

ICT ACCEPTABLE USE POLICY AND PROCEDURES

1	Introduction.....	2
2	Policy Statement.....	3
3	Purpose.....	4
4	Audience	5
5	Ownership.....	6
6	Responsibilities	7
7	Acceptable Use.....	8
8	Unacceptable Use	9
9	Password Policy.....	11
10	Email policy.....	14
11	Email Retention and Recovery Policy	17
12	Google Collaborative Applications.....	20
13	Connecting computing equipment to the network.....	21
14	Mobile Devices (including Blackberry and Mobile Phone Policy)	22
15	Backup Services	24
16	Deletion of Data	28
17	Disposal of Old Equipment.....	29
18	Software and Hardware auditing.....	32
19	Removal of Equipment.....	33
20	Loss and Damage.....	34
21	Access by external entities affiliated to the University	35
22	Investigation and response to ICT violations	36
23	Taking down materials which may incite violence.	39
24	Reporting Security Incidents	40
	Appendix 1: Guidelines and policies References.....	41
	Appendix 2: External Acts	42

1 Introduction

- 1.1 The University of Westminster (referred to hereafter as “the University”) encourages the use of electronic communications to share information and knowledge in support of the University's mission and to conduct the University's business. To this end, the University supports and provides interactive electronic communications services and facilities such as telephones, voicemail, teleconferencing, video teleconferencing; electronic mail, bulletin boards, social networking; electronic publishing services such as the Internet; and electronic broadcasting services such as online radio and podcasting.
- 1.2 These communications services rely on underlying voice, video, and data networks delivered over both physical and wireless infrastructures. Digital technologies are unifying these communications functions and services, blurring traditional boundaries. The Policy recognises this convergence and establishes an overall policy framework for electronic communications.
- 1.3 This Policy clarifies the applicability of law and of other University policies to electronic communications. It also establishes new policy and procedures where existing policies do not specifically address issues particular to the use of electronic communications. Where there are no such particular issues, this Policy defers to other University policies.
- 1.4 An integrated policy cannot anticipate all the new issues that might arise in electronic communications. One purpose of this Policy is to provide a framework within which these new issues can be resolved and that recognises the intertwining legal, institutional, and individual interests involved.

2 Policy Statement

- 2.1 Information and Communication Technology (ICT) is provided to support the teaching, learning, research and administrative activities of the University. The data held on the network forms part of its critical assets and are subject to security breaches that may compromise confidential information and expose the University to losses and other legal risks.
- 2.2 These University guidelines and policies change from time to time; therefore users are encouraged to refer to on-line versions of this and other University policies on the University web site.
- 2.3 Any infringement of these regulations may be subject to penalties under civil or criminal law, and such law may be invoked by the University. Any infringement of these regulations constitutes a disciplinary offence under the University's procedures and may be treated as such regardless of legal proceedings. Abuse of the regulations may result in the user's account(s) being suspended.
- 2.4 These regulations are periodically reviewed by the Information Strategy Committee.
- 2.5 If you have any query on these regulations, contact the Fix-IT centre:
Telephone: +44 (0)20 7915 5488, or 5488 from any University building.
Email: Fix-IT@wmin.ac.uk
Website: ResolveIT - <http://www.wmin.ac.uk/page-10304>

3 Purpose

3.1 This policy has been established to:

- 3.1.1 Provide guidelines for the conditions of acceptance and the appropriate use of the computing and networking resources provided for use by academic, professional and support staff and students of the University in support of the mission of the University.
- 3.1.2 Provide mechanisms for responding to external complaints about actual or perceived abuses originating from the University network and computer systems.
- 3.1.3 To provide the mechanism for responding to internal complaints about actual or perceived abuses against University systems from the internet.
- 3.1.4 Protect the privacy and integrity of data stored on the University network.
- 3.1.5 Mitigate the risks and losses from security threats to computer and network resources such as virus attacks and compromises of network systems.
- 3.1.6 Reduce interruptions and ensure a high availability of an efficient network essential for sustaining the business of the University.
- 3.1.7 Encourage users to understand their own responsibility for protecting the University network.
- 3.1.8 To ensure compliance without limitation to Statutes and Regulatory frameworks.

4 Audience

4.1 These regulations apply to:

- 4.1.1 Users (academic, professional and support staff, students and others with extended access privileges) using either personal or University provided equipment connected locally or remotely to the network of the University. Throughout this policy, the word 'user' will be used collectively to refer to all such individuals or groups.
- 4.1.2 All ICT equipment connected (locally or remotely) to University servers.
- 4.1.3 ICT systems owned by and/or administered by the Information Systems and Library Services (ISLS) department of the University.
- 4.1.4 All devices connected to the University network irrespective of ownership.
- 4.1.5 Connections made to external networks through the University network.
- 4.1.6 All external entities that have an executed contractual agreement with the University.

4.2 ICT staff includes staff in ISLS, and the technical support staff in the School of Electronics and Computer Science.

5 Ownership

- 5.1 The electronic resources of the University are to be used for academic, research, consultancy or other business purposes in serving the interests of the University and its students, staff and clients and in the course of normal operations.
- 5.2 Any ICT or electronic communications address, site, number, account, or other identifier associated with the University or any unit of the University, or assigned by the University to individuals, units, or functions of the University, is the property of the University.
- 5.3 Electronic communications records pertaining to the business of the University are considered University records whether or not the University owns the electronic communications facilities, systems or services used to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, print or otherwise record them.

6 Responsibilities

- 6.1 The holder of a University computer account or computer system connected to the University is responsible for the actions associated with the computer account or computer system.
- 6.2 Users must ensure that they use all reasonable means to protect their equipment and (if applicable) their account details and passwords.
- 6.3 Engaging in any prohibited activities referred to in Section 8 of the University ICT Acceptable Use Policy and Procedures and may result in disciplinary action being taken. .
- 6.4 Users are expected to assist ICT support staff with investigations into suspected violations or breaches of security (includes staff in ISLS and the technical support staff in the School of Electronics and Computer Science).
- 6.5 Users are required to provide assistance to the University's Data Protection Officer / Freedom of Information Officer in response to requests made under the Data Protection Act 1998 and the Freedom of Information Act 2000 in accordance with UK law.

7 Acceptable Use

7.1 The University provides electronic communication systems and services to departments and Schools in support of its academic mission. ISLS encourages their use and makes them widely available to the University community. Nonetheless, the use of these facilities constitutes acceptance of this policy and is subject to the following limitations, necessary for the reliable operation of the electronic communication systems and services.

7.2 Users must comply with all applicable laws.

7.3 The electronic resources should be used for the purpose for which they are intended.

7.4 Users must respect the rights, privacy and property of others.

7.5 Users must adhere to the confidentiality rules governing the use of passwords and accounts, details of which must not be shared.

7.6 Passwords must not be disclosed to anyone even if the recipient is a member of ISLS. Temporary passwords provided by ISLS staff to users must be changed immediately following a successful login.

7.7 The University network may only be used for work which complies with the ICT regulations and JANET's Acceptable Use Policy (<http://www.ja.net/services/publications/policy/aup.html>).

7.8 Whilst the University network is being used to access other networks, any abuses against such networks will be regarded as an unacceptable use of the University network.

7.9 Personal Use

7.9.1 The University network and computing resources may be used for incidental personal purposes provided that:

7.9.1.1 the purposes are of a private nature, not for financial gain and does not contravene any other staff policies;

7.9.1.2 such use does not cause noticeable or unavoidable cost to the University;

7.9.1.3 such use does not inappropriately interfere with the official business of the University;

7.9.1.4 such use does not include any actions defined in Section 8 of the University ICT Acceptable Use Policy and Procedures;

8 Unacceptable Use

- 8.1 The University ICT facilities must not be provided to individual consumers or organisations outside the University except where such services support the mission of the University or are in the commercial interest of the University and permission has been granted by ISLS.
- 8.2 The University adopts a policy of cooperation with copyright holders and law enforcement bodies, and may suspend or remove content published online while investigating claims from such bodies.
- 8.3 The University will from time to time act to suspend or remove content from websites which jeopardize the University's reputation or brand. In the case of content published on University websites, this should be conducted under the relevant policy which can be found at <http://www.westminster.ac.uk/page-15125>
- 8.4 Any misuse of the University network resources may be seen as a breach of the University Disciplinary Code and lead to disciplinary action.
- 8.5 The University network may not be used for the following activities:
- 8.5.1 The creation, dissemination, storage and display of obscene or pornographic material.
 - 8.5.2 The creation, dissemination, storage and display of indecent images of children.
 - 8.5.3 The creation, dissemination, storage and display of hate literature.
 - 8.5.4 The creation, dissemination, storage and display of materials that promote terrorism.
 - 8.5.5 The creation, dissemination, storage and display of defamatory materials or materials likely to cause offence to others.
 - 8.5.6 The creation, dissemination, storage and display of any data that is illegal including, but not limited to, that referred to in Appendix 2.
 - 8.5.7 The downloading, storage and disseminating of copyrighted materials including software and all forms of electronic data without the permission of the holder of the copyright or under the terms of the licenses held by the University.
 - 8.5.8 Any activities which do not conform to applicable laws and other University guidelines and policies regarding the protection of intellectual property and data. Specific emphasis is placed on the downloading and copying of both music and video files through the internet using peer-to-peer file sharing utilities such as but not limited to Limewire, Morpheus, and Gnutella, or Bit torrent etc. In accordance with the laws relating to Intellectual Property Rights, the downloading and copying of files such as but not limited

to MP3, AVI, DIVX and other audiovisual software without the permission of the owner of the copyright is an illegal practice.

- 8.5.9 The deliberate interference with or gaining illegal access to user accounts and data including viewing, modifying, destroying or corrupting the data belonging to other users.
- 8.5.10 Using the network or centrally managed services for commercial work for outside bodies without explicit permission from the Director of ISLS.
- 8.5.11 Use of a username and password belonging to another user.
- 8.5.12 Attempts to falsify your identity or to pretend to have a different affiliation with the University when sending email from a University computer.
- 8.5.13 Attempts to crack capture passwords or decode encrypted data.
- 8.5.14 Any other use that may bring the name of the University into disrepute or expose the University to the risk of litigation.
- 8.5.15 Intentional or reckless creation, execution, forwarding or introduction of any viruses, worms, Trojans or software code designed to damage, self replicate or hinder the performance of the University network.
- 8.5.16 Deliberate actions that might reduce the effectiveness of any antivirus or other ICT security management precautions installed by authorised University staff.
- 8.5.17 Attempts to penetrate security measures (hacking) whether or not this results in a corruption or loss of data.
- 8.5.18 Purposefully scanning internal or external machines in an attempt to discover or exploit known computer software or network vulnerabilities.
- 8.5.19 Engaging in commercial activities that are not under the auspices of the University.
- 8.5.20 Using computing resources (CPU, time, disk space, and bandwidth) in such a way that it causes excessive strain on the computer systems or disrupts, denies or creates problems for other users.
- 8.5.21 Connecting any computer device to the University network unless it meets the desktop security standards established by ISLS on behalf of the University.

9 Password Policy

9.1 Introduction

- 9.1.1 Information stored on the computer desktop, laptop and the LAN (local area network) forms a part of the university's valuable assets. The University operates a single sign-on environment whereby a user can gain access to all network resources with the use of a single username and password underpinned by a robust password policy.
- 9.1.2 Passwords are the primary authentication method for the University's IT resources and are currently the basic authentication method employed. Passwords ensure that only authorised individuals have access to specific computer systems and establish accountability for all changes made to system resources. Strong passwords promote a secure computing environment; badly chosen passwords endanger the information that they are supposed to protect.
- 9.1.3 To counter the forces of social engineering (this happens when an attacker tricks users into divulging their passwords) and online identity theft (where a user's credentials are stolen and used to access university servers without the user's knowledge), users must be diligent in guarding against access to University resources from internal and external threats by adopting strong passwords and by not sharing passwords.
- 9.1.4 Users must guard against responding to emails asking them to provide their username and password for system maintenance, even if the email appears to originate from ISLS. These emails are fictitious and are an attempt to steal a user's identity for nefarious purposes.

9.2 Policy

- 9.2.1 Passwords must be kept confidential and not shared with colleagues. This does not apply to generic departmental passwords, where a group manages the password and in such cases, the password must not be shared outside the group.
- 9.2.2 Your username or variations of the username should not be embedded in your password.
- 9.2.3 Passwords must not be blank.
- 9.2.4 Computer generated passwords must be changed following the initial successful login.
- 9.2.5 Passwords must not be based on personal information (e.g. names of families, pets, name of your street, car registration numbers, telephone numbers)
- 9.2.6 Passwords must not be revealed to your line manager.
- 9.2.7 Passwords must not be revealed to anyone over the phone even if the recipient is a member of ISLS staff.
- 9.2.8 Passwords used within the University must not be used for external Internet accounts or online service providers.
- 9.2.9 Passwords must not include words from a dictionary in any language.
- 9.2.10 Passwords must be unique from previous passwords. The previous passwords should not be re-used.

- 9.2.11 New passwords must not bear any resemblance to the old. For instance, if the old password is April, the new password must not be April1 or 1lirpa or any variation of April.
- 9.2.12 Once the passwords have been changed, the new password must be kept for 8 days before the user can be allowed to change it again.

9.3 Best Practices

- 9.3.1 Passwords should not be included in any automated login process especially on shared computers.
- 9.3.2 Passwords should not be written down, emailed or spoken after a password reset.
- 9.3.3 Passwords should not be typed or saved in electronic documents.

9.4 Setting your Password

- 9.4.1 Passwords for desktop/client operating systems should meet the following criteria:
 - Passwords must be at least six characters long.
 - Passwords should be composed of alphanumeric characters (alphabets – A...Z, numbers – base 10 digits – 0...9).
 - Passwords should include non-alphanumeric or special characters (e.g.; £; \$;);
 - Passwords should be strong e.g.
(choose one or two lines from a poem or song and use the first letter of each word. For example 'Always look on the bright side of life becomes **alotbsol**)

9.5 Changing your password

- 9.5.1 Passwords must be changed under any one of the following circumstances:
 - At least every three months
 - Immediately, if a password has been compromised or after you suspect that a password has been compromised.
 - Passwords must be changed on instruction from the ISLS Fix-IT centre.

Note: You should not change your password last thing on Friday or just before you go on holiday as you may forget it when you next use it.

9.6 System based passwords - requirements for system administrators

- 9.6.1 Privileged and administrative passwords must be subject to stringent composition and frequency of change. Privilege passwords include passwords for routers, switches, hubs, firewalls, network operating systems and any other IT system/resource.
- 9.6.2 All passwords must be documented in the password book and kept in the safe at all times. Only authorised personnel must access the safe.
- 9.6.3 Passwords must be unique for every server system.
- 9.6.4 A number of shared local administrative passwords may be used on machines for specific departments and computer labs.
- 9.6.5 Passwords must be at least eight characters long but preferably longer.
- 9.6.6 The root/super user password must never be used unencrypted across the network to avoid eavesdropping. Wherever possible you must su to root using SSH or similar technology or use sudo.
- 9.6.7 Passwords must be retired after three months.

- 9.6.8 Once the passwords have been changed, the new password must be kept for 8 days before the user can be allowed to change it again.
 - 9.6.9 Service accounts must not rely on admin accounts/passwords.
 - 9.6.10 Accounts created for external contractors should be given restrictive rights to carry out their functions and the accounts should be disabled immediately following the completion of the appointed task.
 - 9.6.11 Administrator/privilege passwords must not be disclosed to external contractors.
 - 9.6.12 Default passwords that come with computer systems or services must be changed during installation or the system should be set up to remind the administrator to change the password at the next login
 - 9.6.13 Passwords must be unique from all previous passwords. The last ten passwords must not be re-used.
 - 9.6.14 Critical systems must implement account lockout policies and be set up to disconnect idle sessions after a period of inactivity of thirty minutes.
 - 9.6.15 Systems must be configured to enforce password changes.
 - 9.6.16 The SNMP community strings must be changed from the standards defaults and should be different from the password used to interactively log in.
 - 9.6.17 Privileged passwords should not be communicated via telephone fax or email.
- 9.7 Password changes
- 9.7.1 All passwords must be changed via the web interface at <https://password.westminster.ac.uk> or the Fix-IT centre.

10 Email policy

- 10.1 The University provides electronic mail services (“email”) to support the teaching, learning, research and administrative mission of the University and which is maintained by ISLS for use by staff, students, faculty, alumni and associates affiliated with the University.
- 10.2 Email is a critical means of communication at the University and many official University communications are transmitted between staff and students.
- 10.3 This policy applies to users (academic, professional support staff, faculty, students and others extended access privileges) and has been established to provide guidelines for the acceptable use of the email service.
- 10.4 Staff email: All official University email communication to University staff will be delivered to their University account and should not be automatically forwarded to external email accounts.
- 10.5 The University of Westminster, in collaboration with Google, has introduced Google Apps for Education, a service that allows institutions and individuals to use Google's communication and collaboration applications under their own domain names. These services are hosted by Google offsite and provide a convenient solution to store or share information which is accessible from any computer device connected anywhere to the Internet (see Section 11 below). Any use of Google Mail by staff is governed by this University email policy.
- 10.6 Staff have also been given Google accounts by default which allows them to use Google Mail as well all the applications in the Google environment.
- 10.7 Email is not a secure method of communication and staff should not send or forward confidential, personal or sensitive business information to non University of Westminster email accounts or through the University Google email service.
- 10.8 Staff are strongly advised not to use Google mail for University business as the user's identity cannot be verified
- 10.9 ISLS do not backup any emails stored in the Google environment so users are individually responsible for keeping backups of any stored in the Google environment.
- 10.10 All email communication from staff should display the following disclaimer.

“This e-mail and its attachments are intended for the above named only and may be confidential. If they have come to you in error you must not copy or show them to anyone, nor should you take any action based on them, other than to notify the error by replying to the sender.”

- 10.11 Confidentiality: Communication between staff is considered a business record and some emails may have attachments that may contain confidential and personal information. The University has a duty of care to prevent the leakage of confidential data from its systems. In addition to that, restrictions may also be applied to certain research projects that may forbid the storage of research data on non-University owned systems. Any such data that is deemed confidential should not be shared in the Google environment and should only be shared on University owned systems and with authorised staff.
- 10.12 Student email: Undergraduate and Postgraduate students, who enrolled in or after September 2008 have been given Google accounts by default which allows them to use all the applications in the Google environment. Students enrolled prior to that date can switch to the Google service by contacting the Fix-IT centre. Students who have not switched to the Google email service may redirect email from their official University account to an external ISP. This is done at the student's risk and does not absolve the student of any responsibility for the official email account and neither is the University responsible for the email servers of the external ISP. Any use of Google Mail is governed by this University email policy
- 10.13 Email between computers connected to the University network and the Internet must be relayed via the University email gateway, either directly or through a local departmental mail server.
- 10.14 The University mail server will not accept mail to external addresses sent from an address, which is itself external to the University.
- 10.15 The University mail server will not accept mail sent from a computer, which has not been properly registered with an authorised network address.
- 10.16 Users of the University ICT facilities shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the University or any unit of the University unless appropriately authorised (explicitly or implicitly) to do so. While it is permissible to indicate one's affiliation with the University, unless it is clear from the context that the author is not representing the University, an explicit disclaimer must be included. An appropriate disclaimer may take the form: "These statements are my own, not those of the University of Westminster."
- 10.17 Users of University ICT facilities must not send email on behalf of another person, or impersonate another user when sending email, except when authorised by that person to do so.
- 10.18 Users of University ICT facilities may only send mass communications in support of the University's business and in accordance with policies on sending bulk messages and guidance from the Marketing, Development and Communications Department.
- 10.19 In general, the University cannot and does not wish to be the arbiter of the contents of electronic communications. Neither can the University, in general, protect users from receiving electronic communications they might find offensive.

10.20 Users of the University ICT facilities are strongly encouraged to use the same personal and professional courtesies and considerations in emails as they would in other forms of communication.

10.21 The email service must not be used to send emails that are intimidating or harassing. Disciplinary action will be taken against any user who sends threatening, intimidating or threatening emails.

10.22 The email service must not be used to inappropriately distribute works protected by Intellectual Property Rights belonging to others.

11 Email Retention and Recovery Policy

11.1 Introduction

- 11.1.1 Users are advised to familiarise themselves with these guidelines to inform their own decision on what information sent or received by email should be retained and for how long, to ensure that important institutional data is being preserved and maintained.
- 11.1.2 The information covered in these guidelines refers to email that is sent through the University Exchange server and does not apply to emails sent through the University of Westminster Google Mail or Google Talk services.
- 11.1.3 All messages sent via the University's email system belong to the University of Westminster and form part of the University's record and are therefore subject to public inspection under the Freedom of Information Act 2000.
- 11.1.4 Following a legitimate request made under UK law (Freedom of Information Act 2000, Data Protection Act 1998, Regulation of Investigative Powers 2001 etc), ISLS may investigate and support the recovery of specific emails in relation to any lawful request with the approval and authorisation of the Registrar and Secretary of the University.

11.2 Email Retention

- 11.2.1 This email retention policy is secondary to the University Freedom of Information Policy and to specific departmental procedures or regulations with regard to record keeping. Any email correspondence containing business information should therefore be retained for as long it is considered relevant under UK law.
- 11.2.2 The primary intent of email backup is for the full recovery of the email system and not for the storage and restoration of old emails. ISLS backup the email system solely for the purpose of restoring the service when it suffers a catastrophic system failure and the whole system has to be restored.
- 11.2.3 ISLS set the parameters for users' storage space and are investigating an email archiving solution that would enable users to archive their own emails. In the meantime, users should keep their core emails within the limit of their system quota.
- 11.2.4 Email correspondence containing business information should only be retained for as long it is necessary for business purposes, in line with any agreed departmental records retention policies and procedures, or as required by UK law.

11.3 Email Recovery

- 11.3.1 Users should be aware that ISLS do not recover individual deleted emails on request; however ISLS may recover individual emails following a RIPA request from the Police or in cases pending legislation. Requests for the recovery of such emails should be approved and authorised by the University Registrar and Secretary.
- 11.3.2 ISLS do backup complete email systems but do not back up individual emails. Snapshots of the email servers are done in an uncoordinated and unplanned way. ISLS may have copies of specific systems, which may be interrogated in exceptional cases and this process is unreliable and expensive and ISLS gives no guarantee that such information is recoverable.
- 11.3.3 In general, when an email is deleted, this is stored within the deleted folder and is automatically deleted after thirty days. This safeguard allows users to retrieve messages, up to thirty days, before they disappear from the system. Any emails deleted after a period of thirty days are not recoverable.

12 Google Collaborative Applications

12.1 Introduction

12.1.1 The University of Westminster, in collaboration with Google, has introduced Google Apps for Education, a service that allows institutions and individuals to use Google's communication and collaboration applications under their own domain names. These services are hosted by Google offsite and provide a convenient solution to store or share information which is accessible from any computer device connected anywhere to the Internet.

12.1.2 The Google Apps package includes the following services and is available for students. Staff have also been given Google accounts by default which allows them to use all the applications in the Google environment:

- **Gmail** – student email including instant messaging; any use of Google Mail, whether by staff or students, is governed by the University Email Policy, Section 10 above.
- **Google Calendar** - an online calendar;
- **Google Talk** - allows users make PC-to-PC free voice calls and send instant messages;
- **Google Docs & Spreadsheets** – allows users to create exchange and collaborate on documents and spreadsheets with different users within the University.

12.2 Purpose

12.2.1 This policy is to establish the appropriate use of Google Apps to protect the University of Westminster business records and to limit the exposure of the University to data and IPR risks by specifying the appropriate conditions under which the Google service may be used. Use of Google Mail, whether by staff or students, is governed by the University Email Policy, Section 10 above.

12.3 Policy

12.3.1 Google provides the Google Apps service on behalf of the University and users are expected to adhere to the University of Westminster ICT Acceptable Use Policy and Procedures such that the same standards of behaviour and adherence are expected in the use of the Google Apps as in the use of all University systems.

12.3.1.1 Ownership/Intellectual Property Rights (IPR): Users must only collaborate on documents to which they own the intellectual property rights or where they have the expressed permission for the contemplated use from the intellectual property owner.

12.3.1.2 Confidentiality: Communication between staff is considered a business record and some emails may have attachments that may contain confidential and personal information. The University has a duty of care to prevent the leakage of confidential data from its systems. In addition to that, restrictions may also be applied to certain research projects that may forbid the storage of research data on non-University owned systems. Any such data that is deemed confidential should not be shared in the Google environment and should only be shared on University owned systems and with authorised staff.

12.3.1.3 The University requires that all calendaring, teaching, research, legal and employment information should be mastered and available on University owned systems, in addition, Google Apps can be used at the discretion of the individual for collaboration and working on drafts.

12.3.1.4 Every current document on Google Apps must have a named owner and if there are joint collaborators on a document it is the responsibility of the departing owner to transfer the ownership of the document.

12.3.1.5 ISLS do not backup any documents or emails stored in the Google environment so users are individually responsible for keeping backups of any documents stored in the Google environment.

12.3.1.6 Personal and sensitive information: In accordance with the Data Protection Act 1998, the following information must not be placed in the Google environment when collaborating or working on draft documents, even when collaborating or working with other University staff:

- Personal information
- Date of birth
- Financial information
- Examination record
- Payment & bank details
- Username & passwords
- Medical records
- Alumni Information
- Any other information that the staff member knows or is expected to know that it is confidential.

13 Connecting computing equipment to the network

- 13.1 In classrooms and public access areas, a network access point already allocated to a configured computer must not be used by another desktop or personal computer.
- 13.2 Computers, workstations and laptops, PDA and smart phones or other removable storage devices such as USB drives or memory sticks may be connected to the University network subject to the regulations of acceptable use and following approval by ISLS.
- 13.3 Users who wish to directly connect personal computers to the network are only allowed to connect via designated official physical network ports or wireless access points.
- 13.4 Users who wish to connect their personal equipment to the network points or wireless network shall have no expectations of hardware or software support from ISLS.
- 13.5 Personal laptops connected to the network should adhere to the following guidelines
 - 13.5.1 Their operating system and any installed software should be fully patched and kept up to date.
 - 13.5.2 Up-to-date antivirus and anti spyware protection should be installed to provide protection from viruses, worms, Trojan horses, disruptive programs or devices or anything else designed to interfere with, interrupt or disrupt the normal operating procedures of the University network.
 - 13.5.3 A personal firewall should be installed to provide protection from unauthorised intrusions
 - 13.5.4 The laptop may not have a blank password and all default passwords should be changed.

14 Mobile Devices (including Blackberry and Mobile Phone Policy)

14.1 Introduction

- 14.1.1 Mobile devices (such as Personal Digital Assistant (PDA) or cellular phones including Blackberries) can be defined as portable hand-held devices that provide computing and information storage/retrieval capabilities for personal or business use.
- 14.1.2 Developments in technology and the business demands placed on users have led to the introduction of many portable devices to be used to access University resources such as emails and calendars.
- 14.1.3 The use of mobile devices for business purposes introduces IT security implications including:
- Loss or theft of the mobile device
 - Loss of business information on the mobile device
 - Unauthorised network access.
 - Data integrity
 - Interception of information during the synchronisation process if using wireless networks
 - Introduction of malware to the University network.
- 14.1.4 Users therefore have a duty of care whilst using such devices to ensure that they are used for their intended purpose, without creating business risks, by understanding the way the mobile devices should be used.

14.2 Policy

- 14.2.1 All University supplied Blackberry or mobile phones are the property of the University and so it has the right to audit and monitor the device, similar to any other electronic device.
- 14.2.2 Users must take reasonable care to protect the device from loss or theft.
- 14.2.3 Users must immediately inform Estates and Facilities (Communications) via the switchboard when the device is stolen or lost to prevent unauthorised access to confidential data.
- 14.2.4 In the event that a Blackberry is lost or stolen, Orange will block the SIM card whilst ISLS will also erase and disable the device to render it useless.
- 14.2.5 Only Blackberries owned by the University will be permitted to connect to its Blackberry Enterprise Server.
- 14.2.6 Personal non-University owned Blackberries are not licensed for use with the University Blackberry Server and as such are not supported by ISLS.

- 14.2.7 Estates and Facilities (Communications) must configure all Blackberry devices before they are given to the user.
 - 14.2.8 The four digit PIN number configured by Estates and Facilities (Communications) must not be removed.
 - 14.2.9 The Blackberry should be locked while not in use.
 - 14.2.10 Power-on passwords must be used on all mobile devices.
 - 14.2.11 Only data stored in Outlook on the Blackberry will be backed up by ISLS. Users are advised to install the Blackberry Desktop Manager application to synchronise the Blackberry with their computer in order to protect all data from damage or loss.
 - 14.2.12 The installation of unauthorised third party software will not be supported by ISLS and will be uninstalled if it causes a problem with any authorised software installed by ISLS.
 - 14.2.13 Network and system passwords must not be stored on mobile devices.
 - 14.2.14 Users must take appropriate measures to protect against the accidental loss, damage or theft of University information held on mobile devices, especially if that information relates to personal information. Sensitive personal information, as defined by the Data Protection Act 1998, should not be stored on a mobile device (racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sexual life and criminal convictions).
 - 14.2.15 Users must report any fault with the device to Estates and Facilities (Communications) in the first instance. If the device fails and needs repair or restoration, Estates and Facilities (Communications) will restore the device to the state it was in on first delivery to the user.
 - 14.2.16 University owned portable mobile devices no longer required must be returned to Estates and Facilities (Communications) for the device to be redistributed.
- 14.3 Reporting loss to ISLS
- 14.3.1 The Estates and Facilities (Communications) team must report the loss of a mobile device to the ISLS Network Security Team as soon as possible.

15 Backup Retention and Archive Policy.

15.1 Purpose:

The purpose of this document is to establish the structures that exist around the management of data; backups; retention; destruction and retrieval of data, documents and digital content held on University of Westminster infrastructure. It also highlights limitations and exclusions to the retrieval of data. This does not replace the University's records management and related policies and can be considered a practical guide to good data management practices.

15.2 Scope:

The audience of this policy includes University users of all University systems and includes academic staff, research staff and other knowledge workers, professional support staff, students and third parties with contractual obligations to the University.

15.3 Policy

15.3.1 System Classifications

ISLS operate a tiered system for University corporate services based on the classification as described in the Information Strategy and Disaster Recovery Policy and where necessary, operate different granularity for backup retention and retrieval:

- **Tier 0** –enabling systems which are necessary for the provision of corporate systems e.g. DNS, IDM, Novell file store, iChain.
- **Tier 1** - corporate applications such as Student Record Systems, Finance Systems, Email intranet/Internet and Blackboard.
- **Tier 2** –applications which are not used across the University but which play a crucial role within specific departments e.g. Calm, Touchpaper Helpdesk System etc.

15.3.2 Infrastructure description:

Rather than relying purely on the processes around backup and restoring from tape libraries, ISLS have embraced newer techniques based on data replication and virtual technologies and these include:

- Data replication - the process of copying data from one server to another using inbuilt “on-the-fly” techniques which do not rely on proactive management and monitoring
- Log shipping -the process of automatically copying and restoring a production server's transaction logs to a standby server in the same or separate data centre
- SANS-the ability to harness large amounts of space from a confederation of smaller physical drives which provide improvements in speed and greater redundancy
- Off site backups - the process of making copies of key data to external locations on a daily and

weekly basis

- Tape Libraries - the legacy tape library is increasingly being retired

15.3.3 **Type of systems** (ISLS operates different policies for different services based on the complexity of each system)

- **Transactional systems** - these are systems, which are database driven such as SITS, SAP, and Agresso.

Where the architecture permits, and depending on the degree of criticality, replication, log shipping and virtualisation techniques are deployed as the primary method for data availability and resilience. Rigorous off-site backup and restore procedures are also used but are not the primary method for data recovery. Most Tier 1 systems rely on these types of backups.

- **File Storage**

This covers those systems which rely on storing digital content on file stores such as Novell (home areas and various shares), Unix file storage and card system security images. Rigorous on- and off-site backup and restore procedures are used as the primary method for data recovery. These mostly apply to Tier 2 applications.

- **Externally managed and hosted systems**

The University has contractual agreements with a number of third parties to manage a number of its corporate systems. Where such an arrangement exists, the third party supplier is responsible for ensuring that regular backups of the systems are maintained in line with the University Backup, Retention and Archive Policy

- **Systems**

Systems are the databases, web and application servers which configuration data only. The backing up of such configuration files is necessary for the total restoration of the system in the event of major failure.

15.4 **Frequency and Timing of Backups**

A full backup of transactional systems is automatically taken every day.

A full backup of file storage systems is automatically taken every day.

Externally managed systems should be backed up daily.

System backups are taken daily, however separate backup routines may exist for certain systems.

15.5 **Verification**

The backup logs are checked daily by ISLS and the system administrator of each service is informed in

the event of a backup failure. Persistent backup failures are noted and investigated immediately

15.6 Roles and Responsibilities:

Roles	Responsibilities
Design and execution of the log shipping, replication and virtualisation	The responsibility resides with Systems manager with escalation to the Director of IT.
Data integrity for restores (quality assurance)	The responsibility for date verification for restores resides with manager responsible for the system(s) including: Applications Manager, Systems Manager, Network manager, Network Security Officer with escalation to the Director of IT.
Locally held data	The responsibility for the backups for data held on local hardware,, USB keys, Google Apps resides with the user
Hosted system	The responsibility for the data backups resides with the data owner within the University.
Managed Service	The responsibility for data backups is as defined in the Service Contract. The primary contact is the business owner with escalation to the ISLS Systems Manager and ISLS Applications Manager.

15.7 Service Backup Levels

Service	Tier	Freq	Data Backed up	Backup Retention
Infrastructure	0		Data Configuration	Log files for > 3 months <i>As File Systems (below)</i>
Web	1	Daily	Data	Up to 3 Months
Applications	1	Daily Yearly	Data Data	Up to 3 Months Up to 3 Years
Applications (Finance related)	1	Daily Yearly	Data Data	Up to 3 Month Up to 7 years
File Systems (H:, L: etc.)	1	Daily	Data	All active files - last 3 versions Deleted files - final version for 2 years
Web	2	Daily	Data	Up to 1 Months
Applications	2	Daily	Data	Up to 1 Months
Workstations and	3	Never	None	Never

removable storage (PCs, Macs, USB keys)				
---	--	--	--	--

16 Deletion of Data

16.1 Users should be aware that data deleted from local disks by the users, may still be accessible in some cases, via certain system tools.

16.2 Contributions to online bulletin boards, non-University owned mailing lists and emails once sent are stored on machines outside the jurisdiction of the University and in these cases withdrawal or deletion of these messages or emails may not be possible.

16.3 Users should be aware that ISLS do not recover individual deleted emails however ISLS may recover individual emails following a RIPA request from the Police or in cases pending litigation and in such cases such a request would have to be approved by the Registrar and Secretary of the University.

17 Disposal of Old Equipment

17.1 Introduction

17.1.1 The frequently changing IT environment means that computing equipment (personal computers, laptops and peripherals such as printers) periodically becomes surplus to requirements or reaches the end of its useful life. Computers are usually passed on to other departments (redeployed), sold on to members of staff, given to charity organisations or disposed of.

17.1.2 The University is bound by statutory obligations such as The Data Protection Act 1998 to ensure that the data stored on these computers is securely removed prior to disposal. Any University data which is discovered by a later owner may cause the University adverse publicity or controversy.

17.2 Policy

17.2.1 Options for the disposal of IT equipment

17.2.1.1 The following order of priority should be applied to computers when they become redundant

- Redeployment to another department/School within the University.
- Subject to University Financial Regulations, equipment with a residual value may be offered to members of staff for a nominal fee, after the completion of the Removal of Equipment Form
- Donation to a University approved charitable organisation, which must guarantee the secure destruction of the data and the environmentally -friendly recycling or disposal of the equipment.
- Disposal/recycling

Note: Procedures for each of these options are detailed below in Paragraph 17.4. In all cases asset and inventory records of the serial number(s) must be accurately updated before the equipment is disposed of.

17.3 Removal of data and software

All traces of the data contained on computer equipment must be removed by ISLS and destroyed prior to their disposal. Care must be taken to meet the requirements of the Data Protection Act regarding the security of data as well as the Copyright, Design & Patents Act 1988 to ensure that software and licensing regulations are not infringed during the disposal process. Merely deleting the file or reformatting the hard drive does not remove traces of all data or prevent its recovery. Specialised “disk wiping” utilities should be used to erase to entire contents of the disk. However in cases where the redundant computer was

previously an open access lab machine, repartitioning or reformatting the disk will effectively remove the software licenses.

17.4 Procedures

17.4.1 Redeploying a computer to another department or School within the University

- Unless the recipient has a business requirement for the transfer of some of the data, ISLS must remove all the data from the computer (*see also 2. above*).
- The Dean of School, School Manager, Director of Corporate Service Department or their representative must give their explicit authorisation before data is transferred.
- If the information held on the computer relates to personal information as defined by the Data Protection Act 1998 (racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sexual life and criminal convictions), the disk should be erased with a secure disk wiping utility.
- Software or licenses must only be retained or transferred to a new owner if the University holds a license and where there is a business requirement to transfer the license.

17.4.2 Offering equipment to member of staff

- All data and software must be removed using a secure disk wiping utility.
- To comply with licences and copyright laws, ISLS must ensure that all software is removed. For the avoidance of doubt, CHEST and other site licensed software such as Microsoft SELECT software is not transferable and reformatting the disk should remove the software and licences.
- If the computer is to be used for personal purposes, the user would be offered the opportunity to purchase their own software license(s).

17.4.3 Donating to an outside body

- Donating redundant computer equipment should only be considered when it has been agreed by ISLS to be redundant in relation to University requirements.
- All software and data must be securely removed using a secure disk wiping utility.
- University licensed software must not be transferred to a third-party.
- The recipients of the computer equipment must be made aware that the University cannot guarantee the safety or suitability of the equipment and resigns all responsibility for its maintenance.
- The outside organisation must be registered as an Approved Authorised Treatment Facility (AATF) for Waste Electrical and Electronic Equipment (WEEE) by the Environment Agency, to ensure that the computer equipment will be recycled and no unusable equipment or parts will end up in landfill.

- Records should be kept of computer equipment donated to third parties, as evidence that the University is committed to increasing the rate of recycling of all appropriate materials.

17.4.4 **Disposal in an environmentally-friendly manner.**

- Older computer monitors are defined as hazardous waste and arrangements for their disposal must be made through the Estates and Facilities Department.
- The University complies with the W.E.E. Directive, which came into force on 1 July 2007. It aims to minimise the impact of electrical and electronic equipment on the environment both during their life time and when they become waste. It encourages and sets criteria for the collection, treatment, recycling and recovery of waste equipment.

Redundant equipment that cannot be redeployed, sold or donated to charity should be disposed off in an environmentally friendly manner in accordance with Section 7 of the University's Environment Policy (<http://www.wmin.ac.uk/page-15990#waste>)

18 Software and Hardware auditing

18.1 The University has an obligation to ensure that only legal software is used on University owned equipment and to support this, appropriate technology may be used to audit University owned software on University owned equipment without staff permission. Note that this will not include privately owned software.

18.2 The appropriate Dean of School, School Manager, Director of Corporate Service Department and/or Director of ISLS may be notified of any illegal software discovered as part of the audit process.

19 Removal of Equipment

- 19.1 No equipment or other electronic communication facility may be borrowed, removed or moved from a designated location, without the explicit permission of the Dean of School, School Manager, Director of Corporate Service Department or Director of ISLS or their representative, as appropriate.
- 19.2 No equipment other than equipment designed to be portable and used outside the University can be taken out of the University premises without the explicit permission of the Dean of School, School Manager, Director of Corporate Service Department or Director of ISLS or their representative, as appropriate. For permission to be granted, the necessary forms detailing the purpose of the removal of the equipment and the equipment details must be filled by the applicant and countersigned by the appropriate manager or owner as mentioned above.

20 Loss and Damage

- 20.1 Save as set out below, the University (including its affiliates, officers, agents and employees) accepts no liability to users (whether in contract, tort (including negligence), breach of statutory duty, restitution or otherwise) for:
- 20.1.1 Any loss or damage incurred by a user as a result of personal use of University ICT facilities. Users should not rely on personal use of University electronic communications facilities for communications that might be sensitive with regard to timing, financial effect, privacy or confidentiality.
 - 20.1.2 The malfunctioning of any ICT facility, or for the loss of any data or software, or the failure of any security or privacy mechanism, whether caused by any defect in the resources of the University or by any act or neglect of the University (including its affiliates, officers, agents and employees) or howsoever otherwise.
 - 20.1.3 For the acts or omissions of other providers of telecommunications services or for faults in or failures of their networks and equipment;
 - 20.1.4 For any injury, death, damage, or direct, indirect or consequential loss (all three of which terms include, without limitation, pure economic loss, loss of profits, loss of business, loss of data, loss of opportunity, depletion of goodwill and like loss) howsoever caused arising out of or in connection with the use of the University's ICT facilities.
- 20.2 The University does not exclude its liability under this Policy (if any) to users:
- 20.2.1 For personal injury or death resulting from the University's negligence;
 - 20.2.2 For any matter which it would be illegal for the University to exclude or to attempt to exclude its liability;
 - 20.2.3 For fraudulent misrepresentation.
- 20.3 Users agree not to cause any form of damage to the University's ICT facilities, or to any accommodation associated with them. Should such damage arise the University shall be entitled to recover from such user, by way of indemnity, any and all losses, costs, damages and/or expenses that the University incurs or suffers as a result of such damage.

21 Access by external entities affiliated to the University

- 21.1 External entities that have an executed contractual agreement with the University may access appropriate resources and must comply with the University's guidelines and policies.
- 21.2 All requests from external entities that have responsibilities for supporting computer systems should submit a request via the Fix-IT Centre to the ISLS Network Security Team and include the following:
- * Date
 - * Name of Individual Requesting Access
 - * Organization
 - * Address and Telephone Number of person requesting access
 - * Name of University systems contact
 - * Resources Required
 - * IP Address of internal machine to be accessed
 - * IP Address of external company
 - * Port number and service required
 - * Operating System
 - * Application software
 - * Number of Users needing access
 - * Length of time access required for (maximum 12 months)
- 21.3 The ISLS Security Team will review and determine the level of risk associated with each request;
- 21.3.1 if the request is approved, the organisation will be notified by the ISLS Network Security Team; and
- 21.3.2 the University contact will notify the requester with the account and access information.
- 21.4 External contractors may access University ICT facilities to gain access to their home site; however they must obey and sign any published rules for their use (e.g. the University Non Disclosure Agreement and the University ICT Acceptable Use Policy and Procedures).
- 21.5 The employer of external contractors or companies will be held jointly liable for any actions on their part or that of their employees, agents or subcontractors that violate the University Acceptable Use Policy and Procedures.
- 21.6 Any external visitors or conferences that have been authorised to use the University ICT facilities are bound by University guidelines and policies and are liable for the actions of the attendees.

22 Investigation and response to ICT violations

22.1 Introduction

22.2 ISLS has the operational responsibility for the University network and central computing resources and it has an obligation to protect the confidentiality, integrity and availability of the network by ensuring that the resources are available and accessible. In some cases, ISLS may devolve some of that operational responsibility and related obligations to a School (e.g. ECS).

22.3 To meet this obligation, the ISLS Security Officer may monitor and respond to network breaches as they occur.

22.4 The University recognises that principles of academic freedom, freedom of speech, and privacy of personal information hold important implications for the use of electronic communications. The University affords privacy protections to electronic communications comparable to those it traditionally affords paper mail and telephone conversations. This policy reflects these firmly held principles within the context of the University's legal obligations.

22.5 University policy prohibits University employees and others from seeking out, using, or disclosing personal information without authorisation, and requires employees to take necessary precautions to protect the confidentiality of personal information encountered in the performance of their duties or otherwise. This prohibition applies to electronic communications.

22.6 Any decisions made by the ISLS Security Officer will be communicated to the appropriate ISLS service and ECS managers who meet regularly to discuss operational issues including non urgent security related issues.

22.7 Policy

22.7.1 Instances of breaches may be drawn to the attention of the University's Network Security Team via internal or external complaints, the intrusion detection system or discovered in the normal course of business.

22.7.2 The actions taken during a policy violation are dependent on the particular circumstances.

22.7.3 The ISLS Network Security Team may temporarily suspend network access if the incident is determined to be interfering with the operations of the University network. In the event that a computer's network access is disabled for operational reasons, the FIX-IT Centre would be immediately informed of the decisions and the reasons behind that decision.

22.7.4 In the event that a user password is compromised, the ISLS Network Security Team would immediately reset the user's password to a one-time only password and inform the FIX-IT Centre accordingly. The FIX-IT centre would contact the user and ask them to reset their

password. Such actions are necessary to mitigate the risks from unauthorised access to University systems.

22.8 The ISLS Security Officer will also:

22.8.1 Determine the impact of the alleged violation and take, without notice, any necessary action if University resources and services are adversely affected to prevent immediate and further damage to the University network. Such actions may include:

- Suspension of an account
- Disconnection of systems or disable network ports
- Termination of running processes and programs
- Any other actions deemed necessary to restore network services.

22.8.2 Gather evidence and provide information as directed by the appropriate Dean of School, School Manager or Director of Corporate Service Department to comply with any internal investigation. In limited cases, the users may not be notified first if the University is required by law to provide the information without notifying the user in accordance with the Regulation of Investigatory Powers Act 2000 in the prevention or detection or crime.

22.8.3 Determine if the University is legally obliged to report the alleged incident to the police authorities via the Office of the Registrar & Secretary.

22.8.4 Investigate and address the complaint. Such investigation may involve examining systems and network activity logs and transaction logs. Contents of emails and other files will not be examined without the holder being notified as part of a routine except in the following circumstances:

- A court order requires that the content be examined and disclosed.
- The ISLS Security Officer is instructed in writing either by the Director of ISLS or the University Registrar & Secretary as part of an internal investigation.
- ICT staff are conducting an internal investigation relating to systems performance or problems which require that user files must be examined to identify a cause. In this case the member of staff must seek guidance from the Director of ISLS or an ISLS manager prior to the work being undertaken. During such investigations if any illegal activity is discovered, then the investigation will be referred immediately to the Vice Chancellor, the University Registrar & Secretary or the Director of ISLS.

22.8.5 If the violation does not prevent other users from accessing network computer resources or result in a disciplinary procedure being instigated, the ISLS Security Officer will notify the FIX-IT Centre of the activities causing the violation. The matter will however be referred to the appropriate administrative authority for disciplinary action if the user refuses to comply.

22.8.6 If the investigation into the violation requires the physical examination of the computer or any removable storage, the ISLS Network Security Officer, with authorisation from the Director of ISLS, may engage the services of an approved external agency to ensure that the digital

evidence is gathered in accordance with ACPO's (Association of Chief Police Officers) guidance as described in "Good Practice Guide for Computer-Based Electronic Evidence"

22.8.7 Network access may be terminated immediately if the violation has been caused by an external entity with a contractual agreement with the University whilst the violation is investigated.

22.9 Unavoidable Inspection

22.9.1 Users should be aware that, during the performance of their duties, personnel who operate and support ICT facilities need from time to time to monitor transmissions or observe certain transactional information to ensure proper functioning of University ICT facilities and services. On these and other occasions they might inadvertently observe the contents of emails.

22.9.2 Except as provided elsewhere in this Policy or by law, they are not permitted to:

- hear, see, or read the contents intentionally;
- observe transactional information where not germane to the foregoing purpose; or
- disclose or otherwise use what they have seen, heard, or read.

Disciplinary action will be taken against any ICT staff observed intentionally gaining access to user data which has no relevance to the investigation

22.9.3 One exception to the foregoing paragraph is the need for systems personnel to inspect the contents of electronic communications and transactional records when redirecting or disposing of otherwise undeliverable electronic communications.

22.9.4 Such unavoidable inspection of electronic communications is limited to the least invasive level of inspection required to perform such duties. This exception does not exempt systems personnel from the prohibition against disclosure of personal and confidential information, except insofar as such disclosure equates with good faith attempts to route the otherwise undeliverable electronic communication to its intended recipients.

22.9.5 Re-routed electronic communications normally should be accompanied by notification to the recipient that the electronic communication has been inspected for such purposes.

22.9.6 Except as provided above, systems personnel shall not intentionally search electronic communications records or transactional information for violations of law or policy but shall report violations discovered inadvertently in the course of their duties.

23 Taking down materials published on the internet in accordance with Terrorism laws.

23.1 Introduction

23.1.1 The University takes all breaches of the Acceptable Use Policy very seriously but this issue is exceptional because the University is expected to act immediately upon receiving the notice from the Police.

23.1.2 Sections 1 and 2 of the Terrorism Act 2006 make it an offence to encourage terrorism and also to distribute information that is deemed to perpetuate terrorism through any media.

23.1.3 Section 3 of the aforementioned Act dictates that any organisation that refuses to remove any information covered by the act without any reasonable excuse will be seen as endorsing the materials and information and so leaves itself liable to prosecution. Section 3 of the Act gives the police the right to serve a notice on the University of Westminster as a provider of electronic communications to remove materials that directly or indirectly promote or disseminate terrorism.

23.1.4 The University will comply with notices to take down information that may be deemed as glorifying terrorism in response to a request by the police under a Section 3 notice.

23.2 Notices under Section 3 of the Terrorism Act should normally be given in writing or email to the University of Westminster Registrar & Secretary identifying the materials to be removed. The University will deal with Section 3 notices issued by the police by using the Acceptable Use Policy as it would with other ICT violations.

23.3 If asked by the police to retain the information for prosecution, ISLS will preserve a snapshot of the website and the backup tapes in conformity with the stipulations of the RIPA Act 2000 which covers the interception of communication.

23.4 The University will deal with any request to remove materials that that may be deemed as glorifying terrorism or which directly or indirectly promote or disseminate terrorism by invoking the Acceptable Use Policy and Procedures (AUP). Under Section 8 of AUP, ISLS will investigate and respond to such a request as it would with other ICT violations.

24 Reporting Security Incidents

- 24.1 All users of the University ICT facilities are encouraged to note and report any observed or suspected security incidents, security weaknesses in or threats to systems and services. Such incidents should be reported via the FIX-IT Centre.
Telephone: +44 (0)20 7915 5488, or 5488 from any University building.
Email: Fix-IT@wmin.ac.uk
Website: ResolveIT - <http://www.wmin.ac.uk/page-10304>
- 24.2 All external complaints against the University of Westminster must be reported to abuse@wmin.ac.uk
- 24.3 All reports of unsolicited emails including spam should be reported to the Fix-IT centre or abuse@wmin.ac.uk.

Appendix 1: Guidelines and Policy References

Combined Higher Education Software Team (CHEST) Code of Conduct
<http://www.eduserv.org.uk/licence-negotiation/general/conduct/>

Copyright Guide for staff
<http://www.wmin.ac.uk/main.asp?page=5895>

Data Protection
<http://www.wmin.ac.uk/page-1563>

Environment Policy
<http://www.wmin.ac.uk/page-15990#waste>

Essential Westminster: The Student Guide 2008/09
<http://www.wmin.ac.uk/page-8183>

Freedom of Information Act Staff Guidance
<http://www.wmin.ac.uk/Default.aspx?page=8274>

Good Practice Guide for Computer-Based Electronic Evidence
<http://www.acpo.police.uk/asp/policies/Data/ACPO%20Guidelines%20v18.pdf>

JANET Acceptable Use Policy
<http://www.ja.net/services/publications/policy/aup.html>

JANET Security Policy
<http://www.ja.net/documents/publications/policy/security.pdf>

Staff handbook
<http://www.wmin.ac.uk/pdf/STAFF%20HANDBOOKV3.pdf>

University of Westminster Records Management Policy
<http://www.wmin.ac.uk/pdf/University%20of%20Westminster%20RM%20Policy%202008.pdf>

Wireless Networking Policy
<http://www.wmin.ac.uk/page-1656>

University of Westminster IP Policy
<http://www.wmin.ac.uk/pdf/UoW%20intellectual%20property%20policy%20October%202007%20v3a.pdf>

Appendix 2: External Acts

The use of computer and network resources is subject without limitation to the following Statutes and Regulations.

- Obscene Publications Act 1964
- Sex Discrimination Act 1975
- Computer Copyright Software Amendment Act 1985
- Copyright, Designs and Patents Act, 1988 and subsequent regulations
- Malicious Communications Act 1988
- Computer Misuse Act, 1990
- Criminal Justice and Public Order Act 1994
- Human Rights Act 1998
- Data Protection Act, 1998
- Freedom of Information Act 2000
- Race Relations Act 2000
- Regulation of Investigatory Powers Act 2000
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Anti-terrorism, Crime and Security Act 2001
- Communications Act 2003
- Terrorism Act 2006
- Criminal Justice and Immigration Act 2008