Title	IT Computing Regulations – **IM20** (formerly UPRs IM01, 03, 13 and 19)
Version	01.0
Effective	13 December 2019

IT AND COMPUTING REGULATIONS

General changes	
New consolidated UPR based on UPRs IM01 Networks and Security, IM03 Information Security, IM13 Online Resources and IM19 Internet, Online Communications and Social Media.	
Section	

Structure

1 INTRODUCTION

1.1 This document sets out the University's policies and supporting institutional regulations and procedures relating to:

i the use of the University's IT facilities and individual user responsibilities – this document;
ii specific IT management responsibilities (Appendix I, refers);
iii the security of IT systems (Appendix II, refers);
iv the external-facing website (Appendix III, refers).

1.2 An Equality Impact Assessment (EIA) for this Policy has been done and the Policy is EIA compliant.

2 DEFINITIONS

For the purposes of this document (UPR IM20) and for all of its appendices the following definitions will apply:

2.1 **'Approved detection software'**:
software that is used to detect and destroy computer viruses, spyware and malware, that has been approved for this purpose by the Chief Information Officer (or nominee);

2.2 **'Authorised Member':**
a person employed by, or retained as a consultant and/or on a temporary or casual basis, by the University, the wholly-owned subsidiary companies of the University or their wholly-owned subsidiaries or staff of member institutions of the Hertfordshire Higher Education Consortium (HHEC) who, as part of the remit of their duties for the University, subsidiary company or Consortium, require access to the University's management and administrative information and whose access to these systems has been authorised in accordance with the regulations set out in this document;

2.3 **'Computer virus, spyware and malware'**:
a self-replicating piece of software which may have the effect of disrupting an information system if introduced into it or a piece of software which, when introduced into an information system, extracts information to send to a third party or permits a third party to access that information system in some way;

2.4 **'Confidential information':**
any information that requires special safeguards because of its private nature, in particular, personal information relating to staff and students or information that is commercially sensitive;

2.5 **'Janet'**:
the UK's education and research network linking education institutions and providing internet and other external communications services that is managed by Jisc on behalf of the UK Further and Higher Education Funding Councils;

2.6 **'Management and administrative information':**
a central or local information system and its content used by the University for corporate management and/or for administrative purposes.

2.7 '**Member of the University'**:
an individual granted membership of the University under the provisions of UPR GV061;

2.8 **'Network'**:
all cabling, infrastructure equipment, including routers, hubs and switches and software providing local area network (LAN), wide Area Network (WAN) and wireless network (WLAN) digital communications within and between University campuses and sites; with external organisations and through the Internet;

2.9 '**Personal and confidential information'**:
information about living, identifiable individuals that is held either in a form in which it can be, or is being, processed automatically (this would, in the main, be on computer systems) or within a structured manual filing system. Statements of fact and expressions of opinion about an individual data subject are personal data as is an indication of the data controller's intentions towards the data subject. This definition also includes data held visually in photographs or video clips (including Close Circuit Television footage) or as sound recordings; information that is confidential to the University, including commercially sensitive documents;

---

[2] UPR FR06 'Corporate Governance and Financial Regulation'

2.10 **'Portable media'**:
any portable media both from within and from outside the University.

2.11 **'Principal user'**:
the person who normally operates the computer system;

2.12 '**StudyNet'**:
the University's managed learning environment and student intranet (including all other services linked to from the StudyNet portal, and Office 365).

3 SCOPE

3.1 Users

These regulations apply to anyone using the University of Hertfordshire IT facilities. This means more than Members of the University (including students and staff). It could include, for example:

- Visitors to the University of Hertfordshire website, and people accessing the institution's online services from off campus;
- External partners, contractor and agents based onsite and using the University of Hertfordshire network, or offsite and accessing the institution's systems;
- Tenants of the institution using the University's computers, servers or network;
- Visitors using the institution's Wi-Fi;
- Students and staff from other institutions logging on using Eduroam.

3.2 IT facilities

The term IT facilities includes, but is not restricted to:

- IT hardware that the University of Hertfordshire provides, such as PCs, laptops, tablets, smart phones and printers;
- Software that the institution provides, such as operating systems, office application software, web browsers etc. It also includes software that the institution has arranged for you to have access to, for example, special deals for students on commercial application packages;
- Data that the University of Hertfordshire provides, or arranges access to. This might include online journals, data sets or citation databases;
- Access to the network provided or arranged by the institution. This would cover, for example, network connections in halls of residence, on campus Wi-Fi, connectivity to the internet from University PCs;
- Online services arranged by the institution, such as Office 365, JSTOR, or any of the Jisc online resources;
- IT credentials, such as the use of your institutional login, or any other token (email address, smartcard, dongle) issued by the University of Hertfordshire to identify yourself when using IT facilities. For example, you may be able to use drop in facilities or Wi-Fi connectivity at other institutions using your usual username and password through the Eduroam system. While doing so, you are subject to these regulations, as well as the regulations at the institution you are visiting.

3.2.1 As a condition of their use of the University's computer networks and information systems, the Boards of Directors of the University's wholly-owned subsidiary companies will adopt these policies and their supporting regulations and procedures. OR

3.2.2 Wholly-owned subsidiary companies which operate within the Financial Regulations (UPR FR06[2]) of the University are automatically subject to the policies and procedures set out in this document (UPR IM20). Wholly-owned subsidiary companies of the Corporation and their wholly-owned subsidiaries (where they operate with separate Financial Regulations), and companies in which the University has an interest (partly-owned companies), will be subject to the policies and procedures set out in this document (UPR IM20) unless, for good reason, an exception is granted by the Chief Information Officer. Where the Chief Information Officer has given consent, provision will be made, as necessary, in Financial Regulations, relevant Shareholder's Agreements and relevant Memoranda of Understanding.

4 COMPLIANCE WITH LEGISLATION, UNIVERSITY REGULATIONS AND NATIONAL AGREEMENTS

4.1 It is helpful to remember that using IT has consequences in the physical world. Use of IT is governed by IT specific laws and regulations (such as these), but it is also subject to general laws and regulations such as the University Policies and Regulations (UPRs).

4.2 Domestic law

4.2.1 User behaviour is subject to the laws of the land, even those that are not apparently related to IT such as the laws on fraud, theft and harassment. There are many items of legislation that are particularly relevant to the use of IT, including:

- Obscene Publications Act 1959 and Obscene Publications Act 1964
- Protection of Children Act 1978
- Police and Criminal Evidence Act 1984
- Copyright, Designs and Patents Act 1988
- Criminal Justice and Immigration Act 2008
- Computer Misuse Act 1990
- Human Rights Act 1998
- Data Protection Act 2018
- General Data Protection Regulation of the EU 2016/679
- Regulation of Investigatory Powers Act 2000
- Prevention of Terrorism Act 2005
- Terrorism Act 2000 and 2006,
- Counter-Terrorism Act 2008,
- Terrorism Prevention and Investigations Measures Act 2011
- Police and Justice Act 2006
- Freedom of Information Act 2000
- Equality Act 2010
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)
- Regulation of Investigatory Powers Act 2000,
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Defamation Act 1996 and Defamation Act 2013

So, for example, users must not:

- Create or transmit, or cause the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;

[2] UPR FR06 'Corporate Governance and Financial Regulation'

- Create or transmit information or material which unlawfully discriminates against any person on the grounds of age, race, religion or belief, pregnancy or maternity, marriage or civil partnership, disability, ethnic origin, sex, gender reassignment or sexual orientation;
- Create or transmit material with the intent to cause annoyance, inconvenience or needless anxiety;
- Create or transmit material with the intent to defraud;
- Create or transmit defamatory material;
- Participate in any form of interference or disruption of an electronic system or display any material which may encourage or incite others to carry out acts of terrorism;
- Create or transmit material such that this infringes the copyright of another person or organisation;
- Create or transmit unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their user organisation has chosen to subscribe;
- Deliberately (and without authorisation) access networked facilities or services;
- Make unauthorised modifications to the contents of a computer with the intention of impairing the operation of the computer or relevant program or data;
- Store personal data (including names and e-mail addresses) without following the Confidential and Personal Data processes and procedures governed by UPR IM20.

4.2.2 E-mails and other documents created on the internet may be subject to requirements to disclose material under the Freedom of Information Act 2000. Members of the University, where applicable, should comply with the Freedom of Information Act 2000, under which a public body is obliged, subject to limited exceptions, to disclose information following receipt of a request made in accordance with the Act.

4.2.3 The University may intercept communications in certain circumstances to monitor or record communications through the University's telecommunications systems. Interception of communications is allowed for a range of purposes including, but not confined to, ensuring compliance with University regulations and to prevent or detect crime. The University does not need to gain consent from staff and students before interception takes place for any of these purposes, although in undertaking these operations the University will have proper regard for the Human Rights Act 1998 and to the Data Protection Act 1998.

4.2.4 Users must not commit any act which could be prejudicial to any on-going case in any Court or held to be in Contempt of Court. Users should also note that the English Courts are increasingly using the laws covering contempt to restrict the transmission of sensitive information which relates, or might relate, to high profile cases which they are considering. Such restrictions apply as fully to information available on, or transmitted across, a restricted network (for example, between parties within the University) as to communications to someone external to the University or to information made available publicly, for example, on a web page accessed via a link from the University's site. The University would be bound to comply with any Order made by a Court for the provision of communication traffic or stored data that breached, or appeared to breach, a contempt of Court Order.

4.3 **Foreign law**

If services are hosted in a different part of the world, users may also be subject to their laws. It can be difficult to know where any particular service is hosted from, and what the applicable laws are in that locality. In general, if you apply common sense, obey domestic laws and the regulations of the service you are using, you are unlikely to go astray.

4.4 **General institutional regulations**

All computer networks and information systems will be used strictly in accordance with all relevant University regulations including, but not limited to, the UPRs published within the Information Management (IM) section of the series and UPR SA123.

4.5 **Third party regulations**

4.5.1 Third party services or resources accessed via University of Hertfordshire IT facilities are bound by the regulations associated with that service or resource. (The association can be through something as simple as using your institutional username and password). Very often, these regulations will be presented to you the first time you use the service, but in some cases the service is so pervasive that you will not even know that you are using it.

Examples of this would be:

- **Using Janet, the IT network that connects all UK higher education and research institutions together and to the internet**
  When connecting to any site outside the University of Hertfordshire you will be using Janet, and subject to the Janet Acceptable Use Policy, https://community.jisc.ac.uk/library/acceptable-use-policy, the Janet Security Policy, https://community.jisc.ac.uk/library/janet-policies/security-policy, and the Network Connection Policy http://repository.jisc.ac.uk/7562/1/janet-network-connection-policy-november-2019.pdf.
  The requirements of these policies have been incorporated into these regulations, so if you abide by these regulations you should not infringe the Janet policies.
- **Using Chest agreements**
  Eduserv is an organisation that has negotiated many deals for software and online resources on behalf of the UK higher education community, under the common banner of Chest agreements. These agreements have certain restrictions, that may be summarised as: non-academic use is not permitted; copyright must be respected; privileges granted under Chest agreements must not be passed on to third parties; and users must accept the User Acknowledgement of Third Party Rights, available at https://www.chest.ac.uk/user-obligations/.
- **Using resources via Jisc Collections**
  Many e-journals, e-books, databases and moving image and sound resources have been negotiated by Jisc Collections, for use by UK Higher Education institutions. A guide to the Jisc Model Licence is available at: www.jisc-collections.ac.uk/Help-and-information/How-Model-Licences-work/Guide-to-Model-Licence

4.5.2 **Licence agreements**

Software and on-line resources are purchased under a number of different licensing arrangements. Definitions and restrictions on use will vary from product-to-product.

5 **AUTHORITY**

5.1 These policies, regulations and procedures were originally approved by the Chief Executive's Group with effect from 1 September 2017 on the authority of the Secretary and Registrar.

---

[3] UPR SA12 'Learning Resources'

5.2 The University's IT facilities are managed by the Chief Information Officer, who advises on the content of these regulations. Unless indicated otherwise in the text of this document, the nominee of the Chief Information Officer is the Head of IT Services.

5.3 Authority to use the institution's IT facilities is granted by a variety of means:

- The issue of a username and password or other IT credentials
- The explicit granting of access rights to a specific system or resource
- The provision of a facility in an obviously open access setting, such as an Institutional website; a self-service kiosk in a public area; or an open Wi-Fi network on the campus.

5.4 If you have any doubt whether or not you have the authority to use an IT facility you should seek further advice from the LCS Helpdesk. Attempting to use the IT facilities without the permission of the relevant authority is an offence under the Computer Misuse Act.

6 INTENDED USE

6.1 Use for purposes in furtherance of institution's mission

The University of Hertfordshire IT facilities are provided for use in furtherance of the institution's mission. Such use might be for learning, teaching, research, knowledge transfer, public outreach, the commercial activities of the institution, or the administration necessary to support all of the above.

The IT facilities, and the Janet network that connects institutions together and to the internet, are funded by the tax paying public. They have a right to know that the facilities are being used for the purposes for which they are intended.

6.2 Personal use

Use of the IT facilities for personal use is currently permitted provided that it does not breach the regulations, and that it does not prevent or interfere with other people using the facilities for valid purposes (for example, using a PC to update your Facebook page when others are waiting to complete their assignments). However, this is a concession and can be withdrawn at any time. Employees using the IT facilities for non-work purposes during working hours are subject to the same management policies as for any other type of non-work activity.

6.3 Commercial use and personal gain

Use of IT facilities for non-institutional commercial purposes, or for personal gain, such as running a non-University club or society, is not permitted.

7 IDENTITY AND ACCOUNTS

7.1 Many of the IT services provided or arranged by the institution require identification so that the service knows the user is entitled to use it. This is most commonly done by providing a username and password, but other forms of IT credentials may be used, such as an email address, a smart card or some other form of security device.

7.2 Protect identity

- Users must take all reasonable precautions to safeguard any IT credentials issued to them.
- Users must change passwords when first issued and at regular intervals as instructed. Users must not use obvious passwords, and must not record them where there is any likelihood of someone else finding them. Users must not use the same password as

for personal (i.e. non-institutional) accounts. Users must not share passwords with anyone else, even IT staff, no matter how convenient and harmless it may seem.

- If a user thinks someone else has found out what their password is, it must be changed immediately and reported to the LCS Helpdesk.
- Users must not use their username and password to log in to unfamiliar websites or services nor to log in to websites that are not showing the padlock symbol.
- Users must not leave logged in computers unattended, and log out properly when finished.
- Users must not allow anyone else to use their smartcard or other security hardware, take care not to lose them, and if lost, report to the LCS Helpdesk immediately.

7.3 **Impersonation**

Users must never use someone else's IT credentials, or attempt to disguise or hide their real identity when using the institution's IT facilities. However, it is acceptable not to reveal identity if the system or service clearly allows anonymous use (such as a public facing website).

7.4 **Attempt to compromise others' identities**

Users must not attempt to usurp, borrow, corrupt or destroy someone else's IT credentials.

7.5 **Authorisation to access management and administrative information**

7.5.1 Access to the University's management and administrative information will be granted solely for the purpose of enabling the conduct of the University's business. Therefore, the level of access granted to an individual will be consistent with his or her responsibilities as an Officer of the University. Management and administrative information may be accessed only by authorised Members. This access will be in accordance with the limits of the authority granted to them.

7.5.2 Each manager is responsible for determining the management and administrative information to which individuals for whom they are responsible should be allowed access.

7.5.3 The Chief Information Officer, in conjunction with the relevant Data Stewards, will establish appropriate mechanisms to monitor access to centrally managed management and administrative information. Heads of Strategic Business Units will establish consistent and appropriate mechanisms in line with this policy to monitor access to locally managed management and administrative information.

7.6 **Suspension and/or termination of access**

7.6.1 An individual's access to the University's IT Facilities will be revoked automatically:

I at the end of his or her Membership of the University;

Ii at the request of his or her Head of Strategic Business Unit and/or the Dean of Students;

Iii where he or she is believed to have infringed these regulations.

7.6.2 The University of Hertfordshire reserves the right to revoke an individual's access to the University's computer networks where the user is suspended during a disciplinary investigation.

7.6.3 **Staff leaving the University**

The Head of Human Resources will establish mechanisms whereby changes in the status of Members of the University who are employed by the institution are communicated immediately to the Chief Information Officer, by means of the regular data transfer, so that these individuals' access to University on-line services and systems can be amended, suspended or deleted (as appropriate).

7.6.4 **Students leaving the University**

The Academic Registrar (or nominee) will notify the Chief Information Officer, by means of the regular student data transfer, of the names of students leaving the University so that these students' access to University on-line services and systems can be amended, suspended or deleted (as appropriate). Continued access to specific systems and services for careers and employment support will normally be granted to graduates of the University for a period of two (2) years after graduation.

7.6.5 **Other Members of the University whose Membership lapses**

The access/usage accounts of other Members of the University will terminate on the date specified at the time their privileges were granted. Where no termination date has been specified, their privileges will be withdrawn automatically after one (1) year.

8 INFRASTRUCTURE

8.1 The IT infrastructure is all the underlying hardware and software that makes IT function. It includes servers, the network, PCs, printers, operating systems, databases and a whole host of other hardware and software that has to be set up correctly to ensure the reliable, efficient and secure delivery of IT services.

8.2 Users must not do anything to jeopardise the infrastructure.

8.3 **Physical damage or risk of damage**

Users must not damage, or do anything to risk physically damaging the infrastructure, such as being careless with food or drink at a PC, or playing football in a drop-in facility.

8.4 **Reconfiguration**

Users must not attempt to change the setup of the infrastructure without authorisation, such as changing the network point that a PC is plugged in to, connecting devices to the network (except of course for Wi-Fi or ethernet networks specifically provided for this purpose) or altering the configuration of the institution's PCs. Unless authorised, users must not add software to or remove software from PCs. Users must not move equipment without authority.

8.5 **Network extension**

Users must not extend the wired or Wi-Fi network without authorization. Such activities, which may involve the use of routers, repeaters, hubs or Wi-Fi access points, can disrupt the network and are likely to be in breach of the Janet Security Policy.

8.6 **Setting up servers**

Users must not set up any hardware or software that would provide a service to others over the network without permission. Examples would include games servers, file sharing services, IRC servers or websites.

8.7 **Introducing malware**

8.7.1 Users must take all reasonable steps to avoid introducing malware to the infrastructure. The term malware covers many things such as viruses, worms and Trojans, but is basically any software used to disrupt computer operation or subvert security. It is usually spread by visiting websites of a dubious nature, downloading files from untrusted sources, opening email attachments from people you do not know or inserting media that have been created on compromised computers. If you avoid these types of behaviour, keep your antivirus software up to date and switched on, and run scans of your computer on a regular basis, you should not fall foul of this problem.

8.7.2 All IT equipment and mobile devices must be capable of running the approved malware detection software. The Head of Procurement and Budget Holders will ensure compliance with this regulation.

8.7.3 All IT equipment and mobile devices must have up-to-date approved malware detection software installed and active at all times. It is the responsibility of each user to ensure that:

i the approved detection software successfully downloads and applies any updates that may be available;

ii a full scan is undertaken not less than once each month;

iii all portable media and any files that they may have downloaded, including files attached to email messages, are scanned before they are opened;

iv all files and/or disks sent to others, either within the University or externally, are free of viruses, spyware and malware before they are sent.

8.7.4 The detection of a virus, spyware and/or malware must be reported to the Helpdesk immediately. Users should refrain from broadcasting warnings regarding real or apparent viruses, spyware or malware and from passing on such warnings received from others, as these warnings themselves may contain malware.

8.8 **Subverting security measures**

The University of Hertfordshire has taken measures to safeguard the security of its IT infrastructure, including things such as antivirus software, firewalls, spam filters and so on. Users must not attempt to subvert or circumvent these measures in any way.

8.9 **Security updates**

8.9.1 All IT equipment and mobile devices must be kept up-to-date with any operating system security updates which may be issued by the operating system manufacturer.

8.9.2 It is the responsibility of each user to ensure that updates are installed as soon as they become available. Where possible, systems should be configured to automatically check for the availability of updates and to download and install them. Otherwise a manual check for new updates should be performed at least once a week.

8.10 **Connecting Member's own devices (Bring Your Own Device)**

8.10.1 Members of the University may connect personal privately-owned equipment into mains power supplies and use designated data points in public areas on campus or wireless networks to access the University's networked services. Members using such devices must also comply with the provisions of 8.7, 8.8, 8.9 and 8.10.

8.10.2 Members of the University in Membership B (eg staff) may apply for an IP address to enable them to connect equipment to the network, however permission will be given only where there is a good business reason, the equipment meets the specification determined by the Chief Information Officer and that it poses no risk to network performance or security.

8.10.3 Visitors may connect to Wi-Fi, by subscribing to and using "The Cloud" service.

8.11 **On-line computer file storage for staff**

8.11.1 The University provides central on-line storage for computer files for all staff. This is provided at both an individual level (user store) and for workgroups to share files (shared store). This storage is necessarily limited by available resources and requires active management by those using that storage.

8.11.2 On-line storage is made available to back-up and share files for academic and research work and other University-related activities only. Staff must check their user store regularly to ensure that outdated and inappropriate material (such as personal photographs, personal music files or software installers) and previous backups are removed.

8.11.3 Shared stores must have a nominated manager who is responsible for checking the shared store regularly to ensure that outdated and inappropriate material is removed.

8.11.4 When a member of staff leaves the University, his or her line manager is responsible for:

I ensuring that the contents of that staff member's computers, mobile devices and user store are checked for essential information that may be required by the University;

Ii arranging for those data and documents to be transferred to an appropriate location;

Iii ensuring that the user store is deleted and all personal information removed from any computers and mobile devices prior to the staff member leaving.

8.11.5 No copyright material may be kept in the on-line store unless the copyright rests either with the University or the member of staff storing the material or the University holds a licence or copyright clearance permission has been obtained for that material.

8.11.6 The University reserves the right to inspect the contents of user and shared stores to ensure compliance with University regulations and efficient management and use of the on-line storage facilities. No material will be removed without prior notification to the member of staff in respect of individual user stores or to the nominated manager in respect of shared areas. In undertaking these operations, the University will have proper regard for the confidential and/or personal nature of the information to which it might gain access during the course of such activities.

8.11.7 Definitive versions of corporate documents must be stored in the document management system or other agreed designated central stores, as appropriate. Staff will normally access corporate documents from these central stores and will not retain copies in their user and shared stores.

8.12 **Fault reporting and maintenance**

8.12.1 Faults should be reported immediately to the Helpdesk.

8.12.2 The University's Janet connection is subject to a regular national weekly 'at risk' time when maintenance work specified by Jisc is undertaken. This is on Tuesdays from 07.00 - 09.00 hours.

8.12.3 The University's computer networks and systems are also subject to a local, separate, weekly 'at risk' time when maintenance work is undertaken. This is on Fridays from 07.00 - 10.00 hours. Maintenance work on other weekdays should finish by 08.30 hours.

8.12.4 Three weekends a year will be advertised as 'at risk' periods for major maintenance activities.

8.12.5 Users are advised not to schedule important activities that require IT services during these regular 'at risk' times.

9 **INFORMATION AND SYSTEMS**

9.1 **Personal, sensitive and confidential information**

9.1.1 During the course of their work or studies, staff and students (particularly research students) may handle information that comes under the Data Protection Act 2018 and the General Data Protection Regulations (GDPR), or is sensitive or confidential in some other way. For the rest of this section, these will be referred to as personal and confidential information (PCI).

9.1.2 Safeguarding the security of personal and confidential information is a highly complex issue, with organisational, technical and human aspects. The institution has policies on Data Protection and Information Management at http://www.herts.ac.uk/about-us/corporate-governance-and-structure/university-policies-and-regulations-uprs, and if a Member's role is likely to involve handling protected information, they must make themselves familiar with and abide by these policies.

9.1.3 Anyone discovering a loss of personal, sensitive or confidential data must immediately notify the University's Data Protection Officer, in order to meet the requirements of the GDPR.

9.1.4 Personal and confidential information must not be stored on the hard drive of any workstation that is not in a secure location, on removable media (such as USB storage devices, removable hard drives, CDs, DVDs) or on mobile devices (laptops, tablet or smart phones) unless it is encrypted, and the key kept securely. Ideally, personal and confidential information should never be stored on the hard drive of any workstation.

9.1.5 **Transmission of personal and confidential information**

When sending personal and confidential information electronically, users must use a method with appropriate security. Email is not inherently secure. Advice about how to send personal and confidential information electronically is available at https://herts365.sharepoint.com/sites/Computing/SitePages/Good-practice-and-standards.aspx.

9.1.6 If personal and confidential information is sent using removable media, users must use a secure, tracked service so that you know it has arrived safely. Advice on the use of removable media and mobile devices for protected information is available at https://herts365.sharepoint.com/sites/Computing/SitePages/Good-practice-and-standards.aspx.

9.1.7 **Remote working**

If users access personal and confidential information from off campus, they must make sure to use an approved connection method that ensures that the information cannot be intercepted between the device you are using and the source of the secure service. Public Wi-Fi services must not be used as they may be insecure. Wireless network access to University systems and services on the staff network will be made available via the Secure Access (VPN) service, which encrypts the data, and is restricted to Members of the University in Membership category B. Users must also be careful to avoid working in public locations where the screen can be seen.

9.1.8 **Personal or public devices and cloud services**

Even if using approved connection methods, devices that are not fully managed by the University of Hertfordshire cannot be guaranteed to be free of malicious software that could, for example, gather keyboard input and screen displays. Users should not therefore use such devices to access, transmit or store personal and confidential information.

9.1.9 Users must not store personal and confidential information in personal cloud services, such as Dropbox.

9.2 **Copyright information**

9.2.1 Almost all published works are protected by copyright. If using material (images, text, music, software), the onus is on the user to ensure that use is within copyright law. The key point to remember is if you can see something on the web, download it or otherwise access it, this does not mean that you can do what you want with it.

9.2.2 Where appropriate, published material shall bear the University of Hertfordshire copyright mark in the format: '© University of Hertfordshire Higher Education Corporation (and year of creation of the copyright work)' (UPR FR06[4], refers).

9.3 **Others' information**

9.3.1 Users must not attempt to access, delete, modify or disclose restricted information belonging to other people without their permission, unless it is obvious that they intend others to do this, or you have approval from the Secretary and Registrar.

9.3.2 Where information has been produced in the course of employment by the University of Hertfordshire, and the person who created or manages it is unavailable, the responsible line manager may give permission for it to be retrieved for work purposes. In doing so, care must be taken not to retrieve any private information in the account, nor to compromise the security of the account concerned.

9.3.3 Private information may only be accessed by someone other than the owner under very specific circumstances governed by institutional and/or legal processes.

9.4 **Inappropriate material**

9.4.1 Users must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening or discriminatory.

---

[4] *UPR FR06 'Corporate Governance and Financial Regulations'*

9.4.2 The University of Hertfordshire has procedures to approve and manage valid activities involving such material for valid research purposes where legal with the appropriate ethical approval. Any researcher, staff or student, who, for the purposes of his or her research, needs to access or store materials that may be considered sensitive under Obscene Publications, Counter-Terrorist or other relevant legislation, must obtain the prior written consent to such access from the Director of the Doctoral College who may not delegate this responsibility. In this regard, the Director of the Doctoral College acts as the Institutional Lead for Research Integrity and nominee of the Secretary and Registrar, from whom such consent must be sought in the absence of the Director of the Doctoral College. The Director of the Doctoral College will ensure that a record is kept of all consents so given. Researchers to whom such consent is given will comply with all relevant regulations and guidelines to ensure the safe and secure storage of any material accessed and will comply with any conditions imposed on access by the Director of the Doctoral College.

9.4.3 There is also an exemption covering authorised IT staff involved in the preservation of evidence for the purposes of investigating breaches of the regulations or the law.

9.5 **Publishing information**

9.5.1 Publishing means the act of making information available to the general public, this includes through websites, social networks and news feeds. Whilst the University of Hertfordshire generally encourages publication, there are some general guidelines you should adhere to:

9.5.2 **Representing the institution**

You must not make statements that purport to represent the University of Hertfordshire without the approval of Pro Vice-Chancellor (Enterprise) and Director of Marketing and Communications.

9.5.3 **Staff profiles**

Members of the University in Membership B may use their staff profile and other University pages which they have created or for which they have been assigned responsibility solely for the publication of information associated with their academic and professional profiles and duties with the University;

9.5.4 Members of the University other than those in Membership B, including students, are not permitted to have personal web, extranet or intranet pages or social media or virtual world presences on University web pages, unless this is an agreed requirement of their course, approved by the Dean of School and the Chief Information Officer.

9.6 **Personal web pages (including use of on-line communications services, social media and virtual worlds)**

9.6.1 All Members of the University, including students, publishing personal web pages or creating presences using University resources or related to University purposes are required to comply with the regulations contained in this document.

9.6.2 Members of the University must not use the Internet, extranets, intranets on-line communications or social media to infringe on the rights and privacy of, nor make ill-considered comments or judgments about other Members of the University.

9.6.3 No personal pages shall incorporate the University's logo without the express written permission of the Pro Vice-Chancellor (Enterprise) and Director of Marketing and Communications. Members of the University other than in Membership B are not permitted to use the University's logo, name or corporate image on personal web pages.

9.6.4 Members of the University:

i. must ensure that all information loaded on to personal web pages and on web pages to which they are hyperlinked and on to social media and virtual worlds is true and accurate, is not misleading, illegal or defamatory and is not such that it would call the University into disrepute.

ii. should note that they are personally liable in respect of information published via the Internet and for their own use of the Internet.

iii. should make it clear in personal postings that they are speaking on their own behalf, in particular write in the first person and use a personal e-mail address. Any disclosure of working for the University should include a statement that your views do not represent those of the University.

9.6.5 **Personal data and photographic images**

Personal data including images, photographs and video must not be shared or placed on the Internet or an intranet or an extranet or a social network service or a virtual world without the prior written approval of the data subject and/or, if applicable, the copyright owner. The subject or copyright owner may withdraw this permission at any time. Once permission is withdrawn, the personal data and/or photographic images must be removed immediately.

9.7 **StudyNet, Office 365 and other intranets and social media which host un-mediated content (referred to below as "StudyNet")**

9.7.1 By accessing StudyNet, the user acknowledges and agrees that the University has no control over the content, accuracy or reliability of any information or material posted by users of StudyNet and the user, therefore, agrees that the University is not responsible for any such information or material.

9.7.2 The University, its officers and other Members do not necessarily endorse, support, sanction or agree with comments, opinions or statements made by users of StudyNet.

9.7.3 The user warrants that any information or material which he or she posts to StudyNet will not be false, defamatory, threatening, obscene, indecent or unlawful and will not infringe the rights of any third party or contain anything which might reasonably be expected to cause offence to any third party and the user indemnifies and will keep the University indemnified against any loss or damage that the University may suffer as a result of the user's breach of such warranty.

9.8 **Accessibility**

9.8.1 The University aims to make all its web-based information and services as accessible as possible to all people including those with disabilities. The University recognises the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines as the standard against which accessibility should be assessed.

9.8.2 The University aspires to Web Content Accessibility AA rating (WCAG 2.0) for:

I new web content and services created by the University;

Ii web content and services provided by third party organisations

Iii existing web content and services as and when they are updated.

9.9 **URL (website addressing) definition and management**

The University URL (Website addressing) policy applies to all University internet, extranet, intranet pages and use of social media and virtual worlds (Appendix III, refers).

9.10 **Publishing for others**

The University's web servers may not be used to host web pages and other services on behalf of external organisations except with the prior written approval of the Chief Information Officer and in accordance with the terms and conditions stipulated by the Secretary and Registrar of the University. Web servers used for this purpose must be registered for external use.

10 SOFTWARE AND ONLINE RESOURCE LICENSING

10.1 All software and on-line resources must be used strictly in accordance with the terms and conditions of the relevant Licence. Unless specified otherwise in the Licence terms and conditions, it should be assumed that all resources are subject to copyright law and provided for Educational Use only – ie no commercial use, and often restricted for Teaching Only.

10.2 No authorised Member of the University shall be excluded from the use of a resource for reasons of nationality or citizenship. (It should be noted that some Licences specifically prohibit the export of product to certain countries. Where software has been installed on a mobile device which is to be used whilst travelling, the Licence should be checked to ensure that there are no restrictions.)

10.3 All computer workstations will be subject to audits.

10.4 Members of the University must:

- familiarise themselves fully with the provisions of any Licence before use;
- ensure that they meet all of the requirements of the Licence;
- comply with any regulations relating to the use of any services involved in the provision of access;
- ensure the security and confidentiality of the resource and not sell, re-sell, copy, distribute and/or display any part of the resource on any electronic network unless this is specifically permitted under the terms of the relevant Licence;
- ensure that they use the resource only for the purposes defined in (and only on those computer systems covered by) the relevant Licence;
- not attempt to by-pass any security measures;
- not remove or alter any ownership, copyright or similar notices;
- not reverse engineer or decompile software or alter, adapt or modify information content unless this is specifically provided for under the terms of relevant Licence;
- not incorporate the resource, or part thereof, or a modified version of the resource, in any work, program or article which they produce, except where this is explicitly permitted by the Licence or where they have obtained the prior written consent of the Licensor and (where the incorporation of extracts in their own work is permitted) must wherever possible include a sufficient acknowledgement of the source of each extract;
- as appropriate, return or destroy all copies of the resource, either at the end of the programme or Academic Year or when their period of employment is terminated or when requested to do so by the University;
- on becoming aware of any unauthorised access or use of Product, or breach of Licence, immediately notify, and provide full information to, the Chief Information Officer.

10.5 **E-mail and other on-line communications**

10.5.1 Use of the University's e-mail service and other on-line communication media is for academic, research and University business and social purposes only. E-mail is not a secure mode of communication and must not be used for the transmission of confidential or sensitive information.

10.5.2 University management communicates with Members of the University by e-mail through their individual e-mail accounts, to Members of the University in category B via their individual University e-mail accounts and to Members of the University in category A via the e-mail address they have provided to the University for this purpose. Members of the University in category A are responsible for providing the University with a current individual e-mail address or their choice. All Members of the University must check their e-mail frequently and regularly for e-mail from the University. Official University communications may be sent by e-mail only.

10.5.3 Users are responsible for the management of their personal e-mail files, including the deletion of out-dated and redundant e-mails.

10.5.4 E-mail messages containing a virus which are trapped on delivery by the University's central system will be discarded. To minimise disruption from virus infections which may not have been trapped by the University's central protection measures, Members of the University must not open any attachment sent via e-mail unless it is expected and/or comes from a reliable source and the user reasonably believes it to be free from all viruses, spyware, malware or other harmful or disruptive components.

10.5.5 Unless agreed otherwise by the Chief Information Officer, all electronic mail services will be managed centrally by the Chief Information Officer for the whole University, including its wholly-owned subsidiary companies and their wholly-owned subsidiaries and for any other individuals, groups and organisations for which the University has agreed to provide electronic mail services. Electronic mail will be received, transmitted and stored through central servers from where it can be accessed or collected by individual account holders.

10.6 **Security of management and administrative information**

10.6.1 All networked management and administrative information must be stored on the corporate systems and file storage infrastructure, on the staff network (a closed logical network that is distinct from that used by students).

10.6.2 Heads of Strategic Business Units will ensure that, within those areas for which they are responsible, schedules are established for making back-up copies on a regular basis of data files stored on computer workstations, network file servers and other computer systems and for recording that the necessary copies have been made.

10.6.2 Management and administrative information located in unsecured areas must be secured against theft and use by unauthorised persons.

10.6.3 Authorised Members logging on to an information system must log off or lock the workstation when leaving the system unattended.

10.6.4 Printed reports containing confidential or sensitive information must be stored in a secure area that cannot be accessed by individuals who do not have the appropriate authorisation. These reports may be made available only to individuals who have the appropriate authorisation or clearance. Confidential reports will be shredded before being discarded or disposed of via confidential waste sacks where these are available.

10.6.5 Managers will establish appropriate mechanisms for monitoring compliance with these requirements.

11 BEHAVIOUR

11.1 The University applies the same standards to conduct and/or behaviour regardless of whether communication is electronic or non-electronic. This policy applies to on-line communications posted at any time and from anywhere, whether to an individual, a limited group or the public world-wide. Staff are required to engage professionally and appropriately, adhering to University standards and not breaching the law. The University respects privacy and understands that staff may use Internet and social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the institution's reputation are within the scope of this policy.

11.2 Conduct online and on social media

The University of Hertfordshire policies concerning staff and students also apply to the use of social media. These include human resource policies, codes of conduct, acceptable use of IT and disciplinary procedures.

11.3 Spam

Users must not send unsolicited bulk emails other than in specific business circumstances.

11.4 Denying others access

If shared IT facilities are being used for personal or social purposes, the user should vacate them if they are needed by others with work to do. Similarly, specialist facilities must not be occupied unnecessarily if someone else needs them.

11.5 Disturbing others

When using shared spaces, remember that others have a right work without undue disturbance. Keep noise down (turn phones to silent if you are in a silent study area), do not obstruct passageways and be sensitive to what others around you might find offensive.

11.6 Excessive consumption of bandwidth/resources

Use resources wisely. Don't consume excessive bandwidth by uploading or downloading more material (particularly video) than is necessary. Do not waste paper by printing more than is needed, or by printing single sided when double sided would do. Don't waste electricity by leaving equipment needlessly switched on.

12 MONITORING

12.1 Institutional monitoring

12.1.1 The University of Hertfordshire monitors and logs the use of its IT facilities for the purposes of:

- Detecting, investigating or preventing misuse of the facilities or breaches of the University's regulations;
- Monitoring the effective function of the facilities;
- Investigation of alleged misconduct;
- Other purposes as defined in the UPRs.

12.1.2 The University of Hertfordshire will comply with lawful requests for information from law enforcement and government agencies for the purposes of detecting, investigating or preventing crime, and ensuring national security.

12.1.3 The University reserves the right, but does not assume the obligation, at its sole discretion, and without notice, to monitor, edit, cancel or remove in whole or in part any material or information posted by any user or to terminate an individual's right to post to and/or access the University website, intranet sites, including StudyNet and StaffNet.

12.2 **Unauthorised monitoring**

12.2.1 You must not attempt to monitor the use of IT without the explicit permission of the Chief Information Officer or Secretary and Registrar. This would include:

- Monitoring of network traffic;
- Network and/or device discovery;
- Wi-Fi traffic capture;
- Installation of key logging or screen grabbing software that may affect users other than yourself;
- Attempting to access system logs or servers or network equipment.

12.2.3 Where IT is itself the subject of study or research, special arrangements will have been made, and you should contact your course leader/research supervisor for more information.

13 BREACHES OF DISCIPLINE

13.1 It should be noted that failure to comply with the regulations and procedures set out in this document may be regarded as a breach of discipline and, in some cases, may be unlawful.

13.2 Sanctions may be imposed if the disciplinary process finds that you have indeed breached the regulations, for example, imposition of restrictions on your use of IT facilities; removal of services; withdrawal of offending material; fines and recovery of any costs incurred by the University of Hertfordshire as a result of the breach.

13.3 **Members of the University in Membership B**

Breaches of these regulations and procedures will be dealt with in accordance with the provisions of UPR HR025 and/or the United Kingdom courts. For the purposes of employment rights, a breach of these obligations may be construed by the University as misconduct.

13.4 **Members of the University other than in Membership B**

Breaches of these regulations and procedures will be dealt with, as appropriate, in accordance with the provisions of UPR SA136 and/or the United Kingdom courts.

13.5 **Reporting to other authorities**

If the institution believes that unlawful activity has taken place, it will refer the matter to the police or other enforcement agency.

---

[5] UPR HR02 'Staff Disciplinary Policy'
[6] UPR SA13 'Student Discipline'

13.6 **Reporting to other organisations**

If the institution believes that a breach of a third party's regulations has taken place, it may report the matter to that organisation.

13.7 **Report infringements**

If you become aware of an infringement of these regulations, you must report the matter to the relevant authorities. Heads of Strategic Business Units are required to submit a written report to the Secretary and Registrar immediately in cases where they have reason to believe that any of these may have been breached.

APPENDIX I – IT AND COMPUTING RESPONSIBILITIES

Structure

1 RESPONSIBILITIES OF THE CHIEF INFORMATION OFFICER

1.1 Networks

1.1.1 The Chief Information Officer has primary responsibility for the development, provision and effective management of the University's computer networks, including: computer network security arrangements (internal and external); computer network back-up arrangements; the issue and recording of Internet Protocol (IP) addresses; the management of domain name services; the monitoring of usage and/or demand; the procurement, installation and repair of central computer network equipment; liaison with external service providers; the provision of local computer network connections to individual desktop services equipment and in communications cabinets; external computer network connections and for the formulation of proposals for the further development of the University's computer networks.

1.2 Licence Management

1.2.1 The Chief Information Officer will:

i ensure that a current record is maintained of all Product for which the University holds University-wide site Licences;

ii ensure that University-wide site Licences are negotiated for all Product where this is beneficial for the University and acceptable to the Licensor;

iii ensure appropriate back-up, copying and distribution of Product and Documentation in accordance with the conditions of the relevant Licence;

iv ensure that advice and support is provided to the Head of Procurement and other managers on appropriate licensing arrangements for other Product;

v ensure that, where appropriate, the University benefits from any nationally and/or consortia-negotiated licensing arrangement;

vi ensure that the University contributes, as appropriate, to national and/or consortia proposals for Product licensing;

vii ensure that, where it is a condition of supply, a single point of contact ('Contact Point') is designated to deal with queries and to provide support for Product (section 5.1.2, refers).

viii determine University arrangements for Product audits;

ix investigate any reported breaches of Product Licences and take appropriate action in accordance with relevant University policies and procedures and use reasonable efforts to prevent any recurrence.

1.3 **Internet and intranets**

1.3.1 The Chief Information Officer is responsible for:

i the computer networks, hardware and software and any third party services used for the corporate use of the Internet, including, domain registration and URL definition and management, site hosting, content management arrangements, search engine optimisation, application development and maintenance, analytics and usage reporting, integration with other services, back office processes and server infrastructure;

ii the development, management and delivery of StudyNet and other intranets;

iii the development, management and provision of on-line communications services.

iv management, implementation and use of the University main domain name: 'www.herts.ac.uk';

v definition, approval and management of all URL web addresses for University web-based information;

vi registration of all University URL web addresses for all domain names and is the University's nominated registrar for all University URL web addresses and all domain names;

vii application to JANET for '.ac.uk' domain names.

1.3.2 The Chief Information Officer (or nominee) will consult with the Pro Vice-Chancellor Enterprise and Director of Marketing and Communications (or nominee) concerning web addresses, including shortcut addresses relating to the University external website and its subsites and to agreed microsites.

1.4 **Administrative information and computer networks**

1.4.1 The Chief Information Officer and the appropriate Head of Strategic Business Unit will:

i develop, implement and maintain appropriate disaster prevention measures and a documented disaster recovery procedure for central management and administrative information and computer networks;

ii develop, implement and maintain a documented change control procedure for central corporate applications and associated programs.

2 RESPONSIBILITIES OF THE DIRECTOR OF ESTATES, HOSPITALITY AND CONTRACT SERVICES

2.1 The Director of Estates, Hospitality and Contract Services is responsible for the location and maintenance of cabling ducts on University premises and the implementation of the Standards agreed with the Chief Information Officer in contracts for new building developments and refurbishments.

3 RESPONSIBILITES OF THE PRO VICE-CHANCELLOR (ENTERPRISE) AND DIRECTOR OF MARKETING AND COMMUNICATIONS

3.1 External website

3.1.1 The Pro Vice-Chancellor (Enterprise) and Director of Marketing and Communications is responsible for:

i all corporate material published by the University via the Internet and social media, including branding and design, information architecture and site navigation, use of terminology and key messages, writing and style guidance, and for ensuring that content supports search engine optimisation;

ii establishing the criteria and granting permission for any subsite and microsites and whether these are to form part of the main University website or operate under a separate distinct web address;

iii establishing appropriate internal communications channels in conjunction with the Chief Information Officer, including arrangements for the staff intranet;

iv establishing appropriate mechanisms, in conjunction with the Chief Information Officer. to ensure compliance with the policies and regulations set out in this document (UPR IM19).

3.1.2 Responsibility for content creation and updating will be delegated to Heads of Strategic Business Units and other authorised staff, as appropriate.

4 RESPONSIBILITIES OF HEADS OF STRATEGIC BUSINESS UNITS

4.1 Networks

4.1.1 Heads of Strategic Business Units are responsible for:

i ensuring that all computer network development and provision is undertaken by staff authorised by the Chief Information Officer to carry out such work;

ii preventing unauthorised access to equipment connected to the staff network;

iii maintaining a local equipment inventory for any equipment that is not managed by LCS, together with the location of that equipment.

4.2 Computer Security

4.2.1 Heads of Strategic Business Units will ensure that local computer systems security policies incorporate appropriate monitoring procedures to ensure compliance with all of the regulations set out in this document and will designate a member of staff within their area (a 'designated person') who will be responsible to them for ensuring compliance with these regulations.

4.3 Licence management

4.3.1 Heads of Strategic Business Units will ensure that:

i a record is maintained of all Product for which the Strategic Business Unit holds local Licences and, where appropriate, the names of the individuals to whom the Product has been made available and/or the serial number(s) of the computer(s) onto which each copy of the Product has been loaded;

ii the Members of the University for whom they are responsible are informed of the terms and conditions under which any Product made available to them may be used;

iii Product procurement and licensing does not duplicate Product already available through University-wide site Licences;

iv advice is sought from the Chief Information Officer and Head of Procurement prior to the acquisition of new or additional Product.

4.4 **Websites, external and intranets**

4.4.1 Heads of Strategic Business Units are responsible for:

i the establishment and co-ordination of appropriate arrangements to create content; maintaining the currency, accuracy and relevance of information and materials made available via the Internet, extranets and intranets, including StudyNet and StaffNet, and social media; ensuring that content is appropriate to the audiences using the respective media, and related quality management measures; in accordance with the arrangements agreed with the Pro Vice-Chancellor (Enterprise) and Director of Marketing and Communications and the Chief Information Officer;

ii the appointment of a designated School/Strategic Business Unit 'content key contact' who will report to the Dean of School/Head of Strategic Business Unit; for notifying the Pro Vice-Chancellor (Enterprise) and Director of Marketing and Communications (or nominee) of these appointments and for ensuring that these members of staff receive the necessary training to enable them to discharge their responsibilities for content and liaison;

iii liaison with the Pro Vice-Chancellor (Enterprise) and Director of Marketing and Communications (or nominee) concerning the presence, format and content of any Internet or extranet web pages, including University use of social media and virtual worlds in connection with the policy set out in section 4 of this document;

iv liaison with the Chief Information Officer (or nominee) concerning Internet, extranet and intranet addresses, access arrangements and technical issues;

v ensuring that Internet and extranet web pages are held on the University's web servers registered for external use;

vi initial approval of all local requests for subsites and microsites and the referral of such requests to the Pro Vice-Chancellor (Enterprise) and Director of Marketing and Communications for consideration in conjunction with the Chief Information Officer prior to the commissioning of any subsite or microsite development work;

vii promotion and use of the agreed University on-line communications arrangements;

viii promotion of and compliance with the policies, regulations and procedures set out in this document among colleagues.

5 **RESPONSIBILITIES OF MEMBERS OF THE UNIVERSITY**

5.1 Members of the University should understand fully their responsibilities in relation to information security and comply with the relevant University policies and regulations. Managers will be responsible for defined areas of information security.

5.2 Members of the University in Membership B[5] are responsible for:

i the relevance, accuracy and currency of the information contained in web, extranet and intranet pages and social media which they have created or for which they have been assigned responsibility, including personal academic and professional staff profiles, monitoring any responses, and for ensuring that the content is consistent with the aims and objectives of the University.

ii knowing the contents of relevant policies and procedures;

iii ensuring that any use of the Internet, on-line communications and social media is carried out in line with this and other relevant policies;

iv seeking relevant authorisation for official postings prior to publication;

v ensuring that all students have read, understood and agreed to the code of conduct /acceptable use policy, before accessing and posting content on University intranet and social media sites, including StudyNet.

APPENDIX II – IT AND CYBER SECURITY

Structure

1 IT AND CYBER SECURITY

1.1 This appendix to UPR IM20, IT and Computing Regulations, must be read in conjunction with the whole UPR and its other appendices. The substantive UPR lays out the regulations for general users of IT systems – the appendices determine the regulations under which these systems will be managed and operate.

1.2 All notifications to the Chief Information Officer required under these regulations should be made through the Helpdesk.

1.3 The University's IT systems will be configured, monitored and managed in accordance and compliance with the UK HM Government Cyber Security Essentials Scheme:

https://www.cyberessentials.ncsc.gov.uk/advice/

1.4 The Chief Information Officer may, in exceptional circumstances, deny an individual access/usage to University IT facilities. Such cases must be reported by the Chief Information Officer to the Vice-Chancellor.

2 COMPUTER NETWORK PERFORMANCE AND SECURITY

2.1 Internal computer network connections

2.1.1 All connections to the University's computer networks must conform to the protocols defined by the Chief Information Officer (or nominee) and with the requirements that apply to IP addresses. Abuses of, or failure to comply with, these requirements will result in immediate disconnection from the network and the withdrawal of the individual's user privileges. Such instances will be reported by the Chief Information Officer to the Vice-Chancellor.

2.1.2 All cabling installations must be in accordance with the standards agreed by the Chief Information Officer and the installation work must be approved by the Department of Estates, Hospitality and Contract Services. Requests for the installation of cabling must be made using the appropriate University request procedure.

2.1.3 Only staff authorised by the Chief Information Officer are permitted to install and maintain active network equipment including hubs, switches, routers, line-of-sight and wireless network units connected to the University's network. The specification of any equipment must be agreed by the Chief Information Officer.

2.1.4 'Public access' equipment may only be connected to the student network.

2.1.5 Equipment connected to the staff network, located outside of the University Data Centres, will not be set up to offer services to other users (for example, to act as servers) unless the prior written consent of the Chief Information Officer (or nominee) has been obtained. This consent will normally exclude all external access.

2.1.6 Equipment connected to the staff network must be located in 'staff only' areas. For the purposes of this document, a 'staff only' area is defined either as an area which students may not enter or, exceptionally, an area which students may not enter unless they are accompanied at all times by a member of staff or unless they are research students authorised by the Chief Information Officer to use that area.

2.1.7 Authorised use of IT equipment connected to the staff network is restricted to those Members of the University in Membership B (UPR GV06[2], refers) and Postgraduate Research students who share research facilities with staff, and who must have entered into an appropriate confidentiality agreement with the University and formally agreed to comply with the University's policies and regulations.

2.1.8 The staff network is linked to the student network by a 'firewall'. This 'firewall' permits access from the staff network to the services and systems, including the internet, connected to the student network. The Chief Information Officer will establish appropriate mechanisms for monitoring the 'firewall'.

2.1.9 Equipment will be connected either to the staff network or to the student network, but never to both.

2.2 **External data communications**

2.2.1 All external data communications will be conducted through the University's Janet connection, or other approved links.

2.2.2 No other external network connections, including use of ISDN lines, on premises owned, managed or occupied by the University or its wholly-owned subsidiary companies, may be made without the prior written consent of the Chief Information Officer (or nominee).

2.2.3 Off-campus access over the internet and on-campus wireless network access to the University's networked services is available for Members of the University via the University's secure access service (VPN). These routes provide authenticated access to designated information systems and services using the individual member's normal University username and password. Approved suppliers for whom off-campus access has been identified as essential by the appropriate Head of Strategic Business Unit and notified in writing to the Chief Information Officer (or nominee), will also be granted access.

2.3 **Boundary firewalls and internet gateways**

2.3.1 The default administrative password for any firewall (or equivalent network device) should be changed to an alternative, strong password.

2.3.2 Each rule that allows network traffic to pass through the firewall (e.g. each service on a computer that is accessible through the boundary firewall) should be subject to approval by an authorised individual and documented (including an explanation of business need).

2.3.3 Unapproved services, or services that are typically vulnerable to attack (such as Server Message Block (SMB), NetBIOS, tftp, RPC, rlogin, rsh or rexec), should be disabled (blocked) at the boundary firewall by default.

2.3.4 Firewall rules that are no longer required (e.g. because a service is no longer required) should be removed or disabled in a timely manner.

2.3.5 The administrative interface used to manage boundary firewall configuration should not be accessible from the internet.

2.3.6 In situations where the administrative interface needs to be accessible from the internet (e.g. because it is supported by a remote administrator or external service provider) the interface should be protected by additional security arrangements, which include using a strong password, encrypting the connection (e.g. using SSL), restricting access to a limited number of authorised individuals, and ultimately 2-factor authentication for the most sensitive data and only enabling the administrative interface for the period it is required.

2.4 **Domain Name Services and Internet Protocol (IP) addresses**

2.4.1 All Domain Name Services (DNS) activity will be managed and monitored centrally, for the whole University, by the Chief Information Officer (or nominee).

2.4.2 The Chief Information Officer is responsible for all University IP address range applications, and for the management, allocation and use of IP addresses.

2.4.3 All equipment connected to the University's computer networks must be assigned a unique IP address from within the University's official range of IP addresses. IP addresses must not be re-assigned to other items of equipment without the prior written consent of the Chief Information Officer (or nominee).

2.4.4 Members of staff must notify the Chief Information Officer of cases where an IP address is no longer required.

2.5 **Additional or changed equipment**

2.5.1 The Chief Information Officer (or nominee) must be advised, in advance and at the earliest opportunity, of any plan to add items of equipment to or to replace or to re-locate equipment that is connected or may require connection to the University's computer network, or of any plan involving a new use, a change of use or addition to the University's computer networks that might impact on the performance or security of the computer networks, such as wireless networks, video conferencing, the use of networked multimedia applications and document imaging systems.

2.5.2 The Chief Information Officer (or nominee) will assess the likely impact on the University's computer networks of the proposed change. The Chief Information Officer (or nominee) will give approval for the proposed change only where appropriate adjustments can be made to accommodate any effects on network traffic that this change MIGHT cause.

2.5.3 All new or changed uses of the computer networks must be approved by the Chief Information Officer (or nominee).

2.5.4 Prior to their installation in the 'live' situation, major network developments should be 'soak-tested' in off-line simulation.

2.5.5 For up to two (**2**) months after the live installation of the new development, the network provision that it is to replace should, wherever possible, remain in place as a 'fall-back' in the event of any subsequent failure of the new development when it is subject to actual user demand.

2.6 **Computer network provision in new and refurbished buildings**

2.6.1 Network provision for new and refurbished buildings will normally be in accordance with the specification ('the standard specification') published from time-to-time by the Chief Information Officer.

2.6.2 The standard specification will be reviewed annually by the Chief Information Officer.

2.6.3 Where the network requirements of a specialist area or activity need a network provision that exceeds the standard specification, the Head of Strategic Business Unit concerned will advise the Chief Information Officer and the appropriate Project Manager of these requirements at the earliest opportunity.

2.6.4 The Project Manager will seek advice from the Chief Information Officer (or nominee) concerning the technical use and cost implications of the proposal. This information will form part of any submission, by the Project Manager, for additional funding to meet the costs of the enhanced network provision that is required.

3 SECURITY OF DATA CENTRES, COMMUNICATIONS ROOMS AND CABINETS

3.1 Access to Computer Network Equipment and Data Centres

3.1.1 All data centres, communications rooms and cabinets will be kept locked at all times.

3.1.2 Other than in an emergency, access to data centres, communications rooms, cabinets and their contents and computer network equipment is restricted to persons authorised by the Chief Information Officer (or nominee). All other entry and interference with computer network equipment is strictly prohibited

3.1.3 In the event of fire or other emergency, Security Staff and/or staff of the Department of Estates, Hospitality and Contract Services and/or the emergency services and/or agreed University contractors, may enter a Data Centre or Communications Room without prior permission, to deal with the incident. The Chief Information Officer (or nominee) must be notified of such entry as soon as reasonably possible.

3.1.4 For regular authorised access to Data Centres, a person must complete a Data Centre Access Request Form and obtain an authorised access card from the Chief Information Officer (or nominee).

3.1.5 All persons granted authorised access to Data Centres must undertake the required training and comply fully with Data Centre security requirements and all relevant University policies and regulations.

3.1.6 Access control standards must be established for all Data Centres which minimise security risks yet allows the University's business processes to be carried out without undue hindrance. Procedures for managing the registration and de-registration of the authorisation of persons requiring access to Data Centres locations shall be established to ensure that all users access privileges match their authorisations. Authorisations and access privileges will be reviewed at regular intervals. The Chief Information Officer will identify the authorised officers to manage and implement these procedures.

3.1.7 Where a University post has designated specific Data Centre responsibilities, this will be made clear in the Job Description and staff appointed to such posts must receive an appropriate briefing and training as part of their induction.

3.1.8 Where computer network equipment is housed in accommodation used for another purpose, the arrangements for access by another user of that accommodation will require the prior written consent of the Chief Information Officer (or nominee). This consent will specifically exclude access by the other user to any communications cabinets or computer network or systems equipment located in the shared accommodation.

3.2 Contractors and visitors

3.2.1 All contractors requiring regular and agreed access to Data Centres must follow the requirements of 3.1 above and sign in and out of the Data Centre on each occasion.

3.2.2 Contractors undertaking equipment maintenance, computer network services and information systems work must have obtained the prior approval of the Chief Information Officer (or nominee) and must also have obtained the appropriate authorisation and the necessary Contractors' badge in accordance with the procedures established by the Director of Estates, Hospitality and Contract Services and the requirements of the University's security regulations and procedures (UPR HS05[7], refers).

3.2.3 Contractors who fail to comply with these requirements may be challenged and may be asked to leave University premises if they are unable to produce a valid badge and the necessary authorisation.

3.2.4 Contractors must be advised of their obligation to observe any specific access conditions which apply within the areas in which they will be working.

3.2.5 Other contractors and visitors requiring ad hoc access to Data Centres must be escorted at all times by an authorised person nominated by the Chief Information Officer (or nominee); comply with the provisions of this University policy and regulation and comply with any specific instructions given by the authorised person during the course of their visit to the Data Centre

3.2.6 External suppliers who are contracted to supply goods and services to the University that will bring them into contact with the University's Data Centre or Communications Room environment must agree to comply with the Data Centre and Communications Room Security arrangements set out in this document and with all other relevant University policies and regulations.

3.3 **Compliance**

3.3.1 Data Centre and Communications Room management processes must enable the University to comply with its legal, statutory and contractual obligations and any national agreements that it has entered into.

3.3.2 Data Centres must be safeguarded appropriately, especially when left unattended. Controls will be established to ensure the safety and security of the Data Centre environment.

3.3.3 It is the responsibility of each individual working within a Data Centre or Communications Room to ensure compliance with agreed good Health and Safety practices. To limit their exposure to personal Health and Safety risks, Members of the University working within Data Centre environments will comply with the following Code of Practice:

a no food or drink may be brought into University Data Centres;
b packaging and/or waste materials must never be left inside;
c furniture must not be brought into any Data Centre without the express permission of the Data Centres Manager, and must be fire resistant;
d aisles and exit routes must not be obstructed;
e cabinet keys must not be left in the racks (a key safe is provided for storage);
f power extension cables must never be used;
g the correct equipment for the job, for example, tile lifters or stepladders must always be used;
h the door to the Data Centre must never be propped open;
i no one must be allowed to 'tail-gate' behind another person entering a Data Centre legitimately.

---

[7] UPR HS05 'Security and Public Access'

3.3.4 The risk to human life associated with the fire suppression system must be fully understood and training undertaken in the emergency evacuation of the Data Centre.

3.3.5 All authorised persons with access to Data Centres are required to participate in annual refresher training in the safe and secure use of Data Centres. Access to Data Centres may be revoked where authorised users fail to undertake the required refresher training.

3.3.6 All authorised persons with access to Data Centres must comply with health and safety requirements for lone working, working in confined spaces, electrical safety and hazardous chemicals.

3.3.7 Any contracts with facilities management or outsourcing companies must have incorporated within them agreed service levels consistent with the regulations set out in this document so that Data Centre and Communications Room security and compliance issues are addressed.

3.4 **Operations**

3.4.1 To ensure on-going compliance with Data Centre security requirements, changes to operating procedures will require the prior written approval of Chief Information Officer (or nominee).

3.4.2 The specification of any equipment to be installed in a Data Centre or Communications Room and the arrangements for the installation of that equipment must have the prior written consent of the Chief Information Officer (or nominee).

3.4.3 Acceptance criteria for new information systems, upgrades and new versions shall include reference to the sustainability of those systems within the University's Data Centres.

3.4.4. The Chief Information Officer (or nominee) will:

i determine and disseminate procedures for the reporting of incidents, security breaches and potential security weaknesses in the University's Data Centres;

ii implement monitoring arrangements to inform Data Centre management;

iii determine and disseminate procedures for the reporting of Data Centre equipment malfunctions and faults;

iv require that all faults and malfunctions are logged and monitored and that corrective action is taken in a timely manner.

3.4.5 The Data Centres Manager must be informed of all breaches of Data Centre security through regular reporting channels and in emergencies. The Data Centres Manager must report major breaches immediately to the Chief Information Officer.

3.5 **Planning and Changes**

3.5.1 Changes to equipment supporting critical business systems must be planned in advance to ensure that adequate processing power, storage and network capacity are available for current and projected needs, all with appropriate levels of resilience and fault tolerance. Equipment shall be correctly maintained.

3.5.2 The implementation of new systems or related projects must be agreed by the Chief Information officer (or nominee) prior to installation into the Data Centre.

3.5.3 Equipment supporting critical business systems shall be given adequate protection from unauthorised access, environmental hazards and electrical power failures.

3.5.4 Capacity demands of systems supporting business processes shall be monitored and projections of future capacity requirements made to enable adequate processing power, storage and network capacity to be available.

4 INFORMATION SECURITY

4.1 Development and support of information security processes

4.1.1 This policy should be read in conjunction with the University's Data Management Policy (UPR IM16[8]) and its appendices.

4.1.2 It is the policy of the University to implement processes to protect the security and confidentiality of its management and administrative information. These processes will:

i identify who may be permitted to access the University's management and administrative information;

ii stipulate the extent to which these individuals may be permitted to manipulate the University's management and administrative information;

iii make clear the obligation placed on authorised workers to maintain security and confidentiality;

iv specify the arrangements for the release of information;

v establish mechanisms to secure management and administrative information against loss, damage, corruption or unauthorised access or use.

4.1.3 The University will address security issues during the purchase and implementation of all new management and administrative information systems. All management and administrative information systems purchased or implemented by the University will, therefore, be capable of compliance with these regulations.

4.1.4 Heads of Strategic Business Units will develop and maintain local management and administrative information security policies which are consistent with this policy for those areas for which they are responsible. They will ensure that members of staff receive training on information security policies that may apply and any amendments that may be made to these subsequently.

4.1.5 The People Development team will ensure that the induction programme for all new staff includes specific information and advice concerning this policy and local management and administrative information security policies.

4.1.6 **Compliance**
Information management processes must enable the University to comply with its legal and statutory obligations and any contractual obligations and national agreements it has entered into.

4.2 Outsourcing and Third-Party Access

4.2.1 External suppliers who are contracted to supply goods and services to the University that will bring them into contact with the University's information resources must agree to abide by the relevant UPRs. UH staff must proactively monitor contractors to ensure that the abide by

[8] UPR IM16 'Data Management Policy'

those UPRs and any other requirements and take appropriate action in the event of a breach. Access rights for suppliers must be terminated as soon as that access is no longer required, and password changes made where there are staffing changes within that supplier.

4.2.2 Any contracts with facilities management or outsourcing companies must include service levels that address information security issues and conform to this policy.

4.2.3 Any contracts which provide services that are hosted off-site (in "the cloud") must include service levels and contractual obligations that address information security and data protection issues, have a data access agreement in place and conform to this policy.

4.3 **User Management**

4.3.1 Access to all systems must be authorised by the Data Steward (as defined in UPR IM16[8]) and/or manager responsible for the information system and a record must be maintained of such authorisations, including the appropriate access privileges and user roles granted.

4.3.2 Procedures shall be established for all information systems to ensure that the access privileges of Members of the University are adjusted appropriately, and in a timely manner, whenever there is a change in business need or role or the Member leaves the University. Members' access privileges will be reviewed at regular intervals.

4.3.3 Termination of Membership or change of Membership status within the University will result in a modification of information system access privileges as stipulated in UPR IM01[3].

4.3.4 Where a post has a specific Information Security responsibility this will be made clear in the job description. All Members of the University should have a clear understanding of their responsibilities under the Information Security Policy and should receive an appropriate briefing at induction.

4.3.5 The Chief Information Officer will maintain a list of all authorised Data Stewards and their nominees and their respective areas of responsibility (Appendix I, UPR IM16[1], refers).

4.4 **Systems Administrators and users with special privileges**

4.4.1 The Data Steward (or nominee) designated for the management and administrative information concerned, is responsible for the authorisation of special access privileges and user roles for use of the management and information system through an authorisation process agreed with the Chief Information Officer. These should be restricted to a limited number and reviewed on a regular basis.

4.4.2 All authorised access privileges and user role(s) for Members of the University will be notified to the Chief Information Officer who will arrange for their recording and secure implementation using an individual University username and password for each authorised person.

4.4.3 Administrative accounts should only be used to perform legitimate administrative activities.

4.5 **Procedures**

4.5.1 The security risks to the information assets of all system development projects shall be assessed and access to those assets shall be controlled.

4.5.2 Changes to operational procedures must be controlled to ensure ongoing compliance with the requirements of information security and must have appropriate management approval.

4.5.3 The procedures for the operation and administration of the University's business systems and activities must be documented with those procedures and documents being regularly reviewed and maintained.

4.5.4 Duties and areas of responsibility shall be segregated to reduce the risk and consequential impact of information security incidents that might result in financial or other material damage to the University.

4.5.5 Procedures will be established and widely communicated for the reporting of security incidents and suspected security weaknesses in the University's business operations and information processing systems. Mechanisms shall be in place to monitor and learn from those incidents.

4.5.6 Procedures will be established for the reporting of software malfunctions and faults in the University's business critical information processing systems. Faults and malfunctions shall be logged and monitored and timely corrective action taken.

4.5.7 Development and testing facilities for business-critical systems shall be separated from operational facilities and the migration of software from development to operational status shall be subject to formal procedures.

4.5.8 Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to migration to operational status. Tests involving live data or periods of parallel running may only be permitted where adequate controls for the security of the data are in place.

4.5.9 Procedures shall be established to control the development or implementation of all business-critical operational software. All systems developed for or within the University must follow, as a minimum, the University's Project Management Guidelines.

4.6 **Secure Information handling**

4.6.1 The creation and management of records must conform to the University's record management policy (UPR IM11[9], refers).

4.6.2 An inventory will be maintained of all the University's business critical information assets and the ownership of each asset will be clearly stated. Each asset will be classified according to sensitivity using the University's agreed information security classification scheme.

4.6.3 When permanently disposing of equipment containing storage media, all sensitive data and licensed software will be irretrievably deleted before the equipment is moved off site.

4.6.4 Areas and offices where sensitive or critical information is processed shall be given an appropriate level of physical security and access control. Members of the University with authorisation to enter such areas are to be provided with information on the potential security risks and the measures used to control them.

4.6.5 Screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons.

4.6.6 Individuals responsible for business-critical systems must ensure that appropriate backup and system recovery procedures are in place.

[9] UPR IM11 – 'Records Management'

4.6.7 Backup of the University's information assets and the ability to recover them is an important priority. Management is responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of the University.

4.6.8 Management must ensure that safeguards are in place to protect the integrity of information during the recovery and restoration of data files, especially where such files may replace files that are more recent.

4.6.9 Prior to sending sensitive information or documents to third parties, the intended recipient must be authorised to receive the information and the procedures and information security measures adopted by the third party must also be seen to continue to assure the confidentiality and integrity of the information.

4.6.10 Sensitive data or information may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured.

4.6.11 All parties/participants are to be notified in advance whenever telephone conversations or videoconference events, such as lectures, are to be recorded.

4.6.12 The identity of recipients or requesters of sensitive or confidential information via the telephone must be verified and they must be authorised to receive the information requested.

4.6.13 No University computer should store credit card or debit card data. The use of credit and debit cards to pay on-line for University services should only be via a University-approved payment agent and with the prior agreement of the Group Finance Director (or designated deputy).

4.7 **Mobile computing**

4.7.1 Members of the University accessing information systems remotely to support business activities must be authorised to do so by an appropriate authority within the University. A risk assessment, based on the criticality of the information asset being used, must be carried out. Where technically feasible, all access should be through the VPN.

4.7.2 The University will publish guidelines for users of mobile computing equipment advising them on how these should be used to conform to the University's information security policy and other good practices.

4.8 **Systems Development and Changes**

4.8.1 The implementation of new or upgraded software must be planned and managed carefully and any development for or by the University must always follow the University's Project Management Guidelines.

4.8.2 Information security risks associated with such projects must be mitigated using a combination of procedural and technical controls.

4.8.3 Formal change control procedures, with comprehensive audit trails, must be used for all changes or upgrades to business software. All changes must be properly authorised and all software, including that which interacts with the amended software, must be tested before changes are moved to the live environment. Changes to vendor supplied systems must be approved by the vendor. All software shall be checked before implementation to protect against malicious code.

4.8.4 Prior to acceptance, all new or upgraded systems shall be tested to ensure that they comply with the University's information security policies, access control standards and requirements for on-going information security management.

4.8.5 New information systems or enhancements to existing systems must be authorised jointly by the manager(s) responsible for the information and the Chief Information Officer. The business requirements of all authorised systems must specify requirements for security controls.

4.8.6 Business requirements for new software or enhancement of existing software shall specify the requirements for information security controls. The information assets associated with any proposed new or updated systems must be identified, classified and recorded, in accordance with the University's record management policy (UPR IM11[7], refers) and a risk assessment undertaken to identify the probability and impact of security failure.

4.8.7 Equipment supporting critical business systems shall be planned to ensure that adequate processing power, storage and network capacity are available for current and projected needs, all with appropriate levels of resilience and fault tolerance. Equipment shall be correctly maintained.

4.8.8 The implementation of new or upgraded software and/or data loads by external suppliers and third-party organisations is subject to prior planning and agreement with the University through the relevant trained and qualified systems management staff.

4.9 **Systems management and maintenance**

4.9.1 The University's systems shall be managed by suitably trained and qualified staff to oversee their day-to-day running and to preserve security and integrity in collaboration with individual system owners. All systems management staff shall be given relevant training in information security issues.

4.9.2 Access controls shall be maintained at appropriate levels for all systems and applications by on-going proactive management. Any changes of access permissions must be authorised by the Data Steward and/or manager of the information system or application and a record of the access permissions granted must be maintained.

4.9.3 Access to operating system commands and system administration functions on servers is to be restricted to those persons who are authorised to undertake these operations as part of their job description. Server administration accounts should only be used to perform legitimate administrative activities and should not be granted access to email or the internet. Server administration account passwords should be changed on a regular basis.

4.9.4 Where feasible, inactive connections to the University's business systems shall shut down after a defined period of inactivity to prevent access by unauthorised persons.

4.9.5 Capacity demands of systems supporting business processes shall be monitored and projections of future capacity requirements made to enable adequate processing power, storage and network capacity to be available.

4.9.6 Security event logs, operational audit logs and error logs must be properly reviewed and managed by qualified staff.

4.9.7 System clocks must be regularly synchronised between the University's various processing platforms.

4.9.8 Equipment supporting critical business systems shall be given adequate protection from unauthorised access, environmental hazards and electrical power failures.

4.10 **Information Security Reporting**

The Chief Information Officer must be informed of all breaches of information security immediately. The Chief Information Officer should bring major breaches to the notice of the University's Data Protection Officer within the Office of the Vice-Chancellor.

5 COMPUTER VIRUS AND MALWARE PROTECTION MANAGEMENT

5.1 Virus and malware detection software

5.1.1 The Chief Information Officer is responsible for the distribution, installation and updating of the approved virus detection software on all University systems, services and computing equipment across the University.

5.1.2 Where appropriate, the Chief Information Officer will arrange for the approved virus detection software to be available to designated authorised persons who will then be responsible for distributing and/or installing the software and any subsequent updates to it, on all computer systems for which they are responsible.

5.1.3 All approved virus detection software that is in use within the University, by its wholly-owned subsidiary companies or their wholly-owned subsidiaries, must be updated at least daily.

5.1.4 All new IT equipment and mobile devices or those which have be re-commissioned should be installed without a network connection until virus detection software has been installed and the equipment is ready to have security updates applied.

5.1.5 Malware protection software should be configured to scan files automatically upon access (including when downloading and opening files, accessing files on removable storage media or a network folder) and scan web pages when being accessed (via a web browser).

5.1.6 Malware protection software should be configured to perform regular scans of all files (eg daily).

5.1.7 Malware protection software should prevent connections to malicious websites on the internet (eg by using website blacklisting).

5.2 Patch management

5.2.1 Software running on computers and network devices that are connected to or capable of connecting to the internet should be licensed and supported (by the software vendor or supplier of the software) to ensure security patches for known vulnerabilities are made available.

5.2.2 Updates to software (including operating system software and firmware) running on computers and network devices that are connected to or capable of connecting to the internet should be installed in a timely manner.

5.2.3 Out-of-date software (i.e. software that is no longer supported) should be removed from computer and network devices that are connected to or capable of connecting to the internet.

5.2.4 All security patches for software running on computers and network devices that are connected to or capable of connecting to the internet should be installed in a timely manner.

5.3 **Secure configuration**

5.3.1 Unnecessary user accounts (e.g. Guest accounts and unnecessary administrative accounts) should be removed or disabled.

5.3.2 Any default password for a user account should be changed to an alternative, strong password.

5.3.3 Unnecessary software (including application, system utilities and network services) should be removed or disabled.

5.3.4 The auto-run feature should be disabled (to prevent software programs running automatically when removable storage media is connected to a computer or when network folders are accessed).

5.3.5 A personal firewall (or equivalent) should be enabled on desktop PCs and laptops, and configured to disable (block) unapproved connections by default.

APPENDIX III – EXTERNAL WEBSITE MANAGEMENT POLICY

Structure

1 INTRODUCTION

This appendix to UPR IM20 'IT and Computing Regulations' should be read in conjunction with the whole UPR and its other appendices, and UPR EQ10[10]; UPR SA12[11]; UPR IM08[12]; UPR IM02[13], the 'JANET Acceptable Use Policy' (section 4.5.1, UPR IM20, refers) and the staff computing guide.

2 SCOPE

This document sets out the regulations and procedures which Members of the University posting, exchanging and publishing information and/or other services via the Internet (section 3.3, refers), an extranet (section 3.4, refers) or an intranet, including StudyNet and StaffNet, (sections 3.5, 3.6 and 3.7, refer), using social media (sections 3.14 and 3.19, refer) are required to follow.

3 DEFINITIONS

For the purposes of this document, the following definitions will apply:

3.1 '**URL':**
('Uniform Resource Locator') a web address used to identify a particular service or resource delivered via a web browser.

3.2 '**Internet**':
a world-wide system of networks and information systems which can be accessed by the general public; This includes, but is not limited to, web sites, on-line communications services and social media

3.3 '**extranet**':
a collection of networked information systems belonging to the University of Hertfordshire which may be accessed by Members of the University and specific groups outside the University (it should be noted that regulations set out in this document which apply to the Internet also apply to extranets);

3.4 '**intranet**':
a collection of networked information systems belonging to the University of Hertfordshire, access to which is restricted to those Members of the University who have been granted access;

---

10 UPR EQ10 'Bullying and Harassment'
11 UPR SA12 'Learning Resources'
12 UPR IM08 'Data Protection Policy and Privacy Statement'
13 UPR IM02 'Information Management Policy'

3.5 **'University web page'**:

a web page which belongs to some identifiable entity or organisational unit, for example, a School, programme, module or society or an individual, for example, a member of staff or a member or officer of a society, that is publicised to be used as part of the Internet or an intranet;

3.6 **'microsite' and 'subsite'**:

a group of web pages which may be used to present a specialised and discreet and/or time-limited set of content and which may function as a distinct supplement to a primary website accessible from the parent website and within the overall information architecture ('subsite'), or where the content is peripheral to the main business of the University, as a separate website ('microsite') which may have a separate design and may be accessed via a distinct web address;

4 POLICY

4.1 The University will use the Internet and social media as a means of building reputation and relationships, inspiring and attracting 'new business' interest from key external audiences, converting interest into commitment and action, showcasing the University's expertise and achievements and disseminating information.

4.2 The University will, as appropriate, use the Internet, extranets and intranets (including StudyNet and StaffNet) and social media to provide information and services to Members of the University and the wider community and to deliver teaching and learning materials, in accordance with University policies, to individuals who are entitled to access them under the provisions of the University's Information Management Principles (UPR IM02[14], refers).

4.3 When made available on-line, information intended solely for use by members of the University's staff will be published on the staff intranet.

5 REGULATIONS

5.1 University web pages (including internet, extranet and intranet, StudyNet and StaffNet,and use of social media and virtual worlds)

5.1.1 Web hyperlinks

Although many University web pages will be concerned principally with information relating to the Strategic Business Unit from which they originate, they must comply with the design, information architecture, navigation, style and terminology agreed for the University's corporate web site and intranets. Within this framework, web hyperlinks should be incorporated. where appropriate, to general information to which unrestricted access has been granted by University management, available on the Internet, concerning the University and its activities.

5.1.2 Corporate identity

All University web pages and use of social media and virtual worlds must incorporate the standard form of the University of Hertfordshire brand and logo as determined by the Pro Vice-Chancellor (Enterprise) and Director of Marketing and Communications.

---

[14] UPR IM02 'Information Management Principles'

Marketing and Communications will provide a library of information, for example, logos and photographic materials, which can be accessed by staff setting up web pages and presences in agreed social media and virtual worlds.

5.1.3 **University website terms and conditions**

The University website terms and conditions and privacy policy apply to every University web page (Appendix I, UPR IM19, refers), and must have a hyperlink from all University websites and FTP servers.

6 REQUESTS FOR NEW WEB ADDRESSES

Requests for new web addresses, those using 'herts.ac.uk' and other domain names should be sent to dns.reg@herts.ac.uk. A minimum of five (**5**) working days' notice is required for the approval, registration and assignment of a new web address.

6.1 Principles and policies

6.1.1 Web addresses should always use all lower case letters and contain no spaces, underscores or URL encoded characters.

6.1.2 The website or service name used for a web address:

a should be transparent and easily understood by the intended user;
b should clearly, unambiguously and succinctly describe the service to be delivered;
c should take account of names in common usage;
d should not refer to the name of the server or the product used to deliver the service.

6.1.3 The 'herts.ac.uk' domain is the University's primary registered domain and should be used for the majority of information and services provided by the University;

6.2 Use of the 'herts.ac.uk' domain

6.2.1 The web address 'www.herts.ac.uk' is used for the University external website.

6.2.2 All material published to this web address will be publicly accessible and the Pro Vice-Chancellor (Enterprise) and Director of Marketing and Communications (or nominee) has full editorial control of all content published via this web address.

6.2.3 To enhance the optimisation of search rankings for the external website, the 'www' prefix to the 'herts.ac.uk' web address is reserved for the exclusive use of the University external website.

6.2.4 None of the published web addresses for other University web-based services should include the 'www' prefix. To meet user expectation and for ease of use, if a user enters the 'www' prefix when requesting other services, re-direction to the correct service will be provided.

(**Note:** Therefore, a member of staff entering 'www.staffnet.herts.ac.uk' would be re-directed automatically to 'staffnet.herts.ac.uk' with the latter address displaying in the browser address bar.)

6.2.5 The format '[servicename].herts.ac.uk' is to be used for University web-based services other than the University external website.

(**Note:** Examples would include:

'netmail.herts.ac.uk' for web access to the staff email service;
'staffnet.herts.ac.uk' for the University staff intranet;
'hr.herts.ac.uk' for the HR system staff portal.)

6.2.6 Agreed 'microsites' that relate to the work of the University but that are not 'subsites' of the University external website should use the web address format '[micrositename].herts.ac.uk'

(**Note:** Examples of currently agreed microsites would include:

'kaspar.herts.ac.uk' and 'heritagehub.herts.ac.uk'.

Naming conventions for, and registration of, agreed microsites where it is not appropriate to use the 'herts.ac.uk' domain are given in section 6.)

6.2.7 Specific web content or a service with a registered 'herts.ac.uk' domain can also be referenced by a shortcut URL or web address.

(**Note:** This will facilitate the effective marketing of a significant section of a website or a specific service by providing a memorable and short web address for users. Shortcut URLs of this type currently take one of two forms, for example:

'go.herts.ac.uk/[shortname]' (therefore, ' http://go.herts.ac.uk/cpdhealth' is used instead of 'http://www.herts.ac.uk/more/professional-development-in-health/home.cfm')

or
'www.herts.ac.uk/[shortcutname]' for a shortcut to a distinct part of a larger site such as 'www.herts.ac.uk/law .')

6.3 **Use of other domains**

6.3.1 The use of other non 'herts.ac.uk' domains requires prior agreement and is acceptable only when the website or service is:

a an externally funded service or website (for example: 'www.dynamicsofvirtualwork.com');
b a collaborative funded or delivered project with multiple external partners (for example: 'www.tabsanetwork.org');
c a commercial venture (for example: 'www.uhonline.co.uk').

6.3.2 The Chief Information Officer may agree to the registration and purchase on behalf of the University of other non 'herts.ac.uk' domain names to protect the University from the use of web addresses by others that may confuse users searching for University web addresses and services or that may give rise to direct competition using web addresses similar to those used by the University. Web addresses obtained for these reasons should not be published or used.

Sue Grant
Secretary and Registrar
Signed: **13 November 2019**