University of South Wales

Software Policies

University of South Wales - Software Policies

The University's software policies are applicable to all software and datasets installed on 'University owned computer equipment'. Hence forth this equipment will be referred to as computer equipment.

Aim

The main objectives of the University's software policies are:-

1. To ensure that the University complies with its legal obligations under copyright law and adheres to the terms & conditions of acceptable use of software.

2. Manage the University's costs in relation to the procurement, maintenance and support of software and computer systems.

Method

The University will achieve these aims by:-

1. Maintaining a list of all software acquired for installation on University computer equipment;

2. Undertaking regular audits of computer equipment ensuring that only software that is licensed to the University is installed;

3. Removing any software from computer equipment where:-
   a. it has not got the approval of the person who has developed and owns the software rights,
   b. the software has not been licensed to, owned by, or legally transferred to the University,
   c. the computer equipment is no longer required by the University;

4. Offering advice and guidance to staff and students in relation to the terms and conditions of use of software;

5. Defining the processes and procedures that will enable the user to abide by the software policies;

6. Ensuring that staff, students and guests of the University are made aware of the University's software policies;

7. Taking action against any member of staff, student or guest of the University who is in breach of the University's software policies or 'University of South Wales IT Computing *Regulations*'.

SOFTWARE COMPLIANCE

Policy and Procedure Requirements

POLICY STATEMENT

It is the policy of the University of South Wales to respect all computer software and music copyrights and adhere to the Terms & Conditions of any licence to which the University is a party. The University will not condone the use of any software or music that does not have a licence and any employee or student found to be using, or in possession of, unlicensed software or music files will be the subject of the University's disciplinary procedures.

The software management policies contained in this document underpin the '*University of South Wales IT Computing Regulations*'.

It is the responsibility of all employees and students to make sure they have read and understood the contents of the software management policies and to ensure that they abide by them.

Staff and students are reminded that under the terms of their employment with the University, and as part of the student enrolment process, they have already committed to agree to all regulations as set out by the University.

SOFTWARE MANAGEMENT POLICIES

The policies and procedures recorded in this document are specifically related to the use of software on University owned equipment.

	Is this policy relevant to:	
	Staff?	**Students?**
040150 Software Acquisition	Yes	Yes
040152 Software Installation	Yes	Yes
040153 Software Movements	Yes	
040154 ICT Hardware and Software Disposal	Yes	
040155 Software Compliance and Documentation	Yes	
040157 Software Evaluation (Freeware, Shareware & Public Domain Software)	Yes	Yes
040160 Internet Downloads	Yes	Yes
040163 Software and Network Audits	Yes	Yes
Disciplinary Procedures for Breach of Software Policies	Yes	Yes
Guidelines for the disposal of obsolete PC equipment and Hard Disks	Yes	
Disposal of Surplus Equipment	Yes	
University's 'Regulations for the development, deployment and use of University computing and telecommunications facilities'	Yes	Yes

Glossary	Yes	Yes
Appendix 1 – Responsibility of Business Support Team		

Policy 040150 - Software Acquisition

SOFTWARE ACQUISITION (staff and students)

This policy ensures that any software acquired for installation on University equipment comes from a reliable source and where applicable is recorded in the University's software asset register(s).

POLICY

All computer software acquired for use on University equipment must be procured from a reliable source and where applicable recorded and secured, preferably in the University's *centralised* software license management database.

Procedure (Includes Acquisition, Installation and Compliance)

The person requiring the software is responsible for ensuring that the details of the software licence agreement, software license key, software media and purchasing information, are recorded and secured, preferably in the University's *centralised* software license management database (USMD).

The USMD is maintained by IT Services, Business Support Team (BST) on behalf of the University.

It is important to record the source of supply of software (and/or data) in case an investigation or audit of the computer require further information.

Acquiring and taking delivery of the software

1. Before acquiring any software, it is worth speaking with BST to see if the University is already licensed to use the software.
2. BST can assist with the process by sourcing suppliers, placing an order and recharging to your budget code if applicable.
3. If you are planning to download software or data files off the internet and you are not sure if the web site can be trusted, you should contact 'IT Support Services' to seek advice.

Before the software is installed

4. The media must be checked for viruses before any software installation takes place onto the equipment.
5. The software should be registered to the University's software audit tool (USAT) by BST, as failure to do so will result in that software being identified as **not** licensed and could result in the software being automatically de-installed. It is your responsibility to make sure that BST has the software details to register with the USAT.
6. Ideally the original copy of the installation media, software license and a copy of the invoice should be passed to BST for storing in a secure area. If this is not appropriate then the faculty/department must ensure that it has a legitimate software licence, confirm the 'terms of use' of the software, and ensure that the University has the ability to reinstall the software if it is required.

Software Installation

7. If you are not sure if the software you are looking to install on University equipment complies with the software policies or whether it contains a virus, then you should contact 'IT Support Services' to seek advice.
8. The software must be installed by a competent person to ensure that any compatibility issues with other software or hardware can be addressed quickly, and that the software is installed within the software's 'terms of use'.
9. Most PCs in the University conform to a 'managed desktop', which means that only IT SERVICES desktop support staff are able to carry out the installation of software on the equipment. You must contact the 'IT Support Services' to seek authorisation to install software and/or to arrange the software installation on this equipment,
10. Some staff and researchers have elected not to have a managed desktop, and have registered with IT SERVICES to manage their own software installations. Details of this opt-out policy are available via the 'IT Support Services'. The users of these PCs, which are deemed to have an unmanaged desktop, are wholly responsible for ensuring the legitimate use of software on this equipment and for ensuring that the software is maintained to a secure standard.,

Note.
IT SERVICES will pass on any costs to the owner of unmanaged desktops for any repairs as a direct consequence of not managing that equipment to the same standard applied to a typical university managed desktop.

Contact Details:

IT SERVICES - Business Support Team (BST)
Email: itsupport@southwales.ac.uk
Room – TR J251
Tel .no. 01443 – 482882

IT Support Services (IT SERVICES)
Email: itsupport@southwales.ac.uk
Tel .no. 01443 - 482882

ADDITIONAL GUIDANCE

You must be licensed to use software and also adhere to the terms of the *End User License Agreement* (EULA). This is necessary to comply with legal requirements and to retain the University's eligibility for ongoing vendor support.

- Using unlicensed software that is not being evaluated under the terms of the licence, is a criminal offence. Both the individual concerned and the Directors of the University may be held accountable.
- Where licence restrictions come to light following a period of use, this may incur additional and unexpected costs for the University and consequently this cost will passed on to the appropriate faculty or department.
- Allowing software to expire or be unlicensed can result in the vendor's refusal to provide support and / or upgrades at a reasonable price. For those areas which rely upon the software in question, this places both the University business processes and the resultant information at risk.

SUPPORTING DOCUMENTS

ISO 17799 REFERENCE(S)

12.1.2.2 Software copyright

SOFTWARE INSTALLATION (Staff and Students)

This policy ensures that users do not install software without regard to the terms of use of the software and its potential impact on other software applications, and that any use does not breach the laws of England and Wales, and does not breach the University's regulations relating to the use of computing facilities.

POLICY

Computer Software should only be installed on University equipment if:

a) it has the approval of the person/manufacturer who has developed and owns the software rights,

Or

b) there is a valid software licence that is owned by, or has been transferred to, the University

And

- the University has given its approval for the software to be installed onto the equipment;

- in doing so any use of the software must be in keeping with any terms of use/agreement of said software license, and does not breach any laws of England and Wales, and does not breach the University's '*Regulations for the development, deployment and use of University computing and telecommunications facilities*'.

Procedure

See Software Acquisition Procedure.

1. If you are not sure if the software you are looking to install on University equipment complies with the software policies then you should contact 'IT Support Services' to seek advice.
2. The software must be installed by a competent person to ensure that any compatibility issues with other software and hardware can be addressed quickly, and that the software is installed within the software's 'terms of use'.

ADDITIONAL GUIDANCE

- If you would like the software to be installed by an IT SERVICES desktop support officer you should contact 'IT Support Services' to arrange a suitable appointment.
- Most PCs in the University conform to a 'managed desktop', which mean that the user of that equipment should not install software onto this equipment if it will, or has the potential to, damage the core software image of that PC. You must contact the 'IT Support Services' to seek authorisation to install software and/or to arrange the software installation on this equipment,
- Some staff and researchers have elected not to have a managed desktop, and have registered with IT SERVICES to manage their own software installations. Details of this opt-out option is available via 'IT Support Services'. The users of these PCs, which are deemed to have an unmanaged desktop, are wholly responsible for ensuring the legitimate use of software on this equipment and for ensuring that the software is maintained to a secure standard - Software Disclaimer.

Note.
IT SERVICES will pass on any costs to the owner of unmanaged desktops for any repairs as a direct consequence of not managing that equipment to the same standard applied to a typical university managed desktop.

Policy 040153 - Software Movements / Relocation

SOFTWARE MOVEMENTS (staff only)

This policy covers the movement of ICT equipment and associated software within the University as a consequence of staff office moves.

POLICY

The movement of ICT desktop equipment between different physical locations must be coordinated through IT SERVICES so that the appropriate software can be added or removed from equipment and the software asset databases can be updated.

Procedure

1. Before any staff office moves take place, you should contact the 'IT Support Services' to register intent.
2. IT SERVICES will meet with the relevant departmental manager to ascertain whether new software will be required or old software can be re-distributed.
3. IT SERVICES will make provision to assist with the relocation and commissioning of all ICT equipment associated with the move.
4. Details of the new locations of staff, their hardware, network points and any additional software will be updated in the IT SERVICES asset database.

Policy 040154 – ICT Hardware and Software Disposal

ICT HARDWARE DISPOSAL (staff only)

This policy makes sure that software/hardware is disposed of in a controlled manner.

POLICY

IT Services has a separate policy for controlling disposal:
IT & Confidential Waste Disposal Policies

Procedure

1. Once a computer is deemed ready for disposal, all software must be removed from the hardware. Arrangements can be made through 'IT Support Services' for a member of IT SERVICES staff to undertake this work.

2. Where the licence permits, the software will be re-used or stored for future use (OEM software will be disposed of with the computer as these licences are non-transferable).

3. All University data must be removed and the hard disk must be wiped clean with DBAN software, and the asset database must be updated. If the data is destroyed by a 3rd party, the certificate of disposal/destruction must be held on file.

4. If the data on the disk is deemed to be of a sensitive nature, i.e. a staff machine or a machine used for administrative tasks, then the technician should perform a 7 pass wipe using the Darik's Boot and Nuke (DBAN) 'dod' command.

   (The above command is the standard recommended by the US Department of Defence.)

5. If the data on the disk is deemed to be of a non-sensitive nature, i.e. a lab machine or similar, then it is at your manager's discretion on how to erase the data. Although a wipe of 1 pass should be sufficient. The DBAN command for this is 'quick'.

Policy 040155 – Software Compliance and Documentation

SOFTWARE COMPLIANCE AND DOCUMENTATION (staff only)

This policy states how the University manages the proof documents that show you have the right to use the software.

POLICY

All faculties and departments must provide a list of software and documentary evidence to verify that it is managing its software assets.

Procedure

See Software Acquisition Procedure.

1. BST offers a service to faculties/departments to maintain the University's centralised software license management database and will take responsibility for securing any software assets in their possession. BST will confirm the 'terms of use' of the software, and ensure that the University has the ability to reinstall the software.
2. Ideally the original copy of the installation media, software license and a copy of the invoice should be passed to BST for storing in a secure area. If this is not appropriate the faculty/department must take responsibility for securing these assets.
3. BST will make an electronic copy of the licence, to store for security purposes.
4. A full inventory of the media should be kept and access to this media should be controlled.
5. The location of media must be recorded at all times. If this is stored with IT SERVICES, it will be signed in and out from by an authorised person in BST.
6. Internal audits of software assets will be undertaken on behalf of the University's Directorate, to ensure the location of media matches with the inventory.

Policy 040157 – Software Evaluation (Freeware & Shareware & Public Domain Software)

EVALUATION (FREEWARE, SHAREWARE & PUBLIC DOMAIN SOFTWARE) (staff and Students)

Users often think that because software is free or on evaluation, it falls outside the boundaries of the University's software policies.

POLICY

Shareware, Freeware & Public Domain software is bound by the same policies and procedures as all software. No user may install any free or evaluation software onto the University's systems without complying with the University's software installation policy.

Procedure

1. Please refer to the software installation policy procedure.
2. If this software is shareware, and requires deletion or licensing after a trial period, the user may wish to contact 'IT Support Services' to seek advice. If this software is not required the software should be uninstalled.

ADDITIONAL GUIDANCE

The use of freeware, shareware and public domain software may impact on the use of other University software and hardware.
It is often difficult to determine whether a program is freeware, shareware or public domain that may require a licence after an evaluation period and to avoid any mistake it is essential that IT SERVICES staff are made aware of the software terms and conditions.

Open source software

In all cases of open source software requests staff must raise a service call for BST to confirm the licence agreements, as some programs have 3rd party components with bespoke agreements. Therefore please anticipate up to 10 days for confirmation from BST for authorisation Desktop Support Teams to install.

Policy 040160 – Internet Downloads

INTERNET DOWNLOADS (staff and students)

There is a danger that a user will download files off the internet which may deliberately or inadvertently, cause damage to the integrity of the University's ICT infrastructure or these files may contain obscene or other offensive material.

POLICY

No software or data files should be downloaded from the internet from an un-trusted web site, or without due consideration of the University's software acquisition and installation policies.

Procedure

1. A user who requires software that can be downloaded from the internet, must comply with the University's software acquisition and installation policies.
2. Files should only be downloaded from a trusted web site. If there is any doubt as to whether a site can be trusted, you should contact the 'IT Support Services' team for advice.
3. IT SERVICES may wish to check the licensing requirements for the software, and where appropriate ensure that a licence is purchased, download the software, virus check the download and benchmark the software, prior to delivery to the end user.

Contact: IT Support Services
Tel. x82882
Email: itsupport@southwales.ac.uk

ADDITIONAL GUIDANCE

There are unscrupulous people purporting to offer legitimate software, to download off the internet, with the intention to gain illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud.

IT SERVICES are the custodian for ensuring the integrity and security of the University's ICT infrastructure. Before software is downloaded from the Internet, they will ensure that the software is coming from a valid web site and will undertake security measures to ensure legitimacy.

Policy 040163 – Software and Network Audits

SOFTWARE and NETWORK AUDITING (staff and students)

This policy alerts users that regular audits are carried out to ensure adherence to University policies.

POLICY

Random and periodic audits will be undertaken on all computers connected to the University's ICT network to ensure that users do not infringe the University's regulations and the Laws of England and Wales.

Procedure

The University uses auditing software on a regular basis to ascertain whether software installed on University equipment has an appropriate license to use. This software audit is checked and reconciled with the software licence database and all unauthorised software will be deleted. The source of the unauthorized software will be ascertained and disciplinary action may be taken.

The University monitors traffic over the network looking for unacceptable use of the internet. All instances of a serious pornographic nature are reported to the police as a matter of course and could lead to prosecution.

Any breach of the University regulations will invoke the University's disciplinary procedures

Disciplinary Procedure for Breach of Software Policies (staff and students)

The University's software policies are implemented to safeguard the University from the many varying laws surrounding software use. Any user found to be breaking these policies will be dealt with under the University's Disciplinary Procedures. In the case of gross misconduct, staff and/or students may be subject to dismissal / expulsion.

Guidelines for the Disposal of Obsolete PC equipment and Hard Disks (staff only)

These are the recommended guidelines for the disposal of obsolete hard disk drives e.g. (when decommissioning obsolete equipment).

- Receive authorisation and confirmation from departmental inventory administrator that the equipment is to be decommissioned.
- Take ownership of equipment and set it up as normal to be able to access hard disk.
- If user is unable to access the disk due to a hardware problem the hard drive may have to be disconnected and re-connected to a different machine to allow the user access.
- If the disk itself is irreparably damaged then further investigation may be required to determine whether the disk needs to be destroyed. This is dependent on whether it is deemed that the data on the disk is still accessible.
- If the data on the disk is deemed to be of a sensitive nature, i.e. a staff machine or a machine used for administrative tasks then the user should perform a 7 pass wipe using the Darik's Boot and Nuke (DBAN) 'dod' command,
- If the disk is usable then boot off a DBAN bootable CD and use the following command to delete all partitions and perform a 7 pass wipe across the whole of the disk:

  'dod'

  The above command is the standard recommended by the US Department of Defence. However it can take up to 9 hours to complete a 40 GB drive on a Pentium4 system. This timescale can change depending on the speed of the computer you are using and the capacity of the hard drive.

- If you have more than one disk installed in a PC/Server/Mac, DBAN detects this and wipes all disks found.

- If you have made the distinction that the data on the disk that you are decommissioning is of a non-sensitive nature, i.e. lab machine or similar, then it is of your manager's discretion on how to erase the data. Although a wipe of 1 pass should be sufficient – the command for this is:-

  'quick'

- After a successful completion of the 'dod' or 'quick' command you should then contact the Estates department who will pick up the obsolete equipment and dispose of it accordingly.

Glossary

EULA	End User License Agreement
ISO	International Standards Office
USMD	University’s Software Licence Management Database
USAT	University’s Software Audit Tool – This tool uses the license information within the University’s Software management database to check that a valid license is available for use on the desktop PC.
IT SERVICES	IT Services
OEM	Original Equipment Manufacturer
PC	Desktop Personal Computer. In the context of these policies this term can refer to a PC or Apple Macintosh.
BST	Business Support Team (A section of IT SERVICES)

Appendix 1 – Responsibility of Business Support Team

The Business Support Team (BST) is a section within (IT SERVICES).

Part of their responsibility is to manage the software assets of the University and to audit the University's network checking that the end user and/or University has a license to use any software installed on University PCs.

Specific Responsibilities relating to Software Management:

1. Check the license terms of software to ensure that the product is being used in accordance with its license terms.

2. To update the University's software asset databases with any changes relating to software licences. These may require updates to the University and Vender specific software management databases.

3. To ensure that the software licence is registered for use by the University's software audit tool.

4. To store the original copy of the installation media, software licence and a copy of the order in a secure place.

5. To undertake regular audits of the University's Desktop PCs ensuring that the University has a license to use any software installed on the desktop.

6. To ensure that software is being used in accordance with the terms of the *End User License Agreement* (EULA)