line service.

13. Loss and Damage

If equipment fails, the SIZ/Service Delivery and IT Service will arrange its repair through its warranty or via a third-party repairer. Where possible, a loan device will be provided for the duration of any repair.

If any piece of equipment is irrecoverably broken, lost or stolen[9], then arranging a replacement and managing insurance claims will require the department and IT Services to work with Finance colleagues. The costs of insurance excess, (if applicable) will normally be met by the department.

14. Homeworking

The University's systems and services are highly flexible, with an everything-everywhere ethos. University Laptops used at home or off campus employ a Virtual Private Network (VPN) which secures information transfer to and from university systems and services[10].

All teaching and core services are available from off campus; however, services may be affected by the configuration and capability of the localised (home) broadband services. Non-University devices will not be connected if the University's firewall detects malware, unlicensed software or other cyber threats.

The University does not fund home broadband and does not accept responsibility for any non-university equipment.

15. Code of conduct for using University equipment and services

Anyone who uses any University IT Service or equipment, either on-site and off-site, must adhere to the Electronic Information Security Policy (link to policy), and the **Code of Conduct** within it. The policy links to essential conditions for using personal equipment that uses infrastructure or identifies with the University in any way.

The Help website (link to help site) includes guidance and advice but also sets out the privacy statements and how the use of services is monitored.

---

[9] If equipment is lost or stolen, you must inform the SIZ immediately, to enable IT to prohibit that device's access to university systems.

[10] NB personal devices, do not use the VPN and do not have strong security, especially when off campus.

The Electronic Information Security Policy is integrated with other policies, such as the Privacy Standard, and the use of social media. Together, these demonstrate the need to ensure that staff and students are vigilant and play an active role in the University's countermeasures to grooming, bullying, radicalisation, and other cyber-threats including any risk to compromising privacy or intellectual property.

16. Staff leaving, and the disposal of equipment

If a member of staff leaves the University, the equipment they have been issued must be returned to the Service Delivery team. This includes when there is an expectation that it will be reissued to a subsequent role holder.

Under no circumstances should University equipment be agreed to be gifted to a leaving staff member.

Where equipment has become surplus, broken or redundant this should be returned to the Service Delivery team. This ensures that any residual data is removed following industry standard security process, and that the equipment can be disposed of in a way that causes least detriment to the environment.

For staff that leave, any personal data storage or access to shared documents will be closed through an automated process triggered by the exit date set in the HR system.

Other than in the case of a small number of (time limited) emeritus relationships, there will be no post-employment access retained to university resources, including University email accounts.

17. Printing, copying and scanning services

All users with a University IT network account can access printing, scanning and copying services. All printers are multifunctional, therefore provide all the above services. Devices are in shared areas to ensure access to these services are within reasonable reach of staff locations.

Access to a dedicated printing, scanning or copying device, such as in a single occupancy office, is not supported.

Due to the associated costs involved, it is strongly advised to keep printing to a minimum and colour usage should only be used in exceptional circumstances. All printing and copying are charged to an individual's department (scanning is provided at no charge). Student printing is charged directly to the student, and their account purse can be topped up via an online payment or at the SIZ desk.

Where high-volume printing is required, this should be organised with the University's Print & Imaging team. All scanning should be completed within each departmental area, as the Print & Imaging service prioritise internal bulk-printing (e.g. student recruitment activities) and income generation through commercial print activities.