COMPUTER NETWORK MANAGEMENT POLICY

SUMMARY OF PRINCIPAL CHANGES

General changes	
This document has been subject to the annual review process led by the Chief Information Officer and has been re-issued with amendments, effective 1 September 2014.	
Section	
5.2	Director Estates, Hospitality and Contract Services – refer to text
6.1.2	Refer to text
7.8	IP addresses – refer to text

---

*(Amendments to version **03.0**, Appendix I, UPR IM01, are shown in italics.)*

Structure

1 PURPOSE

1.1 This policy was originally approved by the Senior Executive Group with effect from 1 September 2001 has *been amended with effect from 1 September 2014 on the authority of the Secretary and Registrar.* It defines the arrangements and responsibilities for the development, installation, maintenance, use and monitoring of the University's computer networks to ensure that, other than during 'at risk' periods or when other agreed development and maintenance work is taking place, these networks are sufficiently adequate, reliable and resilient to support continuous high levels of activity. This document should be read in conjunction with the other component documents which together form UPR IM01[1]. The University's computer networks (as defined in section 2.1, UPR IM01[1]) are managed by the Chief Information Officer. The University's information systems (as defined in section 22.6, UPR IM01[1]) are accessed via and/or used in conjunction with the University's computer networks.

1.3 Nominee of the Chief Information Officer

Unless indicated otherwise in the text of this document, the nominee of the Chief Information Officer is the Chief Technology Officer.

2 SCOPE

This policy applies to any person accessing or using a computer network owned, managed, supported or operated by, or on behalf of, the University of Hertfordshire, including all Members of the University, as defined in UPR GV06[2] and any other organisation accessing services over University computer networks, including persons contracted to repair or maintain the University's computer networks and suppliers of network services.

3 USE OF THE UNIVERSITY'S COMPUTER NETWORKS

The University's computer networks are for use in connection with University business and for academic and research purposes only. No other use is permitted.

4 SECURITY OF THE STAFF NETWORK

4.1 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.

4.2 The Chief Information Officer will establish appropriate mechanisms for monitoring the 'firewall'.

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

4.4 Location of equipment connected to the staff network

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.

---

[1] UPR IM01 'Computer Networks, Security of Information Systems and the Protection of Information Systems from Computer Viruses'
UPR IM01, Appendix I 'Computer Network Management Policy'
UPR IM01, Appendix II 'Security of Management and Administrative Information Systems'
UPR IM01, Appendix III 'Protection of Information Systems from Computer Viruses, Spyware and Malware'
UPR IM01, Appendix IV 'Data Centre Security Policy'

[2] UPR GV06 'Member of the University'

4.5 **Authorised use of desktop services equipment connected to the staff network**

4.5.1 Authorised use of desktop services equipment connected to the staff network is restricted to those Members of the University in Membership B (UPR GV06[2], refers). This access/usage is conditional on the Member of the University concerned having entered into an appropriate confidentiality agreement with the University and having formally agreed to comply with the University's policies and regulations.

4.5.2 **Requests for use of desktop services equipment connected to the staff network for individuals who do not meet the criteria set out in section 4.5.1**

i Heads of Strategic Business Units may apply to the Chief Information Officer for access to be granted to other individuals who do not meet the criteria set out in section 4.5.1, where these individuals have essential duties which specifically require that they use services available only over the staff network, for example, the University's corporate management information systems.

ii In these cases, a written application must be made by the appropriate Heads of Strategic Business Unit to the Chief Information Officer. The application will indicate the level of access/usage of specific information systems and services required for the individual concerned, the proposed monitoring arrangements and the inclusive dates during which the access/usage is requested.

iii Heads of Strategic Business Units should note that it will be considered implicit that, in applying for access/usage under the provisions of this section (4.5.2), they undertake to ensure that the individual's access/usage to the staff network will be monitored and that he or she does not exceed the permitted level of access/usage.

iv Where a request for access/usage is approved, this approval will be conditional on the individual concerned having entered an appropriate confidentiality agreement with the University of Hertfordshire and having formally agreed to comply with the University's policies and regulations.

(**NOTE:**

A Confidentiality clauses are incorporated into the University's contracts of employment (fixed-term and open-ended). Other individuals granted Membership of the University in Membership B, or access/usage under the provisions of section 4.5.2 of this document, are required to complete and sign the appropriate University registration form. Managers should note that where they seek access for any of the individuals referred to in section 4.5.2, they are also responsible for ensuring that the individual for whom access is being sought has entered a binding confidentiality agreement with the University.)

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

4.5.4 **Public access equipment**

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

5 RESPONSIBILITIES IN RELATION TO THE MANAGEMENT OF THE UNIVERSITY'S COMPUTER NETWORKS

5.1 Chief Information Officer

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.

5.2 Director of Estates, Hospitality and Contract Services

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.

5.3 Heads of Strategic Business Units

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.

6 ACCESS TO COMPUTER NETWORK EQUIPMENT AND DATA CENTRES

6.1 Data centres, communications rooms, cabinets, computer network equipment

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

6.1.2 *Other than in an emergency (section 6.2, refers), access to data centres, communications rooms, cabinets and computer network equipment is restricted to designated staff as authorised by the Chief Information Officer.*

6.1.3 Entry to communications rooms and cabinets and interference with computer network equipment is strictly prohibited other than with the prior written consent of the Chief Information Officer (or nominee). Applications for such written permission must be made in writing to the Chief Information Officer (or nominee).

6.1.4 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.

6.1.5 Access and operation of University Data Centres must be in accordance with the detailed arrangements set out in Appendix IV, UPR IM01[1].

6.2 Access in an emergency

In the event of a fire or other emergency, security staff and/or staff of the Department of Estates, Hospitality and Contract Services and/or the emergency services may enter these areas, without permission, to deal with the incident.

6.3 Contractors

6.3.1 Contractors undertaking 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[3], refers).

6.3.2 Contractors must be advised of their obligation to observe any specific access conditions which apply within the areas in which they will be working. These access conditions include, in all cases, that contractors working in main Data Centres and communications rooms must be accompanied by appropriate University personnel.

6.4 Installation of cabling

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.

6.5 Installation of equipment

The specification of any equipment to be installed in Data Centres, communications rooms and cabinets and the installation of that equipment, will require the prior written consent of the Chief Information Officer (or nominee).

6.6 Network equipment

Only staff authorised by the Chief Information Officer are permitted to install and maintain active network equipment including hubs, switches, routers and wireless network units connected to the University's staff and student computer networks.

6.7 Wireless networks

All wireless network and line-of-sight network installations require the prior approval of the Chief Information Officer.

7 COMPUTER NETWORK CONNECTIONS AND USAGE

7.1 All computer network connections

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 (section 7.8, refers). 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.

---

[3] UPR HS05 'Security and Public Access'

7.2 Additional regulations relating to connections to the staff network

7.2.1 Only designated staff authorised specifically by the Chief Information Officer (or nominee), may make initial connections of equipment to the staff network.

7.2.2 Equipment connected to the staff network 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.

7.3 On-line computer file storage for staff

7.3.1 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.

7.3.2 On-line storage is made available to back-up and share files for academic and research work and other University-related activities only. No other use is permitted without the prior written permission of the Chief Information Officer.

7.3.3 Large amounts of storage required for specific purposes will normally be accommodated and must be notified in advance to the Chief Information Officer (or nominee) via the Helpdesk.

7.3.4 Staff must check their user store regularly to ensure that outdated and inappropriate material (such as personal photographs, personal music files or software installers) is removed.

7.3.5 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. The manager of the staff group using the shared area will be the nominated manager, unless he or she notifies the Chief Information Officer (or nominee) of an alternative nominee to whom this responsibility has been delegated.

7.3.6 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.

7.3.7 When backing-up their local computer hard drive and/or mobile devices to an on-line storage area staff must ensure that only appropriate material is backed up and that previous backups are removed.

7.3.8 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.

7.3.9 The University reserves the right to inspect the contents of user and shared stores as permitted under UPR IM19[4], 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.

---

4 UPR IM19 'Internet, Online Communications and Social Media'

7.3.10 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.

7.4 **External access to servers on the staff network**

7.4.1 Where specific external access is required to servers on the staff network, the Chief Information Officer (or nominee) will ensure that this access is strictly controlled. The Chief Information Officer (or nominee) will monitor compliance with the access arrangements that have been agreed.

7.4.2 Abuses of or failure to comply with these arrangements will result in immediate disconnection from the network.

7.5 **Domain Name Services**

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

7.6 **Electronic mail**

Unless agreed otherwise by the Chief Information Officer, all electronic mail services will be managed centrally by the Chief Information Officer (or nominee), 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.

7.7 **Suspension and/or termination of access to computer networks and information systems**

7.7.1 An individual's access to the University's computer networks 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.

7.7.2 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.

7.7.3 **Staff leaving the University**

The Director 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 so that these individuals' access to University on-line services and systems can be amended, suspended or deleted (as appropriate).

7.7.4 **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.

7.7.5 **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.

7.8 **Internet Protocol (IP) addresses**

7.8.1 *All notifications to the Chief Information Officer required under the regulations in this section (7.8), should be made through the Helpdesk.*

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

7.8.3 *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.*

7.8.4 *IP addresses must not be re-assigned to other items of equipment or duplicated without the prior written consent of the Chief Information Officer (or nominee).*

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

7.8.6 *Members of staff should quote the IP address for the relevant piece of equipment whenever reporting a fault or requesting a change either to the equipment or its usage.*

7.8.7 **Inventory control**

As part of their audit responsibilities, Heads of Strategic Business Units are required to record in their local equipment inventory records the IP address assigned to each item of equipment for which they are responsible, together with the location of that equipment.

7.9 **Connection to the student network of equipment that is the property of Members of the University**

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

(UPR GV06[2], refers)

Although these Members may apply for an IP address, using the procedures set out in section 7.8, to enable them to connect equipment to the student network, it should be noted that permission will be given only where the equipment meets the specification determined by the Chief Information Officer (or nominee) and that it poses no risk to network performance or security.

7.9.2 **Members of the University in Membership A**

(UPR GV06[2], refers)

These members connect equipment into mains power supplies as 'stand-alone' machines and use the on-campus data points or wireless networks to access the University's networked services.

7.10 **Additional or changed equipment**

7.10.1 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.

7.10.2 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.

7.11 **External data communications**

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

7.11.2 No other external network connections may be made without the prior written consent of the Chief Information Officer (or nominee). Applications for such written consent must be made in writing to the Chief Information Officer (or nominee).

7.11.3 *The installation and use of ISDN lines on premises owned, managed or occupied by the University, its wholly-owned subsidiary companies of their wholly-owned subsidiaries, will require the prior written consent of the Chief Information Officer.*

7.11.4 With the exception of any special provision agreed for the University's corporate administrative arrangements, the use of modems on equipment located on premises owned, managed or occupied by the University that are linked to the staff network is prohibited.

7.12 **Off-campus access and on-campus wireless network access to information systems on staff and student networks**

7.12.1 **Authenticated access to the student network**

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.

7.12.2 **Authorised access to the staff network**

Off-campus access and on-campus wireless network access via the VPN service to systems and services on the staff network is restricted to Members of the University in Membership B and designated 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).

8 **NEW OR CHANGED USES OF THE COMPUTER NETWORKS**

8.1 The Chief Information Officer (or nominee) must be advised in advance, and at the earliest opportunity, 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.

8.2 The Chief Information Officer (or nominee) will assess the likely impact of the proposed use and will advise on the consequential impact upon the performance of the University's computer network.

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

9 FAULT REPORTING

9.1 *'Urgent' network faults should be reported immediately to the Helpdesk.*

9.2 *'Non-urgent' network faults should be reported through the normal channels to the Helpdesk (email: helpdesk@herts.ac.uk).*

10 COMPUTER NETWORK MAINTENANCE AND REPAIR

10.1 Regular 'at risk' times

10.1.1 The University's JANET connection is subject to a regular national weekly 'at risk' time when maintenance work specified by JANET(UK) is undertaken. This is on Tuesdays from **07.00** - **09.00** hours.

10.1.2 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.

10.1.3 Network users are advised not to schedule important 'network dependent' activities during these regular 'at risk' times.

10.2 Other works

10.2.1 Where planned development, maintenance or repair work cannot be accommodated either within the weekly 'at risk' time or cannot be concluded before **08.30** hours on weekdays, the Chief Information Officer (or nominee) will, where possible, give at least two (**2**) working days' prior notice, by e-mail to the UHQ list and/or by StudyNet News, of the length of time and extent to which network services will be affected.

10.2.2 In the event of a sudden network failure (partial or complete) every effort will be made to restore services as quickly as possible and, subsequently, to give an explanation of the reasons for the failure.

10.3 Disaster recovery and 'back-up' arrangements

10.3.1 To minimise the risk to activities that are critical to the University's business, the University's computer networks will incorporate disaster prevention measures including, as appropriate, alternative routing and back-up arrangements for the main computer network backbones, inter-site connections, data centres and systems.

10.3.2 To ensure the continued operation of the network in the event of power and/or air-conditioning failures, where required, alternative power and air-conditioning supplies will be provided to the main communications rooms and Data Centres.

11 COMPUTER NETWORK PERFORMANCE AND SECURITY

11.1 *The University's computer networks will be configured, monitored and managed in accordance with the UK HM Government Cyber Security Essentials Scheme:*

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf

11.2 The Chief Information Officer (or nominee) will monitor and document computer network performance and usage and will provide the Office of the Vice-Chancellor (OVC) with reports on any performance *and security* issues and risks.

12 NETWORK DEVELOPMENT

12.1 Computer network provision in new and refurbished buildings

12.1.1 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.

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

12.1.3 Where the network requirements of a specialist area or activity need a network provision that exceeds the standard specification (section 12.1.1, refers), 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.

12.1.4 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, to the Office of the Vice-Chancellor (OVC) for additional funding to meet the costs of the enhanced network provision that is required.

12.2 Development Plan

A rolling three (**3**) year network development plan, advising the Office of the Vice-Chancellor (OVC) of appropriate developments aimed at ensuring the future adequacy of the University's computer networks, will be prepared by the Chief Information Officer. This plan will take account of the University's strategic plan; usage and demand patterns; technological change; security; management and cost implications.

12.3 Implementation of new developments

12.3.1 Prior to installation

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

12.3.2 At installation

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.

13 DISPUTES

In the event of a dispute relating to conflicting usage demands on the University's computer networks, the Chief Information Officer will arrange for an investigation of the issues concerned.

Mrs S C Grant
Secretary and Registrar
Signed: **1 September 2014**