INTERNET, ON-LINE COMMUNICATIONS AND SOCIAL MEDIA

SUMMARY OF PRINCIPAL CHANGES

General changes	
Information Hertfordshire re-named 'Library and Computing Services' from 1 January 2016	
Section	
6.4.2	Refer to text

*(Amendments to version **01.0**, UPR IM19, are shown in italics.)*

"1 **INTRODUCTION**

This document should be read in conjunction with *UPR EQ10*[1]; UPR SA12[2]; UPR IM08[3]; UPR IM01[4], Appendix I, UPR IM02[5], UPR IM03[6], UPR IM16[7], *Appendix I,* UPR IM19[8] and the 'JANET Acceptable Use Policy' (section 6.4, 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 '**Member of the University**':

an individual granted membership of the University under the provisions of UPR GV06[9];

3.2 **'information system'**:

any computer system which is used to manage or deliver information and/or services. This includes, but is not limited to, web servers (section 3.13, refers) and File Transfer Protocol (FTP) servers (section 3.15, refers);

3.3 '**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

---

1 *UPR EQ10 'Bullying and Harassment*'
2 UPR SA12 'Learning Resources'
3 UPR IM08 'Data Protection'
4 UPR IM01 'Computer Networks, Security of Information Systems and the Protection of Information Systems from Computer Viruses'
5 UPR IM02 'Information Management Policy'
6 UPR IM03 ' Information Security Policy'
7 UPR IM16 'Data Management Policy'
8 Appendix I, *UPR IM19* 'University Website – Terms of Use'
9 UPR GV06 'Member of the University'

3.4 '**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);

3.5 '**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;

3.6 '**StudyNet**':

the University's managed learning environment and student intranet (it should be noted that regulations set out in this document which apply to intranets also apply to StudyNet);

3.7 '**StaffNet**':

the University's staff intranet; (it should be noted that regulations set out in this document which apply to intranets also apply to StaffNet);

3.8 **'Social Media/Social Networking:**

any on-line tool, such as a website, which allows people to interact with each other in some way – by sharing information, opinions, knowledge and interests. Social networking websites such as Facebook or LinkedIn are perhaps the most well-known examples of social media but for the purposes of this policy, the term also means, but is not necessarily limited to, other web-based services such as blogs, video and audio podcasts, wikis, message boards, photo document and video sharing websites such as Tumblr or YouTube; micro blogging services such as Twitter; communication technologies such as mobile phones, cameras, PDAs, Tablets, Portable Handheld Consoles, Games Consoles or other hand-held devices and any other emerging forms of communications technologies;

3.9 **'virtual world'**:

a computer-based simulated environment intended for its users to inhabit and interact via avatars.

3.10 '**staff profile'**

a web page, or set of web pages, which describe a member of staff's academic and/or professional role and duties associated with the University for both public and internal use. This may be hosted on University web pages or on public services, such as LinkedIn or Academia.edu. It does not include personal profiles which do not relate to the individual's academic and/or professional role at the University.

3.11 **'web browser'**:

a computer program, for example, Microsoft Internet Explorer, Firefox, Safari, Chrome, which can be used to view information on the Internet or an intranet or engage with social media;

3.12 **'web page'**:

a single unit of information which can be viewed using a web browser;

3.13 **'web hyperlink'**:

a link displayed by a browser which enables access either to a new web page or to another part of the web page which is being viewed;

3.14 **'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;

3.15 '**personal web page'**:

a web page relating to an individual Member of the University, not published on a University web page;

3.16 **'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;

3.17 **'web server'**:

a computer hosting one or more web pages: a web server may be hosted within the University or as an agreed managed service with an external provider; a web server may serve web pages to the Internet and/or an intranet;

3.18 '**e-mail**':

a message sent electronically to an individual or to a specific group;

3.19 **'on-line communications'**:

any form of communication between individuals or groups of people sent electronically;

3.20 **'File Transfer Protocol server'**:

a computer allowing users to 'download' files of data or programs onto their computers. An FTP server may be part of the Internet or an intranet;

3.21 **'personal data'**:

information about living, identifiable individuals including statements of fact, expressions of opinion about them (section 7, refers) and photographic images;

3.22 **'JANET'**:

the collection of networking services and facilities which support the communication requirements of the UK education and research community;

3.23 **'RIPA**':

Regulation of Investigatory Powers Act 2000.

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 Policy (UPR IM02[5], refers).

4.3 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.

4.4 Potential and actual breaches of this policy may result internally in investigation under the relevant disciplinary policies and where these breach the law may result in criminal proceedings.

4.5 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 ROLES

(**NOTE:** The University's computer networks (as defined In UPR IM01[4]) are managed by the Chief Information Officer. The regulations in this section (5) relate to the publication of information on-line, using the facilities provided by those networks.)

5.1 *Pro Vice-Chancellor* (*Business and International Development)*

The *Pro Vice-Chancellor* (*Business and International Development)* 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).

Responsibility for content creation and updating will be delegated to Heads of Strategic Business Units and other authorised staff, as appropriate, in accordance with section 5.3 of this document.

5.2 **Chief Information Officer**

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.

5.3 **Heads of Strategic Business Units**

5.3.1 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* (*Business and International Development)* 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* (*Business and International Development)* (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* (*Business and International Development)* (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* (*Business and International Development)* 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.

5.4 Members of the University in Membership B[5]

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.

6 REGULATIONS

6.1 General regulations

6.1.1 The Internet, extranets, social media, virtual worlds, e-mail and intranets (including StudyNet and StaffNet) will be used strictly in accordance with University Policies and Regulations.

6.1.2 The information published via these media must be appropriate to the Vision, Mission and Values of the University; must be consistent with the Strategic Plan; must not be illegal (section 7, refers); must not be such that it may attract civil action or bring the University into disrepute and must not otherwise place the University in breach of the 'JANET Acceptable Use Policy' (section 6.6, refers). Members of the University publishing information must not provide web hyperlinks to material which may be inconsistent with, or contravene, these requirements.

6.1.3 Copyright

Where appropriate, material published via these media 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[10], refers).

6.1.4 Accessibility

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.

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

a new web content and services created by the University;
b web content and services provided by third party organisations
c existing web content and services as and when they are updated.

---

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

6.1.5 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 (section 7, refers). Once permission is withdrawn, the personal data and/or photographic images must be removed immediately.

Members of the University must keep personal information safe and secure at all times. They 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.

6.1.6 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 II, UPR IM19[11], refers).

6.1.7 Hosting external web sites

The University's web servers may be used to host web pages and other services on behalf of external organisations only 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.

6.2 Access to the Internet/intranets/extranets/on-line communications services and acceptable use

6.2.1 Subject to their having obtained the prior written consent of University management (section 6.2.2, refers):

i access to the Internet via University provision, such as University networks and computers, is restricted to Members of the University and other Authorised Users, as agreed from time-to-time by the University;

ii access to intranet and extranet sites and University on-line communications services is limited to Members of the University who have been given permission to do so and other Authorised Users, as agreed from time-to-time by the University, who have been issued with individual accounts for this purpose.

In either case (6.2.1, i or ii), permission is given by virtue of the nature of the individual's Membership of the University.

6.2.2 In issuing individual accounts, the University authorises access to the Internet or intranets or on-line communications services by the individual to whom the account is issued. Such access is granted for the sole use of the individual to whom the account has been issued. This process constitutes the prior written consent referred to in section 6.2.1. This consent is given on condition that the user complies, at all times, with the requirements of UPR IM01[4], UPR IM02[5] and UPR IM03[6], and UPR IM16[7].

[11] Appendix II, UPR IM19 'Domain Registration and URL (web addressing) Definition and Management'

6.2.3 Acceptable use of JANET

All users are responsible for ensuring that their use of the Internet, extranets and intranets complies with the nationally agreed 'JANET Acceptable Use Policy', which applies to any organisation authorised to use JANET. The policy is binding on the University and its Members. The policy is available on-line at:

https://community.ja.net/library/acceptable-use-policy

The connection of any organisation to JANET is governed by the JANET Connection Policy

Where JANET is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of JANET.

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

6.3.1 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.

6.3.2 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* (*Business and International Development)*.

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.

6.3.3 University website terms and conditions

The University website terms and conditions and privacy policy apply to every University web page (Appendix I, UPR IM19[12], refers), and must have a hyperlink from all University websites and FTP servers.

6.3.4 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;

6.3.5 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..

---

[12] Appendix I, UPR IM19 'University Website – Terms of Use'

6.3.6 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 (UPR IM19).

6.3.7 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.

6.3.8 **StudyNet (and other intranets and social media which host un-mediated content)**

i 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.

ii 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.

iii 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.

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

6.4.1 No personal pages shall incorporate the University's logo without the express written permission of the *Pro Vice-Chancellor* (*Business and International Development)*. 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.

6.4.2 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 *or express extremist views that risk drawing individuals into terrorism* 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.

6.4.3 For the purposes of employment rights, a breach of these obligations may be construed by the University as misconduct.

6.5 E-mail and other on-line communications

6.5.1 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.

6.5.2 University management communicates with Members of the University by e-mail through their individual e-mail accounts as recorded on the staff email service or as recorded on a student or other official University contact record. 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.

6.5.3 The University will send e-mail communications 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 of their choice.

6.5.4 Users are responsible for the management of their personal e-mail files, including the deletion of out-dated and redundant e-mails and the efficient use of on-line storage facilities. Use of the University's e-mail service must at all times be in accordance with the requirements of the JANET acceptable use policy (section 6.2.3, refers).

6.5.5 E-mail messages containing a virus which are trapped on delivery by the University's central system will be discarded.

6.5.6 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 Members of the University reasonably believes it to be free from all viruses, spyware, malware or other harmful or disruptive components.

6.5.7 Members of the University will comply with any amendments to the requirements in this section which may be determined from time-to-time by the Chief Information Officer.

7 LEGISLATION

7.1 Members of the University must have particular regard for and must not breach the following:

i Copyright, Designs and Patents Act 1988

Particular care must be taken not to commit any act that could breach the rights of the owner of any copyright work. Preliminary advice on copyright issues should be sought from *Library and Computing Services.*.

ii Data Protection Act 1998 and Freedom of Information Act 2000

Members of the University who hold data relating to a living person must comply with the requirements of the Data Protection Act 1998[3].

Any storage of personal data (including names and e-mail addresses) must be carried out in accordance with the Act. Advice may be sought from the University's Director of Legal Services and University Solicitor (e-mail: k.kwan2@herts.ac.uk; Telephone: 01707 284904) concerning data protection issues[3].
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.

Freedom of Information requests should be directed to the University's Director of Legal Services and University Solicitor (e-mail: k.kwan2@herts.ac.uk; Telephone: 01707 284904).

iii **Computer Misuse Act 1990**

Persons using information systems must not infringe this Act.

Under the provisions of this Act the following acts (amongst others) may constitute criminal offences:

a gaining unauthorised access to computer programs or data;
b gaining unauthorised access with intent to commit or facilitate commission of further offences;
c making unauthorised modifications to the contents of a computer with the intention of impairing the operation of the computer or relevant program or data.

iv **Obscene Publications Acts 1959 and 1964, the Protection of Children Act 1978 and the Communications Act 2003**

Persons using information systems must not infringe these Acts.

Members of the University must take particular care not to transmit obscene or indecent material by any method, whether via the Internet, an intranet, extranet, e-mail or by any other means. In this regard, Members of the University must not commit any act whilst using the Internet, an intranet, extranet, e-mail or by any other means, whether an offence under the above Acts or not, which might reasonably be expected to cause offence to any third party.

v **Equality Act 2010**

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 must not be created, stored or distributed. Advice on Equal opportunities issues should be sought from the Head of the Equality Unit.

Members of the University must not commit any act that could be interpreted as unlawful discrimination within the meaning and scope of any law, order, enactment or regulation relating to equality or discrimination.

vi **Terrorism Act 2000 and 2006, Counter-Terrorism Act 2008, Terrorism Prevention and Investigations Measures Act 2011, *Counter Terrorism and Security Act 2015***

Persons using information systems must not infringe these Acts.

The University is required by the Counter Terrorism and Security Act 2015, to have due regard to the need to prevent individuals from being drawn into terrorism (the 'Prevent Duty'). This Prevent Duty must be implemented by the University in a proportionate and risk based manner. The University fulfils its legal obligations by adhering to the guidance contained in the Revised Prevent Duty Guidance for England and Wales and the Prevent Duty Guidance for Higher Education institutions in England and Wales, as amended from time-to-time.

While fulfilling the Prevent Duty, the University will also have particular regard, and remains committed, to academic freedom and freedom of speech. The University expects that its staff and students will comply with the University's policies and procedures and will co-operate with the University as it carries out its institutional obligation to protect the welfare of its community members.

Members of the University must not:

access, create, download, store or transmit unlawful material *(including material that is or might be prohibited by the Counter Terrorism and Security Act 2015);*

access, create, download, store or transmit material that is indecent, offensive, defamatory, threatening, discriminatory or extremist.

The University reserves the right to block or monitor access to such material. Members of the University must not 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.

Advice on *compliance with the legislation cited in this section (7.1)* should be sought from the *Director of Legal Services and University Solicitor*.

7.2 **Material which is defamatory or offensive**

Advice on defamation should be sought from the University's Director of Legal Services and University Solicitor (e-mail: k.kwan2@herts.ac.uk; Telephone: 01707 284904).

Members of the University must not commit any act using the University's information systems which is defamatory or might reasonably be expected to cause offence to a third party.

7.3 **RIPA**, **Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the Human Rights Act 1998 and Data Protection Act 1998**

RIPA and the Regulations permit the University to intercept communications in certain circumstances to monitor[4] 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.

7.4 **Contempt of Court**

It is implicit that users will 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.

8 SANCTIONS AND PENALTIES

8.1 It should be noted that intentional or reckless misuse of the University's information systems, including abuse of a computer workstation or other computer terminal system, is regarded as misconduct and could also give rise to criminal and civil penalties.

8.2 **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[13] and/or the *English* courts.

8.3 **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[14] and/or the *English* courts."

Mrs S C Grant
Secretary and Registrar
Signed: **1 January 2016**

[13] UPR HR02 'Staff Disciplinary Policy'
[14] UPR SA13 'Student Discipline'