IT and Computing Regulations

UPR IM20 version 02.0

Policies superseded by this document

This document replaces version 01.0 of UPR IM20, with effect from 3 January 2023.

Summary of significant changes to the previous version

This document has been amended to reflect current practices, such as the use of Multifactor Authentication (MFA), Canvas, Microsoft OneDrive. See sections 2.12, 3.2, 5.2, 7.2, 8.9.1, 8.11, 9.1.1, 10.5 and 10.6.2.

Links have also been updated.

Glossary

A glossary of approved University terminology can be found in **UPR GV08**.

Table of contents

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 (see Appendix I);

iii the security of IT systems (see Appendix II);

iv the external-facing website (see Appendix III).

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 and Digital 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 GV06[1];

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;

2.10 '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, Canvas 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:

[1] UPR GV06 ‘Membership of the University’

- 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, multi-factor authentication (MFA) or any other token (email address, smartcard, dongle, MFA token) 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 and Digital Officer. Where the Chief Information and Digital 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 Investigation 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,

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

- 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;

- 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 2018.

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 SA12[3].

[3] UPR SA12 'Learning Resources'

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**
  Jisc 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: https://subscriptionsmanager.jisc.ac.uk/about/jisc-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.

5.2 The University's IT facilities are managed by the Chief Information and Digital Officer, who advises on the content of these regulations. Unless indicated otherwise in the text of this document, the nominees of the Chief Information and Digital Officer are the Heads of Section in 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.

- Users must use multi-factor authentication (MFA) to access their University accounts, or any other systems holding University data, where available.

- 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 their 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 and Digital 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 their Membership of the University;

ii at the request of their Head of Strategic Business Unit and/or the Dean of Students;

iii where they are 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 and Digital 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 and Digital 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. Devices/operating systems which are no longer supported by the manufacturer must not be used to access the University network or services without the permission of the Chief Information and Digital Officer and additional security measures in place.

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 and Digital 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 (Microsoft OneDrive) 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 Microsoft OneDrive 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, their line manager is responsible for:

i ensuring that the contents of that staff member's computers, mobile devices and Microsoft OneDrive 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.

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 Microsoft OneDrive 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 Microsoft OneDrives 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 Microsoft OneDrive 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 All documents must be stored in accordance with the guidance provided on HertsHub, including the file storage to be used and any additional protection required.

9.1.2 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).

9.1.3 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.

9.1.4 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.

9.1.5 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.

9.1.6 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.

9.1.7 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.

9.1.8 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.

9.1.9 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.

9.1.10 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 will bear the University of Hertfordshire copyright mark in the format: '© University of Hertfordshire Higher Education Corporation (and year of creation of the copyright work)' (see UPR FR06[2]).

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.

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 their 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 and Digital 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 will 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 they post 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 (see Appendix III).

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 and Digital 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 Resourcing 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 will 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 and Digital Officer.

10.5 E-mail and other on-line communications including MS Teams and Zoom

10.5.1 Use of the University's e-mail service and other on-line communication media (including MS Teams and Zoom) is for academic, research and University business and social purposes only and not to be used for personal gain, in the employment of others, or for self-employment. 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 and Digital Officer, all electronic mail services will be managed centrally by the Chief Information and Digital 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 any data which for any reason cannot be stored on a University server is backed up on a regular basis.

10.6.2 Heads of Strategic Business Units will ensure that, any data which for any reason cannot be stored on a University server is backed up on a regular basis.

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 HertsHub.

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 and Digital 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 HR02[4] 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 SA13[5] 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.

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.

Sharon Harrison-Barker
Secretary and Registrar
Signed: **3 January 2023**

Alternative format
If you need this document in an alternative format, please email us at governanceservices@herts.ac.uk or telephone us on +44 (0)1707 28 6006.

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