IT Policy, Procedures and Guidance
University College, Oxford

Patrick Baird

IT and Web Fellow

Andy Hamilton

IT Manager

Helene Augar

College Registrar

Summary

This policy and guidance document is presented as a core document (overview) followed by a series of ten appendices where the details under various headings can be found. The table of contents produces a quick summary with links to the appropriate sections of the document. The authors recognise that some aspects of IT provision and guidance may become out of date relatively quickly and that occasionally links may become broken. We therefore welcome feedback to correct for this and in general constructive criticism to improve the clarity and scope of the document; such feedback should be addressed to the IT department.

Contents

1. Introduction

The purpose of this document is to inform members of College of what can be expected in terms of Information Technology (IT). This covers the use of all computers and other related hardware such as printers and projectors and the use of the network infrastructure. Since the College's network is directly linked to the main University network this policy document necessarily includes the *Regulations and Policies applying to use of University ICT Facilities* laid down by the University and which can be viewed at: http://www.it.ox.ac.uk/legal/rules/. In the following, the use of computers connected to the College network both for academic and administrative purposes is covered together with the procurement of IT equipment and the maintenance and support of it by the College.

2. Service and Support

2.1. Structure. At the heart of the College's IT structure is the IT department. The IT Manager is responsible for the day-to-day running of IT services and for ensuring the priorities of work follow the agreed service level description available at: http://www.univ.ox.ac.uk/content/policy-documents. The IT Fellow is responsible to the Governing Body for all aspects of the College's IT service, support and development. In addition, there is a Web Fellow who is separately responsible for the development of the College's websites and for web communications.

2.2. Support Priorities. The Service Level Description (SLD) gives a detailed description of the service and support priorities currently employed by the IT department (Appendix A); here we give only a summary of the priorities which are ranked A to G.

A: The first priority is to ensure the IT infrastructure remains in operation; this includes both the network and servers. From time to time upgrades and developments to the network and servers will be necessary and will take high priority in order to minimise overall disruption and to accommodate on-site contractors.

B: The College administration infrastructure is next; this includes supported departmental systems such as databases and booking systems, also shared printers. [Priority for any one department will depend on time of year, so, for example, the Academic Office is given priority during the admissions cycle; the Domestic Bursary during the conference season and the Treasury at the time of the Bursar's report.] Finally, within this category is equipment to be used for an imminent presentation within college.

C: Academic priorities: this includes support for Fellows and College Lecturers to ensure there is no serious interruption in the operation of their IT equipment.

D: The College computer rooms: to ensure these remain fully operational with an ordering of: (a) the network integrity for an entire room, (b) breakdown of a printer or other peripheral device, where no alternative is available locally.

E: For the single-user: breakdown of an individual computer or other college-owned peripheral devices; software problems, major hardware problems affecting *non-college owned equipment* but being used for academic or college-related work.

F: Current students with critical problems involving their own personal PCs; single-user network or software problems.

G: Help and advice on equipment, software upgrades and general IT requests from Fellows and Lecturers.

Notwithstanding the above ordering it will be open to either the IT Manager or the IT Fellow to escalate a support request if it has consequences for the operation of an immediate college activity.

3. Security

3.1. Network and Computers. Security of our network and of the computers used for the administration of College business is a crucial aspect of our IT-policy. For this reason, all computers attached to the network must have anti-virus software installed and in general should be checked before any connection is made to the network by the IT department. Owners of personal computers are responsible for ensuring that their software is up-to-date in terms of security patches and anti-virus updates. In general, this will be configured automatically but owners must ultimately take responsibility for their own equipment. This includes care in the choice of passwords and in the use of email accounts. Breaches in security where this is due to inappropriate computer use will be viewed seriously by the College and could result in temporary exclusion from the network (- see also under section(11)). In addition, the University has now released (July 2012) its own information security policy available at: http://www.oucs.ox.ac.uk/network/security/ISBP/ispolicy.xml?ID=aims. The College as part of the part of the University adheres to this policy and, in particular, recognises that:
"The University is committed to protecting the security of its information and information systems in order to ensure that:

(1) the integrity of information is maintained, so that it is accurate, up to date and fit for purpose;
(2) information is always available to those who need it and there is no disruption to the business of the University;

(3) confidentiality is not breached, so that information is accessed only by those authorised to do so;
(4) the University meets its legal requirements, including those applicable to personal data under the Data Protection Act; and
(5) the reputation of the University is safeguarded."

We interpret "University" here as including the College.

Furthermore, we note the University policy requires that:

"There must be a written policy in place at the local level for the handling of confidential information, whether electronic or hard copy, and a copy of the procedures must be provided to every user so that they are aware of their responsibilities.

Any failure to comply with the policy may result in disciplinary action."

Our relevant policy is contained in Appendix B.

For reference the relevant legislation includes, but is not limited to, the following:

* The Computer Misuse Act (1990)
* The Data Protection Act (1998)
* The Regulation of Investigatory Powers Act (2000)
* The Telecommunications (Lawful Business Practice) (Interception of Communications)
* Regulations (2000)
* The Freedom of Information Act (2000)
* The Special Educational Needs and Disability Act (2001).

3.2. Firewall. The College network incorporates a *firewall* to control data traffic into and out of our local network; this increases the security of our network and helps to keep the threat of malicious attacks to a minimum and to keep confidential information secure. The description of our firewall and the policy relating to it are given in Appendix C

3.3. Retention of Data. Anti-terrorism, crime and security law have implications for the data we retain with regard to digital communications. In brief, the Data Retention (EC Directive) regulations of 2009 require Internet Service Providers (ISPs) to retain data necessary to:

(i) trace and identify the source of communication;
(ii) identify the destination of a communication;
(iii) identify the date, time and duration of a communication; and

(iv) identify the type of communication.

In the words of the 2009 Regulations, this includes data generated or processed by means of 'mobile telephony', 'internet access', 'internet email' and 'internet telephony.' It is also necessary to identify the users' communication equipment. Further background information is provided in Appendix D.

4. Software

The College takes seriously breaches of software licence agreements and piracy with respect to software packages. For the purposes of the College's administration, computer software will be installed by the College's IT department; for students' personal computers software will be assumed to be *bona fide* and kept up-to-date with the latest security patches where appropriate (e.g. for Adobe Reader, Microsoft Office, OSX etc). For standard software configurations provided by the IT department see Appendix E.

5. Procurement of IT Equipment

In general computers and other equipment used by the various College Offices are procured by the IT Manager under a rolling renewal policy. Computers used for administrative purposes have in general a common program suite to cover most daily tasks as well as specific departmental software. Other additional software can be arranged through the IT Manager as necessary subject to the user's need in relation to their College duties. All new college computers will have appropriate anti-virus, anti-spyware and malware software installed, and generally software updates will either be automatic or organised through the IT Manager on a routine basis. Procurement of mobile devices (section 10) should be authorised by line managers giving business cases for each device requested; these should be set up and registered by the IT department. In ordering equipment for the College, the IT Manager will ensure that full use is made of educational and other discounts and will ensure that an up-to-date database (inventory) exists for all such equipment, including mobile devices; this is to ensure timely upgrades of equipment under the renewal policy and to assist in cases of theft leading to insurance claims (Appendix E).

6. The College Network

The College network comprises optical, wired and wireless connections throughout the various college sites. Switch gear and wireless access points are the property of the College and are maintained by the College for its academic pursuits and its administration. Only contractors engaged by the IT department and the members of the IT department shall have direct access to any hardware component of the network, and interfering with any part of the wiring, optical fibres and hardware by any college member will be deemed to be a serious matter.

7. Oxford Email Accounts and the Internet

To obtain a University/College email account a user first requires a University Card. Once this has been issued an email account is automatically created by Central IT Services; this will be of the form: *first.last@college.ox.ac.uk* While it is open to the College to set up an office name to cover, for example, general enquiries, this needs to involve the IT department. For further details see for example: http://www.oucs.ox.ac.uk/email/oxford/index.xml?splitLevel=-1.

Other email accounts, available through outside providers, e.g., *gmail, hotmail* etc., can be set up by individuals but accounts incorporating the College's name should only be used by agreement with the relevant line manager and IT Fellow; the IT Manager should hold all relevant details of the account including passwords which should be sufficiently strong to ensure necessary security. Such accounts should not be used in any way that attracts unauthorised cost or defamation to the College or University. Inappropriate use of email accounts or the internet may lead to sanctions and to suspension from the network (see also, section 11).

As regards use of the internet, all students and visitors should read and sign the College's acceptable use policy (Appendix F); this includes and extends item 7 of the University's own regulations, *viz.*

"Users are not permitted to use University IT or network facilities for any of the following:

(1) any unlawful activity;

(2) the creation, transmission, storage, downloading, or display of any offensive, obscene, indecent, or menacing images, data, or other material, or any data capable of being resolved into such images or material, except in the case of the use of the facilities for properly supervised research purposes when that use is lawful and when the user has obtained prior written authority for the particular activity from the head of his or her department or the chairman of his or her faculty board (or, if the user is the head of a department or the chairman of a faculty board, from the head of his or her division);

(3) the creation, transmission, or display of material which is designed or likely to harass another person in breach of the University's Code of Practice on Harassment;

(4) the creation or transmission of defamatory material about any individual or organisation;

(5) the sending of any e-mail that does not correctly identify the sender of that e-mail or attempts to disguise the identity of the computer from which it was sent;

(6) the sending of any message appearing to originate from another person, or otherwise attempting to impersonate another person;

(7) the transmission, without proper authorisation, of e-mail to a large number of recipients, unless those recipients have indicated an interest in receiving such e-mail, or the sending or forwarding of e-mail which is intended to encourage the propagation of copies of itself;

(8) the creation or transmission of or access to material in such a way as to infringe a copyright, moral right, trade mark, or other intellectual property right;

(9) private profit, except to the extent authorised under the user's conditions of employment or other agreement with the University or a college; or commercial purposes (including advertising commercial services) without specific authorisation;

(10) gaining or attempting to gain unauthorised access to any facility or service within or outside the University, or making any attempt to disrupt or impair such a service;

(11) the deliberate or reckless undertaking of activities such as may result in any of the following:

(a) the waste of staff effort or network resources, including time on any system accessible via the university network;

(b) the corruption or disruption of other users' data;

(c) the unauthorised access, transmission or negligent loss of data;

(d) the violation of the privacy of other users;

(e) the disruption of the work of other users;

(f) the introduction or transmission of a virus or other malicious software into the network;

(12) activities not directly connected with employment, study, or research in the University or the colleges (excluding reasonable and limited use for social and recreational purposes where not in breach of these regulations or otherwise forbidden) without proper authorisation."

Furthermore, particular attention is drawn to 13 (5) in Appendix F. This means that distributed file sharing is not permitted under any circumstances; for the avoidance of doubt this means file-sharing programs, including but not limited to (BitTorrent, Kazaa, eMule, uTorrent, Limewire, Thunder, Vuze and Ares) should never be used on the College network.

Please be aware that computers on a high bandwidth network such as ours are a prime target and new vulnerabilities are discovered every day. You are encouraged to keep your machine's protection software updated and to take great care when opening email attachments. The IT team will advise you on sensible precautions as necessary.

8. Guidance on the Use of Emails

Use of electronic mail is both widespread and common throughout the University. While use email communication is of tremendous value there are, nevertheless, a number of potential pitfalls and all users should be aware of these when transmitting, receiving and storing such messages. Below some guidance is provided which both represents good practice and identifies some of the major risks. (More information and guidance can be found on the central IT Services website at: http://www.oucs.ox.ac.uk/email/netiquette/)

8.1. Risks associated with Email Correspondence.

(1) Emails carry the same weight of evidence as other types of written communication. Do not type anything which you would not be comfortable printing with a University letterhead since in the eyes of the law there is no difference.
(2) Emails sent using University systems belong to the University and not to you as an individual.
(3) Emails are legally enforceable. If you 'informally' agree to do something by email or use email to request goods or services, the email constitutes a contract.
(4) Because email has the same legal status as a signed document on University letterhead, email exchanges for contractual discussions must be managed carefully, to ensure that there is *a clear distinction between negotiating the terms and conditions of a contract, and agreeing them (and thereby entering into a contract).*
(5) Emails are legally disclosable. In response to requests under the Freedom of Information and Data Protection acts, and following court orders, most information contained in an email is disclosable.
(6) Email is not secure and is easily intercepted.

8.2. Inappropriate Use of Email.

(1) When transferring documents, particularly where you wish to make documents available to multiple recipients, email is not the most suitable means of distribution. For each person to whom the email is being distributed, a copy is stored in each of their email accounts, as well as in your own sent items folder. This is inefficient use of mail store quite apart from any security issues.
(2) In situations where you need to transfer documents to others: the best practice is to place the documents in a location accessible to all of your recipients, whether this is an intranet , sharepoint or internet site, or your departmental networked file store. You can then email your recipients with details of the location.
(3) When communicating about other members of staff (or students) you need to be mindful that under the Data Protection Act, staff and students have a number of rights. This includes the right to access almost any information held about them by the University, including emails *in which they are identified.* This is a right which is increasingly being used in grievance/complaints situations. If you need to communicate potentially sensitive information (including communicating with HR), it is more appropriate to carry this out in person and (if need be) commit a summary of meeting notes in your own, non-work related, private diary/notebook.

9. Social Media

Social media accounts set up in the name of the College, or attributable to the College, can provide a fast route for feedback, comments and ideas. As such this facility provides a valuable forum for discussion. Unfortunately, it is open to abuse and can in extreme cases lead to reputational damage to the Institution or individual defamation of character and subsequent legal action. With this in mind, all College related social media accounts (facebook, twitter etc) should have a key administrator who takes responsibility for the account and who is responsible for granting *write* (administrator) access to the account. The College Registrar is to be the key administrator on all such college accounts and should hold account details and any necessary passwords. As a general rule there is a need to be careful over copyright, trademarks, data protection and the use of logos. Also, in the interests of security users should avoid revealing personal information where possible, avoid any dialogue with journalists and avoid unsubstantiated claims. Further details of the policy under this heading are given in Appendix G.

10. Management of the College Websites

The College's websites are overseen by a Communications Group which meets regularly during the academic year. There are currently representatives from the Governing Body, the Academic Office, the Development Office, the IT department, the Library as well as from the WCR and JCR. The Group is chaired by the Web Fellow with the College Registrar acting as secretary for the group. To ensure coherence across the site a protocol has been established which is given in Appendix H; the College Registrar is responsible for ensuring compliance with relevant legislation and with the College's policies and standards regarding quality and presentation. This includes the accuracy of the content and ensuring that the site is kept up to date.

11. WiFi andVoIP

The College is aware of the growing use of mobile equipment and is expanding its WiFi provision accordingly for all members of College. In some areas such as the Staverton site there is both commercial provision for conferences and, for University members WiFi which is linked to the Janet network for academic use. Around the main site there are WiFi access points for connection to the University network, the college's intranet and the internet via OWL or eduroam. There is also access to UCO-Public both in and out term time; this is maintained for College guests who are not academic members of the University. The College has set as a high priority complete coverage of the main site in the near future. In the most recently refurnished and new accommodation, provision has also been made for voice over internet telephones (VoIP). The University's need to move away from standard, exchange-linked telephony has been noted and this strategy is driving our

own IT development. (See, for example, http://www.oucs.ox.ac.uk/telecom/voip/ for further information). Our policy on WiFi is laid out in Appendix I.

12. Mobile Devices

Mobile devices are becoming increasingly common and sophisticated. These range from tablet computers and iPads to smartphones. In what follows devices which use SIM cards of any description are included. The College only supports the acquisition and maintenance of mobile phones (including smartphones) and other mobile devices where a person's work requires the use of such devices. In these cases the choice of network (carrier) will be at the College's discretion using a corporate account. Use of such College-owned devices should be related only to calls and emails made in the context of College activities. (The full mobile device policy is contained in Appendix J.)

13. Transgressions (Junior Members)

A student who receives a University *cease and desist* notice, which is copied on to the IT department in College, will usually be blocked by central IT services. Within College the procedure that then operates is outlined below.

(1) The IT Manager will email or otherwise contact the offender as well as the IT Fellow and the Dean. (The student would normally be asked to bring in their computer and arrange a time for the IT staff to look at the machine.)
(2) The IT staff would then "clean" the computer following the University's instructions and then report back to the IT Fellow, Dean and central IT Services.
(3) An invoice would be created by the Treasury and would be sent to the student to cover the time taken to clean the machine and to cover the charge levied by the University; altogether this is likely to be in the region of £100. In addition, it is open to the Dean to impose further punishment in severe cases; this could take the form of a fine or additional time without a network connection. (At best, the offender could be offline for the time it takes to clean the machine - roughly 1-2 days).
(4) If a SECOND notice is subsequently issued by the University then the College would normally increase the cost to the offender; the time spent offline would then become a decision for the Dean and IT Fellow.
(5) Should a THIRD notice ever be issued, the financial cost would be a matter for the Dean and IT Fellow to decide; however, at this point the Proctors may also become involved and may impose additional University-wide sanctions.

In other cases involving a breach of security, or a charge of computer hacking, damage or improper use of equipment, or use of equipment that affects the entire college network, then the following sequence of events would be triggered.

(1) The student would get an email from the IT department.
(2) The IT Fellow would also be informed.
(3) There will be an interview with the student either conducted by the IT Manager, the IT Fellow, or both depending on the nature of the breach. The student's account would be temporarily suspended, while the breach is investigated, usually for a period of 1-2 days.
(4) If the breach is significant and further measures are necessary then the Dean, IT Fellow and Proctors are likely to become involved.
(5) It will be up to the IT Fellow, and Dean to impose a fine or a period offline or both quite apart from any University sanctions imposed by the Proctors.

14. Flexible Hours and Working at Home (Staff)

It is recognised that there may be situations when college staff may wish to work at home and that it is desirable for them to do so. Alternatively, there may be good reasons for some staff to have flexibility within their contracted hours. Where this is approved by the relevant authority, e.g. head of department, arrangements will need to be made to ensure that college-owned equipment is both made available and is maintained for this activity. In these situations, where IT support or equipment is needed, arrangements with the IT department will need to be made. However, the IT department can give no guarantees for support out of normal hours. In addition, from time to time, there may be special circumstances under which a significant amount of college work is undertaken away from college premises. Arrangements for these special circumstances, for example during a major flu pandemic, might necessitate variations to the overall IT policy, and nothing contained within this policy shall prevent justifiable variations as approved by the IT Fellow and Governing Body. Further details and conditions pertaining to working at home and flexible working hours can be found in the relevant College policy documents but nothing therein shall be taken to override this policy concerning IT services.

15. Revisions to this Policy

It is anticipated, with the speed of development in IT equipment and infrastructure, that revisions may from time to time be necessary to this policy document. In the first instance it will be for the IT Fellow to bring forward such changes which will then go to Governing Body for approval. In any case, the policy document will be reviewed annually and updated as necessary in the light of developments both within College and in the wider University.

Appendices

Appendix A: Full Service Level Document (SLD)
Appendix B: Security Policy Document
Appendix C: Firewall Security Policy
Appendix D: Data Retention Policy
Appendix E: IT Equipment and Software Policy
Appendix F: Acceptable Usage Policy
Appendix G: Social Media Policy
Appendix H: College Website Protocol
Appendix I: WiFi Policy
Appendix J: Mobile Device Policy

APPENDIX A

Service Level Description: Computer Support

A. Hamilton

1. Service Objectives

We aim to respond to the notification of a problem in categories B to F below within one working day. Our working days are Monday to Friday, 8.30am to 5.30pm. For example, if a problem is reported at 2pm Monday to Thursday, our target is to respond before 2pm the next day. If you tell us of a problem at 2pm on a Friday, our target is to respond by 2pm on the following Monday.

Telephone and email notifications are given identical priority. If we cannot attend to the notified problem within one working day we will contact you within one working day to hear about your problem and to make a suitable appointment to assist with it. If a major problem occurs outside the working day, we will respond as soon as we can, but out-of-hours staff availability cannot be guaranteed and the timescale for response will therefore vary. (Note that not every response takes the form of a physical presence or a 'call out.)

For problems not covered by our response priorities, but within our overall remit (category G), we will arrange to assist you when time becomes available, which may be during a less busy period.

2. Response Priorities

A: Our first priority is always to keep the Colleges IT infrastructure up and running. Failure at this level will always be regarded as a category A emergency and, so far as necessary, other work, including planned and promised work, will give way to it.

The following sub-priorities will apply in the event of multiple simultaneous problems: (1) Network infrastructure - a. Switches; b. Firewall; c. Security Systems; d. Cable breakages (2) Server infrastructure - a. DHCP; b. Department servers; c. Groupwise; d. Domain server.

B: Our next priority is to ensure that the College's administrative and support functions are not significantly impaired. Priority B will include problems in College departments (and problems reported by College Officers) that are interrupting essential work. Problems with terminals in the Library (but not in the computing rooms) are dealt with in this category.

The following sub-priorities will apply in the event of multiple simultaneous problems: (1) Network offline department-wide; (2) Breakdown of a PC; (3) Breakdown of a shared printer where no alternative is available locally; (4) Supported departmental systems (e.g., Current Members, Kinetix, Raisers Edge etc.

Where problems occur in more than one department, the type of function being impaired determines priority. At admissions time, for example, the working of the Academic Office would take priority; in conference periods, it might be the Domestic Bursary.

Emergency problems with audio-visual equipment are also treated as a category B priority, irrespective of who has the problem.

C: Our next priority is to ensure that the general academic work, or work for the College, Fellows and College Lecturers is not interrupted by serious computing problems.

Where multiple users have problems simultaneously, priority is determined by the following considerations. Fellows take priority, all else being equal, over College Lecturers. Work immediately affecting the College, its students, or its prospective students takes priority, all else being equal, over other kinds of work, including research.

D: Our next priority is to ensure that the College's computing rooms are fully functional.

The following sub-priorities will apply in the event of multiple simultaneous problems: (1) Network offline for a whole computing room; (2) Breakdown of a printer or other peripheral where no alternative is available locally.

E: The following problems may be experienced by all groups and will be dealt with in the order of B, C and D above.

(1) Network offline for a single user; (2) Breakdown of a single PC; (3) Breakdown of other college-owned printers and peripherals where no alternative is available locally; (4) Software problems, including email client problems; (5) Major hardware problems afflicting non-college-owned equipment used primarily for academic or College-related work.

F: Our final response priority is to assist the College's current students with critical problems in their personally owned computing facilities. Daily drop-in clinics are held during term-time and students are expected to attend clinics for their software and hardware problems. Only under exceptional circumstances will a clinic be cancelled.

The following sub-priorities will apply in the event of multiple simultaneous problems: (1) Network offline for a single user or at a single location; (2) Software or hardware problems on a desktop PC.

G: Other problems (dealing with annoying computer behaviour, help with upgrades, advice on choice of equipment, etc.) are not regarded as urgent

and are not covered by our one working day service aim. If they are within our remit we will, however, try to help where we can, but subject to our availability after taking account of priorities A to F above.
The following sub-priorities will apply in the event of multiple simultaneous requests: (1) Departmental requests for assistance; (2) Requests by Fellows; (3) Requests by College Lecturers; (4) Requests by students and (out of term) by conference guests.

Notwithstanding the above ordering it will be open to the IT Manager to escalate a support request if it has consequences for the operation of an immediate college activity. An example might be support for mobile equipment used during a visit abroad as part of a College campaign.

3. What is not within our computing support remit

Maintaining the code or the content of any college website (except for the intranet website). Systematic training (as opposed to occasional problem-solving) on software, including operating systems, email clients, database programs, etc. Support for new technologies unless we have ratified them first as fit for the intended purpose. (Even then we do not undertake to become experts but only to support on a what we already know basis.) Support for software supplied to the College by a third party where a support contract is in place, or if we have not had the correct training. [Exception: we will endeavour to help where the supplier or service contractor is prepared to provide full technical support to us in doing so.] Support for your internet connection at home, (unless supplied by the college). Providing hardware repairs to student-owned computers (although we might take a quick look). Installing or reinstalling operating systems on student-owned computers. Support for WiFi or other network devices, unless they conform to the University and College rules, and we have purchased and set up the equipment being installed. [NB: Network devices are not allowed except with the Colleges permission, which will rarely be forthcoming.] A single students multi-computer setup. [NB: multi-computer setups are not allowed except with the Colleges permission, which will rarely be forthcoming.] Pulling through ethernet or fibre cabling; installing or rewiring ethernet points. Moving furniture, in computing rooms or elsewhere. Building computers from scratch to meet a user's specifications. Photocopiers and telephones (except VoIP).

APPENDIX B

Security Policy Document

A. Hamilton

1. Introduction

The College IT department is committed to ensuring that, as far as it is reasonably practicable, the way we provide services to the public and to our staff reflects their individual needs and is in line with the College and University Equality Policies. University College will do its utmost to support and develop equitable adherence to all policies. Managers are responsible for ensuring that all staff, within their area of responsibility, are aware of the College's policies and that staff adhere to them. Managers are responsible for ensuring that a system is in place which keeps their staff up to date with new policy statements. Staff are responsible for ensuring they are familiar with policies, know where to locate the documents on the College's website and intranet site, and seek out every opportunity to keep up to date with them. Independent contractors must put forward a person to be responsible for ensuring their Staff are aware of the College's policies. This policy is individual to University College. The College does not accept any liability to any third party that adopts or amends this policy.

2. The Reason for this document

All electronic information, either in the form of learning and research material or staff and student information is a valuable resource; the College for its part needs to take measures to protect against many hazards, e.g. the loss, corruption or the unauthorised access and modification of data. In addition, such information and the way it is processed are subject to UK law, specifically the eight principles of the Data Protection Act 1998. This document follows the broad outline of ISO-17799 guidelines for information security.

3. Scope

This document defines how the College will secure electronic information, that is:

- the security of information held in electronic form on any College computer;
- information belonging to College staff and students;

- information belonging to external users and guest users that are authorised to use College IT facilities;
- action in the event of a breach of the policy;
- the locations of College electronic information.

4. Legislation and Policy

4.1. Legislation. The supply and use of the University IT facilities (and therefore College facilities) is bound by the laws of the UK. A list of these rules is given in the Regulations and Policies applying to all users of the University's ICT facilities (http://www.ict.ox.ac.uk/oxford/rules/).

4.2. Associated Policies. Applicable policies include those listed below. This list is not exhaustive and may be subject to change.

(1) JANET Acceptable Use Policy
(2) Oxford University Acceptable Use Policy
(3) Chest Code of Conduct
(4) University College Acceptable Use Policy
(5) Regulations and Policies for the use of the University's ICT facilities.

5. Asset Clarification

The IT department will maintain an inventory of assets under two categories:-

- Hardware
- Software

This inventory is in addition to asset records maintained under University financial regulations. Any system and the data it contains, which is not part of the above inventory, is the responsibility of the user of that system, but is still subject to this Security Policy.

6. People Issues

The IT department maintains and has access to directories of people authorised to use the College IT facilities. Staff, students, external users and guest users are subject to the College's conditions for use of IT but have differing rights and responsibilities. For the purposes of this policy:

(1) College staff are those people registered on the College's Personnel / Payroll systems.
(2) College students are those people registered to College on the OSS (Oxford Student System) and current members system.
(3) users are people permitted temporary access to the College's public IT facilities.
(4) users are all other people permitted access to the College's IT systems

The definitions of people authorised will be reviewed from time to time, as the College's activities change, in order to include all possible categories of user.

6.1. Staff Responsibilities. All staff (including agency and temporary staff) must agree to written terms and conditions covering the use of IT when they register to use College IT systems. The Academic Office is currently responsible for obtaining a staff user ID. The user ID agreements are currently held by the University's IT Services. Temporary staff accounts will be set to expire at the end of the relevant contract period. All new employees are required to sign their agreement to the terms and conditions in the staff handbook. The staff handbook includes information regarding confidentiality, electronic information security and conditions of employment. All references are checked by individual department heads prior to a new member of staff commencing employment. Access to the College's systems may be withdrawn and College disciplinary procedures may be invoked where a serious or deliberate breach of the policy is discovered.

6.2. Student Responsibilities. In order to use the College IT facilities, students must agree to the terms and conditions. To ensure that all students see and consent to these conditions, students must expressly sign the Acceptable Use and JANET documents. The College's disciplinary procedures, including withdrawal of access to IT systems, may be invoked if students fail to recognise their responsibilities under this policy.

6.3. External User Responsibilities. All external users must be sponsored by a member of the University. The external user must agree in writing to the acceptable use policy and JANET terms and conditions. Records of these agreements are held by IT department. Examples of external users are:

(1) Students from another college;
(2) People teaching on University courses who are not employed by the College (for example a lecturer from another college, teaching in University College);
(3) Staff who have left but have an ongoing working relationship with the College;
(4) External examiners;
(5) Outside researchers collaborating with College academics;
(6) Auditors.

External user accounts will be of limited duration (a maximum of 24 months). Breaches of the terms and conditions may result in suspension of the account as well as possible disciplinary/legal proceedings against the user or sponsor.

7. Communications and Operations Management

7.1. Reporting and Investigating Security Incidents. Staff should report suspected security breaches through their line manager to the IT department.

These incidents will be monitored by the IT department and an appropriate investigation and action plan will be prepared. Within the provisions of the law, the University reserves the right to intercept and monitor communications at any time, that is, in accordance with the Regulation of Investigatory Powers Act, the Telecommunications (Lawful Business Practice), (Interception of Communications) Regulations and any other relevant legislation. Monitoring and recording is carried out routinely as part of systems operation and auditing. Specific interception/monitoring of individual activity shall normally only take place with the express written approval of the Master or IT Fellow, but may be undertaken without any prior notice to the users of College systems.

7.2. Operational Procedures and Responsibilities for Information Systems. The IT department will maintain procedures for the operation (e.g. start up, backup, shut down and change control) of those College Core Systems where risk and impact would be high if such procedures were not carried out correctly. Performance of these systems will be monitored to ensure reliability.

7.3. Protection Against Malicious Software and Hacking. All systems will be protected by a multi-level approach involving firewall, router configuration, e-mail scanning, virus and spy/malware protection on all workstations on the College network. All College workstations will have appropriate anti-virus software installed by the IT department, set up to update anti-virus signatures automatically. Users must not turn this off. Staff and students may use their own PC hardware to connect to the wired and wireless networks. Equipment so used will be subject to security checks and a number of pre-requisites before being allowed to connect. Details of these will be published on the IT department's internal web pages. Network traffic will be monitored for unusual activity.

7.4. Housekeeping. System backups will be performed by the relevant IT support staff in accordance with documented procedures. The procedure will include keeping backups off site in secure storage, via the University Tivoli system. Periodic checks will be made to ensure backup media can be read and files restored. Records of backups will be monitored by IT department. Backups of data are taken on a daily basis for critical systems or less frequently if appropriate. Backups protect electronic information from major loss or failure of system software and hardware. Backups are not designed to guard against accidental deletion or overwriting of individual user data files.

7.5. Management of Network Configuration. The configuration of critical routers, firewalls and other network security devices will be the responsibility of the IT department who will maintain and secure the devices. No IT equipment may be connected to the College network without approval by IT department. The IT department also reserves the right to disconnect and remove equipment that has not been properly approved.

7.6. Exchange of Information with Outside Organisations. Requests by external bodies for the provision of electronic information from internal systems will be referred to the system owner and in some cases the IT department. This includes Data Subject Access Requests made under the auspices of the Data Protection Act 1998. Responses to Data Subject Access Requests in respect of systems owned and operated by IT department will be coordinated by the IT Fellow and IT Manager. Requests for information under the Freedom of Information Act will be referred to the College. All electronic information will be handled in accordance with the Regulations and Policies applying to all users of the University's ICT facilities

7.7. Internet and Email. The use of email and Internet is governed by the College Acceptable Use Policy and Regulations and Policies applying to all users of the University's ICT facilities.

7.8. Software Installation. All software installation on College systems must be in accordance with the University's procedures and relevant copyright legislation.

8. Access Control

8.1. Access Categories. Access to IT facilities will be restricted according to the type of user. College staff, students and some external users may use:

- Standard software (currently installed on machines);
- file stores (if available);
- email, calendar and public folders;
- University Business systems** ;
- internet.

[** These services will not be provided to all external users.]
Guest users may use:

- Standard software (currently installed on machines);
- internet;

8.2. Username and Password Control. Primary access to all the College IT facilities is governed by a network username and password giving access to a set of network services, depending on department and status. The IT department maintains procedures for the issue of and closure of network accounts. Authorisation of access to systems and to the data held by them is the responsibility of both the system owner and IT department. The College aims to minimise the number of accounts required by each individual. The control of network passwords is the responsibility of the IT department. Re-issue of network passwords is through the IT department. System administrator passwords will be issued on the express authority of the IT Manager on a need-to-know basis. Such passwords will be

changed regularly and when authorised system administrator staff leave. For the Novell operating system the following will be enforced:

- network passwords - these must contain a minimum of 6 characters
- network passwords will be subject to enforced periodic change
- accounts will be locked if there are too many failed login attempts

The IT department must be notified by department heads when staff leave and will be responsible for removing their network accounts. Responsibility for retention of any files held by staff that leave lies with their department and should form part of their staff exit procedure. Departments responsible for electronic information assets (as in section 5) will be informed when staff authorised to access those assets leave and will be responsible for controlling access rights to those assets.

8.3. Mobile Computing. The danger to information stored on portable computers (laptops, notebooks, tablets and smartphones) is recognised. The IT department will provide security advice to staff, which follows the central University guidelines. Wireless computer networks potentially introduce new security risks that are the subject of a specific Wireless Security Policy; this should be read in conjunction with this Security Policy.

8.4. Auditing and Monitoring. All use of College IT equipment may be monitored and audited in accordance with the Regulations and Policies applying to all users of the University's ICT facilities. Remote access by third party contractors to maintain and support College's IT systems will be subject to appropriate monitoring and control measures defined by the IT department, including written agreement on electronic information security.

APPENDIX C

Firewall Security Policy

A. Hamilton

1. Introduction

1.1. Scope. This Policy establishes which services are allowed through our current firewall and in which direction these services operate. We also attempt to define whether or not the default is normally open or closed.

1.2. Definitions. A firewall is a system (or network of systems) specially configured to control traffic between two networks. A firewall can range from a simple packet filter, to multiple filters, dedicated proxy servers, logging computers, switches, hubs, routers and dedicated servers. A gateway or bastion host is a secured computer system that provides access to certain applications. It cleans outgoing traffic, restricts incoming traffic and may also hide the internal configuration from the outside.

1.3. Why Use a Firewall?

- Each external connection to the internal network should be secured so that it does not reduce the security of the internal network. The security of the network is only as secure as its weakest link.
- Every enterprise should have a firewall and/or security policy, and connections to external networks should conform to that policy. Normally, this is only possible through some kind of firewall.
- A firewall can help stop confidential information from leaving a network and attackers from entering it.
- It can provide detailed statistics on communication between the networks (for example, who used what service and how often, as well as showing details of performance and bottlenecks).
- It can provide logging and audit trails of communications; the analysis of logs can be used to detect attacks and generate alarms.
- However, a strong firewall doesn't mean that the internal host security is no longer needed - on the contrary, most successful attacks come from insiders!
- Our policy is to take a widely used firewall solution and use it for all external connections.

- Examples of technical threats addressed by firewalls include IP spoofing, ICMP bombing, masquerading and attempts to gain access to weakly configured internal machines.
- Examples of risks reduced by firewalls are attacks from curious and malicious hackers, commercial espionage, accidental disclosure of company data (i.e. customer, employee and corporate data) and denial-of-service attacks.

2. Internet Firewall Policy

2.1. Security Requirements.

2.1.1. *Access Control.* All internet access from the University's network must pass over the situated firewall. The default configuration, unless otherwise specified, is that services are forbidden. All users are allowed to exchange emails in and out through the firewall. IT department users are allowed to use www, ftp, https; others require authorisation.

2.1.2. *Assurance.* Firewall machines are to be installed as sensitive hosts. All unnecessary services are to be stopped. Users should not be able directly to logon to these machines, but only through the IT department's machines. The firewall policy and configuration must be accurately documented. The firewall machines must be subject to regular monitoring and yearly audits. Users and firewall administrators should be aware of their responsibilities and be educated so that they can assume these responsibilities.

2.1.3. *Logging.* Detailed logs must be kept (where possible on a separate server). They should be automatically analysed, with critical errors generating alarms. Logs should be archived for at least six months and up to one year. The non-trivial log entries should be examined daily.

2.1.4. *Availability.* The firewall must offer high availability and fulfil the resilience requirements (including backup/restores functions etc.) Processes exist for the change of management and incident response.

2.2. Required Functionality.

2.2.1. *Outgoing services.* The following services are required from specific internal hosts (e.g. via proxies) to the internet:

- Email, www (http), ftp, telnet, SSH,
- DNS (resolve Internet names),
- News (NNTP),
- NTP (Network Time service),
- ODBC/DSL link information on port 1545,
- Aerohive (WiFi AP) Management connection.

2.2.2. *Incoming Services.* The following Internet services need to be allowed in:

- Email: all users should be able to receive internet email

- News (NNTP)
- Secure Logins via VPN + SSH
- https
- RDP
- University IT Services IP Ranges.

Anyone requiring other internet services will need to ask the IT department for authorisation. Access from the hosts to the internal network follows the same rules as access to internet hosts and should always use VPN.

2.2.3. *Special Services provided to the Internet.* These include:

- www Servers (like meals.univ);
- Bradford Campus Manager (Guest checking);
- Eventually a User ftp Server for special projects / collaboration with other companies;
- Internal Server access for specific remote access by third party companies that maintain internal systems (e.g., Accurate solutions, Kinetics). These are provided a specific location IP and sometimes an assigned port.

2.3. Monitoring. The College IT department will continue to monitor, evaluate, develop and, where applicable, incorporate new rules and checks into the firewall. The College IT department will also monitor the traffic going through the firewall, to identify any threats or misuse of the network.

3. Dissemination of the Policy

The policy will be available to staff and academics through the standard College communications channels, i.e. team briefings and the website.

4. Review Date

This policy will be reviewed on a yearly basis or if and when there are changes made to the network configuration. This will be monitored by the IT department.

5. Glossary

IP Spoofing: This is a technique used to gain unauthorised access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host.

ICMP Bombing: The Internet Control Message Protocol (ICMP) is used by internet routers to notify a host computer when a specified destination is unreachable. An attacker can effectively knock a computer off the internet by bombing it with bogus ICMP messages. (This is similar to a denial-of-service attack).

Masquerading: A masquerade is a type of attack where the attacker pretends to be an authorised user of a system in order to gain access to it or to gain greater privileges than would otherwise be the case. A masquerade may be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through bypassing the authentication mechanism. The attempt may come from within an organisation, for example, from an employee, or from an outside user through some connection to the public network. Weak authentication provides one of the easiest points of entry for a masquerade since it makes it much easier for an attacker to gain access. Once the attacker has been authorised for entry, they may have full access to the organisation's critical data, and (depending on the privilege level they pretend to have) may be able to modify and delete software and data, and make changes to network configuration and routing information.

Denial-of-Service Attack: In the world of computing, a denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, the motives for, and the targets of a DoS attack may vary, it generally consists of efforts to interrupt temporarily or indefinitely, or to suspend services of a host connected to the internet.

[1]The current version of this policy is held on the IT part of the Intranet website. Please check on the Intranet to ensure sure that this printed copy is the latest issue

APPENDIX D

Data Retention Policy

A. Hamilton

1. Introduction

This policy document relates to the requirements on public communications providers to retain data for a fixed period (usually 1 year) during which the relevant authority, as defined by the Regulation of Investigatory Powers Act [RIPA] (2000), may request access to the communications data that is held. This includes the internet which is deemed to be a "public network" and any communications platforms whether or not funded by public bodies. There remains a question of whether or not the College is a Qualifying Internet Service Provider (ISP) and whether or not JANET can be properly regarded as a private network in this context. There is also the competing requirements of the 1998 Data Protection Act that requires that personal data must not be kept for *longer than is necessary*, a vague statement that is generally taken to mean no longer than 60 days. (http://www.oucs.ox.ac.uk/network/security/logging.xml?ID=retention).

The Anti-terrorism, Crime and Security Act (ATCSA) was passed in 2001. This legislation introduced a voluntary code that made it possible for details of every website visited, the transmission of every email sent and every phone call made in the UK to be retained and made available to authorities on request.

Since then ATCSA has been followed by European Union legislation, the Data Retention Directive 2006; this was introduced in the wake of the Madrid train bombings (2004) and the London terror attacks (2005). The Data Retention Directive was implemented in the UK in respect of telephone communications, i.e., fixed telephone lines, and mobile telephones by the Data Retention (EC Directive) Regulations 2007, which together with the ATCSA voluntary code, have now been superseded by the Data Retention (EC Directive) Regulations of 2009. These Regulations extend the range of data to be retained to internet-related data which is defined to include data arising from 'Internet access', 'internet telephone services' and 'Internet e-mail' .

The 2009 Regulations apply to data generated or processed in the UK and specify that the data that must be retained are data necessary to:

(i) trace and identify the source of a communication;
(ii) identify the destination of a communication;
(iii) identify the date, time and duration of a communication; and

(iv) identify the type of communication.

In the words of the 2009 Regulations, this includes data generated or process by means of 'mobile telephony', 'internet access', 'internet email' and 'internet telephony.' It is also necessary to identify the user's communication equipment.

2. Data Retention: Anti-Terrorism, Crime and Security

Traffic Data: Traffic data, for the purposes of data interception and retention is defined in the RIPA as follows.

(1) Any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted.
(2) Any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted.
(3) Any data comprising signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of any communication.
(4) Any data identifying the data or other data as data comprised in or attached to a particular communication, but that expression includes data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored.

Content: Communications Data is defined by RIPA as any of the following:

(i) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;
(ii) any information which includes none of the contents of a communication [apart from any information falling within paragraph (i)] and is about the use made by any person-
  (a) of any telecommunications service; or
  (b) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;
(iii) any information not falling within paragraph (i) or (ii) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a telecommunications service.

An example of the differences between Traffic Data and Content, is as follows.

The Traffic data of an email contains the following: where it has come from and where it has gone to, the User ID of the person sending it (email account) and the server it was sent from. The Content of the email is the message contained in the main body of the email.

3. Differences between Traffic Data and Content (under the RIPA)

Traffic Data: "Traffic data, for the purposes of data interception and retention is defined in RIPA:

(i) Any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted.

(ii) Any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted.

(iii) Any data comprising signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of any communication.

(iv) Any data identifying the data or other data as data comprised in or attached to a particular communication, but that expression includes data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored.

Content: Communications Data is defined by RIPA as any of the following:

(i) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;

(ii) any information which includes none of the contents of a communication [apart from any information falling within paragraph (i)] and is about the use made by any person-
   (a) of any telecommunications service; or
   (b) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;

(iii) any information not falling within paragraph (i) or (ii) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a telecommunications service.

(iv) An example of the differences between Traffic Data and Content, is as follows: The Traffic data of an email contains the following: where it has come from and where it has gone to, the User ID of the person sending it (email account) and the server it was sent from.

The Content of the email is the message contained in the main body of the email.

4. Additions made by the Digital Economy Act 2010

New rules are proposed to deal with the online infringement of copyright, including the copyright and performers rights and penalties for infringement. The amendment of the Communications Act 2003 requires Internet Service Providers (ISPs) to disclose details of customers (in our case students), who repeatedly

infringe copyright, on production of sufficient evidence, with a possible fine of £250,000 for non-compliance. In these cases, it is possible that the University may take most of the brunt, however, as the University tends to refer to colleges as ISPs it could leave us with the requirement to comply. In particular, there could be: (a) the requirement that the ISP blocks access to sites that can allow "substantial" infringement, and (b) employs "temporary suspension" of internet connections for repeat infringers of copyright following warnings from the ISP. Other provisions in the bill include an amendment to the Copyright, Designs and Patents Act 1988 to increase the criminal liability for "making or dealing with infringing articles" and "making, dealing with or using illicit recordings" to a maximum of £50,000, so long as it is done during the course of a business. The UK government is also able to intervene directly to control the use of the UK's domain name space, currently overseen by the independent body Nominet.

5. Issues that relate to Libraries, Universities and WiFi Providers

There has been and will continue to be a debate on the position of Libraries, Universities etc. in the new rights bill. There is evidence to show that most will be considered ISPs; , they could, however, quite easily be looked at as a subscriber to the JANET network or as a communications provider. It seems that currently the O.U.C.S, treat each College and Faculty as an ISP, which under the new act would mean that we would have to hold more in the way of data logs than we currently do. The best reference at this point is the Example-Infringement-Notification document, created by the Department of Business Innovation and Skills (BIS).

6. Conclusions and Policy

Questions remain as to the extent to which the Janet network can be regarded as private. Indeed, as this feeds into the internet which is public system one could argue that College should follow the EC Directive and retain data for the prescribed 1 year. IT Services on the other are recommending a period of 60-day data retention (http://www.oucs.ox.ac.uk/network/security/logging.xml?ID=retention) based on a balance between the data protection and data retention. With this in mind the College is adopting the following action.

1. Update to the Forti-gate firewall, with Acu module and Forti-Analyzer box. 2. Switching on more logging on the Forti-gate firewall (both Normal Traffic and Web Traffic). 3. The addition of the Forti-Analyzer will enable us to keep the required data needed as an ISP for the required amount of time (6 months to 1 Year). It will also allow us to search the data more easily. 4. The extension of the DHCP logging to 1 Year, allowing us to trace dynamically allocated IP addresses to a specific computer (M.A.C.) address. 5. The Installation of the Bradford N.A.C. unit, to keep logs of current students who logon to the network. This will also stop any rogue servers or computers being placed on the network. 6. The

installation of the Bradford client on all Admin and Fellows computers that are owned by the College.

7. Further Refinements

Additional Strategy may yet include the following adjustments.

1. Bradford to be added to the University WiFi network, if the University doesnt do this itself. Currently the WiFi spark equipment logs all data needed, for the Non-JANET networking, however, we need to be sure what is currently logged by the current University WiFi system. 2. Use of data blocking for URL, thus blocking known terrorist websites, blogs, and forums. 3. Blocking of traffic from known terrorist countries, or at least checking relevant links. 4. Checking email addresses or email servers of known terrorist or security risk entities. 5. Creation of more stringent logins for students (encrypted passwords, emails etc.) and Guests (conferences). 6. Installation of VLANs on the network to segment traffic (i.e. Student from Administration etc.) 7. Installation of a singular IDS/IPS system, to act as a double check of the Forti-gate firewall and to act as a 'sticking plaster for security breaches while patches are applied. It would also be valuable if the new equipment in future could prevent data leakage (e.g. by copying data onto an usb stick, if the user is not authorised).
Provisions have been made for 5, 6 and 7 to be carried out over vacations.

Addendum

Malware infections

The increase in serious malware infections like Zeus, may well require us look at better ways of reducing the risks.

The main reasons why a machine can become infected with Malware like Zeus are as follows:

(1) Rogue code (in .jpg picture files, .pdf files)
(2) Links that take the user to infected websites, where any click will download the Malware.
(3) Banners that have become infected with malware, where people then roll over to click on them, infecting their machine.
(4) Counterfeit Anti-spyware/ Anti-Virus programs (downloaded from the internet)
(5) TV streaming sites.

There are many other ways in which a user can become infected by malware. The list below lists how infections can happen through emails

(1) A link in an email sent to the user that then takes the user to an infected website, or downloads an infected file.
(2) An infected .EXE file is sent to the user and they click on and open the file.
(3) An infected .PDF file is sent to the user and they click on and/or open the file.
(4) An infected .JPG file is sent to the user and they click on and/or open the file.

Possible Solution

One solution is to stop of all .EXE, .BAT, .PDF and .JPG traffic coming in via emails. As these are currently the most commonly used file types after .DOC files this could cause problems and irritation to users. It would mean users would have to encrypt or zip these files for them to go through scanning. Another possible route would be to stop connections to certain websites. These would be to specific countries (e.g. Russia and the Eastern Europe) and any known distribution websites.

The Terrorism Trail

There seems to be an increased commonality between terrorist activities and specific countries. Most security firms and governments are starting to look at this as a way of spotting activity patterns.

Possible solution, should one be needed:

(1) Country patterns - Check to see where data are coming from and going to. This would include the websites; IP addresses of particular known servers and countries.
(2) Chatter patterns Check on the data being sent from a particular IP/M.A.C to another IP/M.A.C on a regular basis (that are not known servers or known services)
(3) Emails Check the flow to known email addresses and email servers.
(4) Web sites Ban all known terrorist websites and check for words associated with terrorism in the web data flow (if possible).
(5) Blogs Ban all known terrorist Blog sites and check for words associated with terrorism in the data flow (if possible).
(6) Forums Ban all known terrorist forums and check for words associated with terrorism in the data flow (if possible).
(7) Known terrorism servers (if any) to be blocked and checks made on a regular basis to current college servers for any breaches.

In the above cases we would need to hold more data than the recommendations for data retention. The main data that would need to be held for users, would be: user ID (login), IP, M.A.C, Application. This should be possible through the Forti-gate firewall and IDS/IPS systems.

APPENDIX E

IT Equipment and Software Policy

A. Hamilton

1. Introduction

The College IT department is committed to ensuring that, as far as it is reasonably practicable, the way we provide services to the public and our staff reflects their individual needs and does not discriminate against individuals or groups on the basis of their age, gender, race, disability ,religion/belief or sexual orientation.

Managers are responsible for ensuring that all staff, within their area of responsibility, are aware of the College's policies and that staff adhere to them.

Managers are responsible for ensuring that a system is in place which keeps their staff up to date with new policy changes.

Staff are responsible for ensuring they are familiar with policies, know where to locate the documents on the College's Intranet website, and seek out every opportunity to keep up to date with them

Independent contractors must put forward a person to be responsible for ensuring their staff are aware of the College's policies.

This policy is individual to University College. The College does not accept any liability to any third party that adopts or amends this policy.

2. Machines that can be supplied - 2012 Specification

Lenovo desktop machines currently supplied are of medium specification, with a processor and ram size appropriate for the current operating system.

Desktop

- Lenovo M91 i5 4 Gb of RAM memory
- 23 Lenovo multi-positional TFT screen
- Standard corded usb Lenovo mouse and keyboard.

Laptop

- Lenovo E530 i5 laptop, 15.6 TFT screen.
- Samsung series 5 laptop, 13 TFT screen.

2.1. Software installed on all administration machines as the standard. A current version of Microsoft Office and Microsoft Windows, that is seen as safe (normally not the newest but with at least SP1).

TABLE 1. Software 2012 specification

Microsoft windows 7	7-Zip	SuperAntiSpyware
Microsoft Office	Java	Malwarebytes
Sophos anti-Virus	Filezilla	Spybot
Adobe Reader	Imgburn	Adaware
Sea-monkey	Quicktime	CCleaner
Firefox	Adobe Flash	
Chrome	LogMeIn	

Additional software is then installed, that is specific to each of the departments and the jobs people do. Full IT support is given to these machines in accordance with the SLD.

3. Staff (admin) Home working machines

The software installed on home working machines is similar to that installed on administration machines. However, the specific software needed per department is not installed. Instead, LogMeIn or Remote Desktop are used to access the office work machine from the home working machine. Therefore, additional requirements for the home-working machine are:

- A Remote desktop icon this is setup specifically to connect to a users office computer.
- VPN Cisco anywhere connect software.

RDP (Remote Desktop) is the home-working connection of choice, as it gives a full screen window. RDP access has to be setup both at the firewall and on the specific office machine for security reasons. Full IT support is given to these machines in accordance with the SLD, with the added remote support.

4. Teaching Fellows' Machines

As the teaching Fellows' machines are not really owned by the IT department, but purchased on the Fellows' academic allowance, the setup and support is very spartan. Fellows can purchase any machine/s they choose, but we would always try to steer them into a cost effective and support-efficient way. To this end the following manufacturers are suggested. (The IT staff would look at each Fellow's needs, so that only the machine/s that fit the requirements are suggested for purchase.)

4.1. Standard Suppliers. Orders made through the IT department will usually attract an educational discount from the supplier. Typical suppliers are listed below.

Lenovo laptops and desktops. Models depending on purpose Samsung - laptops / ultras books. Mac - desktops / laptops / ipads. HP - Printers /scanners. Samsung , HTC, Acer (Android) tablets.

IT support is a minimum as the devices are not classified as IT department equipment.

4.2. Standard Software - Fellows' Machines.

(1) Microsoft Office
(2) Adobe Reader
(3) Sophos Anti-virus

Other software could be installed where needed, however a license would need to be purchased or provided and the installation of this software would be on an *ad-hoc* and time permitting basis. We would also add another (admin) user to the machine for emergency purposes only. The actual support of these machines (time frames) is as given in the SLD but if anything major was needed, we would have to carry out this work on an *ad-hoc* basis and when time permits.

5. Mobile Smartphones

The mobile smartphones that the IT department currently support are listed below:

(1) Blackberry Bold or Curve
(2) Apple iPhone
(3) Galaxy S3 mini
(4) HTC Desire C

APPENDIX F

Acceptable Usage Policy

P.E.G. Baird

1. Introduction

The use of the IT network and facilities is ultimately governed by regulations set by the University's Council. The latest version (July 2012) is reproduced below because it is automatically incorporated within this policy document. The College wishes to place particular emphasis on the following.

2. Usage Policy

1. In these regulations, unless the context requires otherwise, 'college' means any college, society, or Permanent Private Hall or any other institution designated by Council by regulation as being permitted to present candidates for matriculation.

2. University IT and network facilities are provided for use in accordance with the following policy set by Council:

(1) The University provides computer facilities and access to its computer networks only for purposes directly connected with the work of the University and the colleges and with the normal academic activities of their members.

(2) Individuals have no right to use university facilities for any other purpose.

(3) The University reserves the right to exercise control over all activities employing its computer facilities, including examining the content of users' data, such as e-mail, where that is necessary:

(a) for the proper regulation of the University's facilities;

(b) in connection with properly authorised investigations in relation to breaches or alleged breaches of provisions in the University's statutes and regulations, including these regulations; or

(c) to meet legal requirements.

(4) Such action will be undertaken only in accordance with these regulations.

3. These regulations govern all use of university IT and network facilities, whether accessed by university property or otherwise.

4. Use is subject at all times to such monitoring as may be necessary for the proper management of the network, or as may be specifically authorised in accordance with these regulations.

5. (1) Persons may make use of university facilities only with proper authorisation.

(2) 'Proper authorisation' in this context means prior authorisation by the appropriate officer, who shall be the Chief Information Officer or his or her nominated deputy in the case of services under the supervision of IT Services, or the nominated college or departmental officer in the case of services provided by a college or department.

(3) Any authorisation is subject to compliance with the University's statutes and regulations, including these regulations, and will be considered to be terminated by any breach or attempted breach of these regulations.

6. (1) Authorisation will be specific to an individual.

(2) Any password, authorisation code, etc. given to a user will be for his or her use only, and must be kept secure and not disclosed to or used by any other person. Exceptions may be made for accounts set up specifically to carry out business functions of the University or a unit within it, but authorisation must be given by the head of the unit.

7. Users are not permitted to use university IT or network facilities for any of the following:

(1) any unlawful activity;

(2) the creation, transmission, storage, downloading, or display of any offensive, obscene, indecent, or menacing images, data, or other material, or any data capable of being resolved into such images or material, except in the case of the use of the facilities for properly supervised research purposes when that use is lawful and when the user has obtained prior written authority for the particular activity from the head of his or her department or the chairman of his or her faculty board (or, if the user is the head of a department or the chairman of a faculty board, from the head of his or her division);

(3) the creation, transmission, or display of material which is designed or likely to harass another person in breach of the University's Code of Practice on Harassment;

(4) the creation or transmission of defamatory material about any individual or organisation;

(5) the sending of any e-mail that does not correctly identify the sender of that e-mail or attempts to disguise the identity of the computer from which it was sent;

(6) the sending of any message appearing to originate from another person, or otherwise attempting to impersonate another person;

(7) the transmission, without proper authorisation, of e-mail to a large number of recipients, unless those recipients have indicated an interest in receiving such e-mail, or the sending or forwarding of e-mail which is intended to encourage the propagation of copies of itself;

(8) the creation or transmission of or access to material in such a way as to infringe a copyright, moral right, trade mark, or other intellectual property right;

(9) private profit, except to the extent authorised under the user's conditions of employment or other agreement with the University or a college; or commercial purposes (including advertising commercial services) without specific authorisation;

(10) gaining or attempting to gain unauthorised access to any facility or service within or outside the University, or making any attempt to disrupt or impair such a service;

(11) the deliberate or reckless undertaking of activities such as may result in any of the following:

(a) the waste of staff effort or network resources, including time on any system accessible via the university network;

(b) the corruption or disruption of other users' data;

(c) the unauthorised access, transmission or negligent loss of data;

(d) the violation of the privacy of other users;

(e) the disruption of the work of other users;

(f) the introduction or transmission of a virus or other malicious software into the network;

(12) activities not directly connected with employment, study, or research in the University or the colleges (excluding reasonable and limited use for social and recreational purposes where not in breach of these regulations or otherwise forbidden) without proper authorisation.

8. Software and computer-readable datasets made available on the university network may be used only subject to the relevant licensing conditions, and, where applicable, to the Code of Conduct published by the Combined Higher Education Software Team ('CHEST').

9. Users shall treat as confidential any information which may become available to them through the use of such facilities and which is not clearly intended for unrestricted dissemination; such information shall not be copied, modified, disseminated, or used either in whole or in part without the permission of the person or body entitled to give it.

10. (1) No user may use IT facilities to hold or process data relating to a living individual save in accordance with the provisions of current data protection legislation (which in most cases will require the prior consent of the individual or individuals whose data are to be processed).

(2) Any person wishing to use IT facilities for such processing is required to inform the University Data Protection Officer in advance and to comply with any guidance given concerning the manner in which the processing may be carried out.

11. Any person responsible for the administration of any university or college computer or network system, or otherwise having access to data on such a system, shall comply with the provisions of the 'Statement of IT Security and Privacy Policy'.

12. Users shall at all times endeavour to comply with policies and guidance issued from time to time by IT Services to assist with the management and efficient use of the University's ICT facilities.

13. Connection of any computer, whether college, departmental, or privately owned, to the university network is subject to the following additional conditions:

(1) (a) Computers connected to the university network may use only network identifiers which follow the University's naming convention, and are registered with IT Services.

(b) The University's Trade Mark and Domain Name Policy specifies, inter alia, that all university activities (other than those within OUP's remit) should be presented within the ox.ac.uk domain. Any exception to this requires authorisation as defined in that Policy.

(2) (a) Owners and administrators of computers connected to the university network are responsible for ensuring their security against unauthorised access, participation in 'denial of service' attacks, etc. In particular they are responsible for ensuring that anti-virus software is installed and regularly updated, and that rules and guidelines on security and anti-virus policy, as issued from time to time by IT Services, are followed.

(b) The University may temporarily bar access to any computer or sub-network that appears to pose a danger to the security or integrity of any system or network, either within or outside Oxford, or which, through a security breach, may bring disrepute to the University.

(3) (a) Providers of any service must take all reasonable steps to ensure that that service does not cause an excessive amount of traffic on the University's internal network or its external network links.

(b) The University may bar access at any time to computers which appear to cause unreasonable consumption of network resources.

(4) (a) Hosting Web pages on computers connected to the university network is permitted subject to the knowledge and consent of the department or college responsible for the local resources, but providers of any such Web pages must endeavour to comply with guidelines published by IT Services or other relevant authorities.

(b) It is not permitted to offer commercial services through Web pages supported through the university network, or to provide 'home-page' facilities for any commercial organisation, except with the permission of the Chief Information Officer (IT Services); this permission may require the payment of a licence fee.

(5) Use of file-sharing technology and participation in distributed file-sharing networks may be subject to additional regulation and restriction in order to prevent excessive use of university network resources, or the use of those resources for purposes unconnected with the University. If a user has any reason to suppose that an application employs peer-to-peer (p2p) or other file-sharing technology, they

should seek the advice of the IT officer responsible for the college or departmental network on which they propose to use the software.

(6) (a) No computer connected to the university network may be used to give any person who is not a member or employee of the University or its colleges access to any network services outside the department or college where that computer is situated.

(b) Certain exceptions may be made, for example, for members of other UK universities, official visitors to a department or college, or those paying a licence fee.

(c) Areas of doubt should be discussed with the Head of IT Services.

(7) Providing external access to University network resources for use as part of any shared activity or project is permitted only if authorised by the IT Committee (ITC), and will be subject to any conditions that it may specify.

(8) If any computer connected to the network or a sub-network does not comply with the requirements of this section, it may be disconnected immediately by the Network Administrator or any other member of staff duly authorised by the head of the college, section or department concerned.

14. (1) If a user is thought to be in breach of any of the University's statutes or regulations, including these regulations, he or she shall be reported to the appropriate officer who may recommend to the appropriate university or college authority that proceedings be instituted under either or both of university and college disciplinary procedures.

(2) Access to facilities may be withdrawn under section 42 of Statute XI pending a determination, or may be made subject to such conditions as the Proctors or the Registrar (as the case may be) shall think proper in the circumstances. Examining Users' Data

15. All staff of an IT facility who are given privileged access to information available through that facility must respect the privacy and security of any information, not clearly intended for unrestricted dissemination, that becomes known to them by any means, deliberate or accidental.

16. (1) System Administrators (i.e. those responsible for the management, operation, or maintenance of computer systems) have the right to access users' files and examine network traffic, but only if necessary in pursuit of their role as System Administrators.

(2) They must endeavour to avoid specifically examining the contents of users' files without proper authorisation.

17. (1) If it is necessary for a System Administrator to inspect the contents of a user's files, the procedure set out in paragraphs (2)-(5) below must be followed.

(2) Normally, the user's permission should be sought.

(3) Should such access be necessary without seeking the user's permission, it should, wherever possible, be approved by an appropriate authority prior to inspection.

(4) If it has not been possible to obtain prior permission, any access should be reported to the user or to an appropriate authority as soon as possible.

(5) For the purposes of these regulations 'appropriate authority' is defined as follows:

(a) in the case of any university-owned system, whether central or departmental: if the files belong to a student member, the Proctors; if the files belong to any member of the University other than a student member, the Registrar or his or her nominee; or, if the files belong to an employee who is not a member of the University, or to a visitor to the University, the head of the department, college, or other unit to which the employee or visitor is responsible, or the head's delegated representative;

(b) in the case of a departmental system, either those named in (a) above, or, in all circumstances, the head of department or his or her delegated representative;

(c) in the case of a college system, the head of the college or his or her delegated representative.

Particular attention is drawn to 13 (5) within the College context. This means that distributed file-sharing is not permitted under any circumstances and this in turn means that file-sharing programs, including but not limited to BitTorrent, Kazaa, eMule, uTorrent, Limewire, Thunder, Vuze and Ares; these should never be used on the College network.

Please be aware that computers on a high bandwidth network such as ours are a prime target and new vulnerabilities are discovered every day. You are encouraged to keep your machines protection software updated and to take great care when opening email attachments. The IT team will advise you on sensible precautions as and when necessary.

3. Sanctions

Breaches to this usage policy can have significant consequences. For junior members this may involve decanal action and withdrawal of network privileges; at the University level it might involve the Proctors who have University-wide powers. All users are of course subject to UK law and inappropriate use of IT facilities including social media can lead to prosecution.

4. Review ofPolicy

This policy area will be updated inline with changes in University regulations pertaining to IT facilities and services; it will be automatically updated inline with College disciplinary procedures and policies issued under the auspices of the IT Fellow.

APPENDIX G

Social Media Policy

Helene Augar

1. Policy Statement

University College will manage and maintain social media sites and platforms as part of its ongoing commitment to engage with previous, current and future students, Fellows, staff and partners about College activities and interests. The College encourages its members and staff to contribute to Univ's online social media presence and social network communities.

2. Scope

Social media encompasses a wide, and constantly changing, variety of electronic communications tools and sites which facilitate digital creation and interaction. This policy is designed to provide Univ members and employees with guidance in using social media to communicate professionally.

3. Aims of using Social Media

Univ members and staff are increasingly using social media and networks personally or for interacting and engaging with current, previous and potential students, staff and visitors. The College is actively exploring how it can attract wider audiences to its website and other electronic communications tools by providing new ways to communicate and it is in the interest of all members and staff to learn about and participate in these new models of engagement.

Social media is about enabling a conversation, but we do not control that conversation. Instead of controlling the content, social media is about engagement and enabling a more dynamic method of web communications.

4. Application of the Policy

If members and staff are creating or contributing to blogs, microblogs, wikis, social networks, or commenting on a post on a site, or if they are using any other kind of social media to communicate and *they are identifiable as a Univ member or employee* then this policy will be applicable.

The way in which social media sites are facilitated makes it even more difficult to differentiate between use in professional and personal capacities than say the

telephone or Internet. It is important to note that this policy applies even to personal use of social media where a member or an employee is identifiable as an employee of University College or the University of Oxford. Following the principles set down in this policy will help them to avoid personal liability for what they write, as well as protecting the privacy, confidentiality and interests of the College. This policy should be read in conjunction with the University Regulations relating to the use of Information Technology Facilities, the University College Employee Handbook and the Univ Website Protocol.

All Fellows, members, staff and students who use social media and can be identified as a Univ member or employee should familiarise themselves with this policy.

In particular,staff or members who:

- Actively manage and maintain a social media presence on behalf of one of the Colleges departments, activities or affiliated projects;
- Contribute comments, reviews and content to social media sites, forums, networks **including those for personal use**. Examples include:
  (1) Maintaining a profile page on one of the social networking sites (such as LinkedIn or Facebook) where the individual is identified as a member or employee of the College or an affiliated project;
  (2) Displaying an @univ.ox.ac.uk e-mail address or listing University College or an affiliated projects as the individuals place of work;
  (3) Joining a Univ network on a social media site;
  (4) Actively running a personal blog that covers aspects of the individuals professional work.
  (5) Communicate Univs participation in any forms of social media, such as when speaking at a conference, giving a presentation, running a training course, taking part in case studies etc.

5. Respect for the Law

- All members and employees of the College have an obligation to obey current laws and regulations, including (but not limited to), trademark, copyright, libel, fair use, equality, data protection and privacy laws. Any queries relating to this should be directed to the College Registrar or Domestic Bursar.
- Individuals should be cautious about endorsing products, services, viewpoints or political positions in a manner which could imply College endorsement.
- Individuals should not post other peoples or organisations materials without explicit permission. This includes photographs, videos and audio recordings.

- The College branding, logos and trademarks should be used on all official College social media sites but should be used with care, following the Colleges brand guidelines which are available from the College Registrar.
- Individuals should not refer, link to or tag individuals on College profiles or pages without their explicit consent.
- Individuals should not publish any personal information on individuals which might contravene data protection laws.
- Individuals should not publish any information or material which discriminates any of the protected characteristics as outlined in the Equality Act 2010.
- It is illegal for companies to create false reviews, for example, using a personal/anonymous profile to fabricate reviews for the College's services or products.
- Individuals should never comment on anything relating to legal matters, litigation or any parties with whom the College is in litigation without the appropriate approval.
- The College's social media accounts or sites are not to be used for the commercial gain of any individual managing or maintaining them.

6. Parent or Guardian Consent for under 18s

Written consent must be sought from parents/guardians before any posts or updates are published with the details and/or photos of anyone under the age of 18.

We cannot control who follows, friends, or links with the College's social media sites and accounts and therefore authors should bear in mind that their audience could, and most likely will, include persons under the age of 18.

7. Social Media Terms and Conditions

Each social media site will have its own terms and conditions for use and it is the responsibility of each individual using the site to follow those terms of use. For example, *Facebook* does not permit multiple personal accounts

8. Confidential or Reserved Information

Care should be taken to avoid revealing information on College or personal sites or tools that might compromise the College or the University in any way.

ndividuals should not post:

- Personal or commercially sensitive information;
- Product or service developments;
- Business strategy;
- Current legal proceedings;
- Offensive, pornographic or indecent content;

- Images of anyone under the age of 18 without the express parental consent;
- Anything that may bring the College into disrepute.

9. Transparency

- If an individual can be identified as a member or employee of the College, their profiles should make it clear that the views they express are their own views and not those of the College. An explicit disclaimer should be used if necessary.
- If the individual is using their own professional or personal social networking contacts to promote a College activity or initiative, they should disclose that they are a member or employee of the College.

10. Appropriate Behaviour

There have been several high profile cases in the media which have resulted in cases being taken to court and resulting in criminal convictions. In many of these cases, the author should have used the social media with greater responsibility and following the points below should help authors to keep within the law:

- Respect the confidentiality of the College, its members and employees.
- Do not write material that you would not be prepared to say in person, and be mindful about posting photographs or comments about colleagues, students or events which others consider to be private.
- Be respectful to others.
- Individuals should be mindful that content they post can reflect on their own professional standards.
- Exercise judgement in deciding which peers, contacts, industry figures, and clients it is prudent to link to, follow, or 'friend, in particular when choosing to combine personal and professional social networks.

11. Dealing with the Media

The Dean is responsible for dealing with the media and therefore members and employees should avoid entering into dialogue with the media and instead direct them to the Dean.

12. Cookies

If embedding social media feeds, content etc into a website, always check for an embed without cookies option and use if available (e.g. YouTube's "Privacy-enhanced Mode").

13. Facilitating and Encouraging Debate

People who are new to using social media can often be apprehensive about the prospect of receiving negative posts or feedback from readers. In practice this is very rare and if the principles contained in this policy are followed, they will continue to be so.

Social media allows healthy debate and interaction. In most cases, social media tools maintained by the College for its projects should be set so that other users can respond to and comment on posts.

It is good practice to review comments before accepting them, but comments should generally only be rejected or deleted if they are:

- Offensive. (If comments contain swear words, is abusive or if they perpetuate discrimination on the basis of any of the protected characteristics as defined in the Equality Act 2010 (age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion and belief; sex; sexual orientation));
- Personal or professional attacks of any kind;
- Irrelevant to the subject matter;
- Direct advertising for a product;
- Spam;
- Phishing;
- Unlawful or advocating illegal activity;
- Infringing on copyrights or trademarks;
- Information that may compromise the safety, security or proceedings of public systems or any criminal or civil investigations.

Criticism or responses mentioning (but not advertising) competitors should be allowed. Negative responses should be responded to in an open and honest manner in order to address the criticism. If an individual is requested to remove a post for any of the above reasons, they should do so immediately. If they do not, the College Registrar will report them to the operators of the social media site.

14. Managing College Accounts

The College requires that sites and accounts are regularly maintained, updated and managed according to this policy. The Web Communications Group will retain an oversight of the College's professional account and any new College accounts must be approved by the IT and Web Fellow to avoid duplication of effort.

Sustainability

It is important that College accounts are sustainable, so that no accounts are inaccessible if a staff member is unable to be contacted or leaves. The following stipulations apply when setting up professional accounts:

- Use generic e-mail addresses (e.g., it@univ.ox.ac.uk or access@univ.ox.ac.uk). If you do not have access to a generic e-mail account, please ask the manager of the account or the IT Manager for assistance.
- All access information (e-mail address, username, password etc) should be shared with the: (i) IT Manager, and (ii) College Registrar
- Privacy settings on browsers should be set so that usernames and passwords for College accounts are not remembered each time the browser is opened.
- If an account is hacked (for example, if a spam direct message is received on Twitter), the College Registrar should be informed immediately so that the account log in information may be reset and any other necessary action is taken to prevent the account being jeopardised.
- A policy for posting, removing and dealing with urgent issues in the event that the account manager is unavailable should be submitted to the Web Communications Group. This does not need to be lengthy or burdensome, but it is essential that another member of College staff can access the account.
- It is strongly advisable for more than one person to be responsible for the day-to-day management of the account to share the commitment required to maintain sites and accounts.
- Staff are strongly encouraged to post details about all College activities and events to the appropriate social media sites. This could include, for example, school visits or alumni dinners.
- The College Registrar will grant permissions to members and staff to manage or administer College social media accounts as required. The College Registrar must be an administrator of all the Colleges professional accounts and can devolve day-to-day management to a relevant officer. This will allow moderation of the sites along with the ability to report on trends in activity where these features are enabled (for example, Facebook allows page activity data to be analysed).

Professionalism

College accounts and sites should reflect the College and University as a whole and adhere to this policy.

College Responses, Misuse and Moderation

The College will encourage 'likes', 'shares' or 're-tweets' of any post and also welcome comments. Under the Univ Website Protocol, any comments or posts made to a College site which require a College response should be reported as soon as possible to the College Registrar who will then arrange for an appropriate response to be posted. Negative feedback or comments can often be neutralised by responding positively and in a timely manner.

If any member or employee of the College observes a College social media site being misused or notices any inappropriate updates or comments posted to the site, they should report the incident to the College Registrar immediately.

The College Registrar will make every effort to remove any libellous, defamatory or inappropriate postings in line with the rules which apply within this policy and at her discretion and/or will respond in a manner which limits any potential damage the reputation of the College. Senders of these comments will be blocked from the account and reported to the operators of the site for offensive behaviour.

We encourage people to post comments in English. If they pose comments or questions in other languages then we may not be able to answer them (if we do, it will be in English) and we might need to remove the comment.

Frequency of posts/updates

Social media sites are a living entity and if they are not maintained with regular posts and updates, people quickly lose interest and stop following or visiting the site. Social media sites vary and there is no absolute rule for how often posts or updates should be made or how much information to include. However, it is important to follow these guidelines:

- Do not overwhelm followers with information;
- But the account or site should show regular activity;
- Professional accounts must not be 'abandoned. If a professional account is no longer required, either a notice should be posted to say it will no longer be updated or the account should be closed.
- If an account is to be closed, the College Registrar and IT and Web Fellow must be informed.

Posting content for Univ

When publishing content, posts or updates to the Colleges social media sites, it is helpful to remember the reasons for doing so. When using Univs social media sites, the aims should be to:

- Promote the Colleges activities;
- Reach a wider, more diverse audience than the website alone;
- Educate, inform and entertain;
- Endorse the teaching and research of Univs Fellows and academic staff;
- Promote debate with a view to finding solutions
- Consider alternative viewpoints;
- Promote activities events.

15. Writing for Social Media

Again, there are no hard and fast rules for writing for social media, but the following principles apply:

- Be concise and brief. Followers and people reading posts/updates on social media sites are not interested in reading lots of text and will skip over posts which are too long.
  - Twitter only allows 140 characters in a Tweet. If appropriate paste in a URL,
  - Twitter will automatically shorten it to allow you the maximum number of characters in your Tweet.
- Use plain English
- Include words which followers or readers might search for in your post
- Be authoritative. If you have done your research (see above) then you should be able to be confident and assertive in your post/update.
- Take care about using internal terms or acronyms
- Photos, videos and other audio visual material can be included or linked to and these can add interest to posts/updates.
- Take care before re-tweeting or re-posting information published by others. It may contain a link to another page with disparaging information about the College or University.
- On Facebook the News Feed regularly reverts to sorting posts what it deems to be Top Stories. Therefore, the Top Story post from a Friend or Liked page may not be the most recent and they could have posted an update on the information contained in the original post. It is best to always check that posts are sorted by Most Recent before sharing a post.

16. Research

- Time should be taken to research topics. The College is full of experts if writing about the College, its history, collections or one of its projects.
- If the individual is not the Colleges expert on a topic then they should make this clear to their readers and write in the first person.
- Do not lie. Aside from the legal implications, readers will only be interested in what is being said if it can be trusted.
- If a mistake is made, the individual should admit it as soon as possible. Once content has been posted, mistakes become a matter of public record. If you have made an error or have posted a personal viewpoint which has been interpreted as fact, it is best to admit your mistake. The original post can be removed but this will not necessarily delete it from the public record because someone else may have already quoted it or re-posted it on their own social media site. When a comment is made online it becomes searchable and can be stored long after it was made so if the author is in any doubt then they should not write the post or comment.

16.1. Adding Value.

- Keep posts helpful and thoughtful.

- Social media should drive users to the College's other content, especially content on the College website. Social media content should not stand alone but should work harmoniously with other content.
- Content should be well written and grammatically correct. Please refer to the University's style guide

17. Staying Safe Online

There has been significant media coverage recently offering guidance on how to stay safe online and there are lots of resources available on the web offering tips on how to protect yourself on the Internet. This is not just for children and young people: often adults can be less safe than younger people as they are less familiar with how social media sites operate. The way in which people use and engage with social media makes it a particularly vulnerable target for unscrupulous people and activity, therefore, although this should not inhibit the use of social media, this should be kept in mind when publishing content.

The following tips can help to keep you safe when using social media:

- Who is this post for? Whenever you are about to post something online, pause and imagine the Master or a Senior Officer of the College reading that post or looking at that photo. If that feels uncomfortable, do not post it.
- Be careful about which photos and videos you share on social media sites. Once a photo is published online, other people may be able to see it and download it.
- Create a strong password. The password should be between 8 and 12 characters and should combine capital and lower case letters, numbers and symbols. The password should not contain any family (or mothers maiden) name. A strong password might be, for example for the Univ Twitter account: Un1v+tW1tt3R (N.B. This is not the real Univ Twitter password!).
- For personal accounts:
  - Use a nickname instead of your real name if you are signing up to a microblogging site like Twitter.
  - Consider setting up a separate, personal email account to use with social media sites, rather than using your work, or even your main personal email. Remember, only connect to people you know.
  - Use the privacy and security settings on social media sites so that only friends and family can see your pages.
  - Then ask friends and family and encourage them to tighten their privacy settings too as they could affect you.
  - Even if your account is locked as private, personal information you have shared with others could still be accessed through their pages.

It is worth asking your friends/followers to apply the same levels of security on their accounts.

– Do not post any personal information publicly online. This includes your address, email address, telephone or mobile phone number. Just one piece of personal information could be used to find out even more. If you want to include your birthday in your profile it is safer not to actually display it publicly. Providing your full date of birth makes you more vulnerable to identity fraud.

18. Support and Guidance

Social Media sites are created to be user friendly and anyone new to using them should be able to navigate their way around fairly easily. The College cannot provide support for using personal accounts.

The College Registrar can provide advice and guidance on using social media for College activities including which sites or forms of media are most appropriate for your project or activity.

19. Additional resources and references

Australian Government: Australian National Botanic Gardens Social Media Policy (17 March 2010)

BBC WebWise Top Ten Online Safety Tips: http://www.bbc.co.uk/webwise/0/21259413

Twitter Guide: http://www.esrc.ac.uk/funding-and-guidance/tools-and-resources/impact-toolkit/tools/interactive-media/twitter/index.aspx

Harvard University Guidelines for Using Social Media (8 January 2012)

McCarthy, L (2012) Crafting a Social Media Policy. Presentation. University Administration Services Conference 2012, University of Oxford

McCarthy, L (2012) Bodleian Libraries Corporate Social Media Policy.

University of Oxford: style guide

Warwick, Claire (5 February 2013) Guardian Higher Education Terror of Tweeting

Rowbottom, J (2012) To Rant, Vent and Converse: Protecting Low Level Digital Speech. The Cambridge Law Journal Vol 71, Issue 02, pp 355-383

20. Updates

This policy may be updated as social media tools and trends change. Any questions or concerns relating to this policy should be directed to:

Ms Helene Augar, College Registrar: helene.augar@univ.ox.ac.uk

Dr Patrick Baird, IT and Web Fellow: patrick.baird@univ.ox.ac.uk

21. Current College Social Media Accounts

Facebook Pages:

- Univ page Maintained by College Registrar and Schools Liaison and Access Officer
- Univ OM page Maintained by Communications Officer
- Univ Library Maintained by College Librarian and Library Assistant
- Univ JCR Maintained by JCR
- Univ WCR Maintained by WCR
- Univ Boat Club Maintained by Boat Club

Facebook Groups:

- Univ Ambassadors Maintained by Schools Liaison and Access Officer and Student Ambassadors

Twitter:

- univoxford Maintained by College Registrar and Communications Officer
- univpercy Maintained by the College Registrar and Porters
- Univ JCR Maintained by JCR

Flickr:

- universitycollegeox

Vimeo:
At http://vimeo.com/universitycollegeox Vimeo

YouTube:
At http://www.youtube.com/universitycollegeox YouTube

Audioboo:
At http://audioboo.fm/univoxford Audioboo

Podcasts:
At http://podcasts.ox.ac.uk/units/university-college,Podcasts

LinkedIn: University College, Oxford

Google+ University College, Oxford

LinkedIn: University College, Oxford

Google+ University College, Oxford

22. Definitions and Glossary

Note: These definitions explain terms used in this Social Media policy but they are not an exhaustive list.

Blog (a shortened version of a 'web log') An easily updatable web page that usually displays entries in reverse chronological order. Blogs offer a regularly updatable format for commentary, descriptions of events or other material (graphics, photos, videos etc.). They often offer facilities for comments to be posted, allowing feedback and facilitating discussion, and readers can subscribe to blogs via RSS feeds.

Blogs are updated and usually hosted on a dedicated blogging website, although they can be made to look like they are hosted on your own site.

'Blog' can be used as a noun or a verb (as in 'to Blog').

Blogger The author of a Blog.

Facebook Groups Facebook allows users to set up groups. Groups can be open or closed (all Facebook Groups for Univ members, students, old members and/or staff should be closed. This means that people can only join by request and those authorised can view posts in the Group page) and are managed by administrators. There should always be more than one administrator for a group.

Facebook Pages Facebook allows users to create pages for businesses, organisations or societies. All pages should be managed by more than one administrator.

Facebook News Page Lists posts from friends, groups and pages the individual has liked.

Friend/Follow Social networking sites often offer users the opportunity to subscribe to other users accounts. What this means may vary by site. On Twitter users follow other users Tweets, whilst on Facebook users Friend each other to connect and share updates.

Microblog A microblog differs from a traditional blog in that its content is smaller or shorter. Major microblogs include Twitter and Tumblr, but other services may have microblogging features.

Profile A personalised page created by an individual or an organisation on a social network site. This typically provides space for a photo, contact details, short pieces of information and a variety of other personal details.

RSS Short for "Really Simple Syndication". RSS allows you to subscribe to content on blogs and other websites and have it delivered to your e-mail inbox via a feed.

Social networks, social network sites and social media Social media or networks include web-based and mobile technologies and sites that allow the exchange and creation of user-generated content. These include blogs, microblogs, content communities such as Vimeo, YouTube and social networking sites such as Facebook.

Tweet A post on Twitter. 'Tweet' can be used as a noun or a verb (as in to 'Tweet'). It is also possible to 'Re-tweet'. This is when you re-post a Tweet written by someone else on Twitter.

Wiki A webpage or set of pages that allows users to work collaboratively, adding and modifying content using a simplified online editor. The best known example is Wikipedia.

APPENDIX H

College Website Protocol

P.E.G. Baird

1. Introduction

The agreed protocol given here is intended to ensure the College website and intranet remain well organised and fit for purpose. It is also intended that these rules will ensure coherence across the site by providing a clear framework with areas of designated responsibilities and transparency in the site management. In general, when major changes are proposed these will be considered first by the Web Communications Group which reports to the General Purposes Committee. Day-to-day commissioning of video and photographic content will remain under the oversight of the Web Fellow and College Registrar. The Communications Group will keep the content and structure of the College website under review; a record of the meetings and any decisions taken will be kept and circulated to members of the Group and to GPC.

2. Website Protocol and Management

(1) All changes to the top (landing page) of the College website must have the ultimate approval of the College Registrar (for accuracy and to ensure compliance with legal regulations) and the Web Fellow.

(2) All changes to second and lower layers of our website will require the authorisation of the relevant Head of Department e.g. Academic Matters the Senior Tutor; Alumni the Development Director; Library the College Librarian; IT matters the IT Fellow; Graduate Matters the Senior Tutor and Dean of Graduates; Welfare Matters the Welfare Dean; College Regulations the Keeper of the Statutes and/or the Dean.

(3) Job vacancies should be authorised by the relevant Head of Department, Senior Officer, the Master and/or the Governing Body, depending upon the type and seniority of the post. Once appropriate authorisation has been granted, job vacancies should be published in the Vacancies section of the website by Web Editors for vacancies which fall within their own department or area of responsibility, or if there is no trained web editor in the department or they are unavailable, by the College Registrar. The College Registrar will monitor the Vacancies section to ensure all adverts

are current, but responsibility for removing vacancies when the application deadlines have expired will remain with the relevant department. It is essential that job vacancies are removed from the website within 48 hours of the application deadline having been reached.

(4) Changes made to these lower layers should be passed to the College Registrar once authorised the relevant Head for a check of overall compliance and style.

(5) A news editor is to be identified to act as the relevant person to sanction additional news items and removal or archiving of old (out-of-date) items.

(6) New sections of the College website must have the approval of the Web Fellow.

(7) Each meeting of the Communications Group will be provided with an up-to-date plan of the website with changes highlighted; the group will be invited to comment and to suggest changes or modifications.

(8) Timing. None of the above regulation is intended to cause significant delays; rather decision-making can be done by email with relevant copies to the Web Fellow and Registrar.

(9) Changes which have consequences for College IT structure and network must be presented to the IT Manager who will if necessary seek approval from the IT Fellow.

(10) Changes affecting the overall website design, for example, the Colour palette, font design etc. must be presented to the Communications group (by email if necessary) for speedy resolution. The College Registrar and Web Fellow will be empowered to make such changes only once the views of the Communications group have been received.

(11) The Web Fellow as Chair of the Communications Group will be empowered to vary the rules and regulations governing the site but only after informing the Group and seeking the views of all members.

(12) The social media aspects of the website will require some policing and here the College Registrar will have overall responsibility; she may delegate some oversight to deputies but, in general, any observations of misuse of the social media or any comments requiring a College response should be reported to the Registrar.

(13) The College Intranet development also falls within the remit of the Communications Group. In the first instance the College Registrar will act as overall editor for the inclusion and removal of items subject to (2) above and subject to ensuring the Communications Group is kept informed

APPENDIX I

WiFi Policy

A. Hamilton

1. Introduction

1.1. Scope. This policy establishes principles and requirements that govern the use of wireless (WiFi) access points (APs) at University College. This Policy applies to all wireless network users (staff, students, faculty and visitors) and equipment operating within the College. The wireless network runs in parallel with the wired College network and aims to satisfy the needs of users who require mobility and flexibility in terms of their working locations.

1.2. Principles. In order to limit the potential security risks that may be associated with wireless network technologies, access to the wireless network must take place in a controlled and secure manner, by liaising with the IT department as and when necessary.

1.3. WiFi Policy. The campus WiFi is the official WiFi system for the College and takes precedence over other WiFi installations within the College estate. The IT department has a duty to ensure correct use and management of devices that both create and connect to the WiFi and that these are maintained.

1.4. Responsibilities. In line with the University Regulations, the WiFi usage is subject to ICTC Regulations and Wireless Regulations. It is also subject to the Colleges and the University's *Acceptable Use Policies.* The College IT department is responsible for authorising, managing and auditing connections to the College campus WiFi network, as well as for the security and integrity of the network. In particular, the College IT department is responsible for managing the campus WiFi network *spectrum*, given the potential for co-channel and adjacent-channel interference from competing wireless network devices within a given location. No extra wireless (AP) installations are allowed without the authorisation of the IT Manager and IT Fellow.

2. Implementation

2.1. Connecting to the Service. Any wireless enabled device (e.g. laptop, or mobile device) using 802.11a/b/g/n standards can be connected to the Wi-Fi network. The name of the WiFi hotspots (SSID) will appear in your list of WiFi

services. The current University-wide connections are OWL and eduroam. The IT department can assist you in setting up WiFi access on your device. Each user is responsible for the set up on their own equipment as the configuration of each manufacturer's device is unique; please refer to the manufacturer's documentation for the relevant connection instructions. No guarantee is provided that you will be able to make a wireless connection. No guarantee is provided that you will be able to access the internet service or third party website you may require.

2.2. Monitoring. The College IT department will continue to monitor, evaluate, develop and, where applicable, incorporate new wireless network technology to the benefit of the College community. The College IT department is responsible for maintaining the availability of the College wireless network spectrum. In order to manage and to monitor the wireless spectrum, and to identify rogue devices and possible misuse of the network, the College will make periodic sweeps of the College's wireless coverage area.

2.3. Security. In view of possible interference from other sources within the 802.11 wireless 2.4GHz frequency range (this is currently in line with the specifications available from the WiFi alliance http://www.wi-fi.org/), the College wireless spectrum should be kept clear of unauthorised transmissions. Any unauthorised wireless devices operating within the College's wireless spectrum will be considered rogue devices. As such, depending upon the configuration, these devices may present a significant security threat and will be subject to removal from the network. It is expressly forbidden to connect any wireless network device or equipment *directly into the wired campus network*. Wherever possible all wireless network traffic over the air should be encrypted. Where this is not possible or due to service considerations not required, it should be clearly stated to the clients that the wireless session is insecure and is potentially open to eavesdropping. As a result of inherent security weaknesses and available hacking tools, use of static WEP encryption keys is discouraged and should in general be considered unsafe. OWL-Unsecured is just that but becomes secured when connected via VPN software using remote access credentials. Eduroam-Unsecured, becomes secured when connected via the University's radius servers using the remote access credentials. UCO-Public-Unsecured, is not secure but traffic is logged. In order to mitigate the clients exposure to external threats, users devices which are used to connect to wireless network must: if possible utilise a personal firewall; run anti-virus software and maintain any virus definition updates; ensure that their operating system is fully patched and running the latest service packs; not run in ad-hoc mode (i.e. peer-to-peer mode) or be made into a hotspot without permission and setup by the IT department. If users of the wireless network are in any doubt as to how to maintain their particular client device, assistance can be gained in the first instance from: wireless networking at http://www.oucs.ox.ac.uk/network/wireless/

3. Breaches of the Policy

Breaches of this Wireless Network Policy will result in immediate action being taken to disconnect any unapproved networking equipment and in the case of deliberate or repeated abuse may be treated as a disciplinary offence.

4. Dissemination of the Policy

The policy will be available to staff and academics through the standard University College communications channels, i.e. team briefings and the website.

5. Review Date

This policy will be reviewed on a yearly basis or if there are any changes in the configuration or WiFi deployment, both (AP) and services. This will be monitored by the IT Department.

6. Reference Documents

University College Security Policy
University College Acceptable Use policy
Oxford University WiFi Usage and regulations.
WiFi Alliance.
London Borough of Hillingdon WiFi acceptable usage policy
NHS Linconshire.

7. Glossary

- Access Point/Wireless (Wi-Fi) Access Point (AP): A device that allows Wi-Fi devices to connect to a wired network.
- Installed Access Point: A non-IT Department installed/managed access point.
- Campus Wi-Fi: The term used to refer to UCO-PUBLIC, OWL or Eduroam wireless networks.
- SSID: Wi-Fi Hotspot Name (the name of a Wi-Fi network that can be seen in the vicinity of another Wi-Fi device).

APPENDIX J

Mobile Device Policy

A. Hamilton

1. Introduction

1.1. Scope. This policy governs the procurement and use of all mobile devices, capable of connecting to the college WiFi or any mobile networks (including 3G) that has been procured by the College and supplied by the IT department.

This policy sets out clear guidelines and responsibilities for managers and staff that use these devices.

In the context of this policy, the term mobile device refers to smartphones, including Blackberry, iPhone and any other mobile devices including tablets that can connect to WiFi.

[Exceptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) an assessment must be conducted and authorised by IT Fellow.]

The Procurement part of this policy does not apply to Teaching Fellows, as items are purchased from their individual academic allowances, although the standard rules of this policy should still be followed.

1.2. Principles. The College IT department recognises that staff should be able to use mobile devices where it is appropriate to do so and subject to privacy considerations.

Mobile devices represent a significant risk to information security and data security. If the appropriate security applications and procedures are not applied they can be a conduit for unauthorised access to the organisations data and IT infrastructure. This can subsequently lead to data leakage and system infection. The College has a requirement to protect its information assets in order to safeguard its users, intellectual property and reputation. This document outlines a set of practices and requirements for the safe use of mobile devices.

2. Mobile Device Policy

Mobile devices provided to staff are for the operational effectiveness and to aid communications. In this instance the IT department has a duty to ensure that the correct use, software and management of mobile devices is maintained.

2.1. Responsibilities. In line with the Colleges rules and regulations with regard to the security of assets, the security of the mobile devices purchased by the College is the responsibility of the assigned user. The assigned user must read and have agreed to abide by this policy.

Standard mobile devices for staff will be acquired via the Domestic Bursary after approval by the individual service managers and in consultation with the IT department. The Domestic Bursary will use the College's approved supplier for standard phones with network (carrier) contracts.

Personal calls made by a mobile device provided by the College should only be used in emergency situations and call time kept to a minimum. In the light of download limits on devices and possible excess charges on particular tariffs, the Domestic Bursary and IT Manager will liaise to ensure that the correct SIM and tariff are procured. Any abuse or extensive use of the mobile device for personal use will be treated as misconduct. In cases where a mobile device is used as a team phone, the manager of the team must take overall responsibility.

2.2. Software. A considerable amount of software is now available for smartphones, in particular for iPhones and android devices. Those issued with smartphones must take responsibility for any additional software that they install and any costs associated with such software, e.g. iTunes. The IT department cannot take responsibility for the effects on the operation of any device unless IT staff have been consulted beforehand.

2.3. Legislation. It is an offence for a person to drive a motor vehicle if they cannot have proper control of the vehicle. A new clause with the Road Vehicles (Construction and Use) Regulations 1986 was added to come into effect from 1st December 2003 covering the use of mobile phones as follows:-

Mobile Phones 110. - (1) No person shall drive a motor vehicle on a road if they are using -

(a) a hand-held mobile telephone; or

(b) a hand-held device of a kind specified in paragraph (4) (a device "similar" to a mobile phone includes a device that can be used for sending or receiving spoken or written messages, sending or receiving still or moving images or providing Internet access, e.g. Blackberry).

New legislation to increase the penalty for using a hand-held phone whilst driving or riding a motorcycle came into force on 27th February 2007.

It is also illegal to supervise a learner when using a hand-held telephone.

Although hands-free telephones are not covered under this Regulation, their use is seen as a distraction and the driver could be prosecuted for not having proper control of a vehicle if the Police witness poor driving while using one.

It is an offence to cause or permit the use of a hand-held mobile phone when driving. It is also an offence to cause or permit a driver not to have proper control of a vehicle.

Staff must not use mobile phones whilst driving (the College does not require it) and it is the responsibility of each member of staff to ensure their own personal safety.

The College will not be responsible for payment of any fines incurred under this Regulation.

3. Procurement

All mobile devices that can be configured to integrate into the main corporate network (location) and or the centralised email system should be secured using the following procedure: 1. The department heads will liaise with the IT department to find the most appropriate device for the user. The make and model will be taken from the current pool of IT supported devices. 2. If the device is not in the current IT support pool as described in the IT Equipment Policy (Appendix E), then time will be given to the IT department to look at whether the new device can be supported and how best to do this. A decision between the IT Manager and IT Fellow will be taken on the inclusion of the new device into the currently supported pool. 3. Once support for the device has been agreed, the head of the department requesting the device will send a note to both the Domestic Bursary and the IT department, effectively signing off the device for use; this will include the reasons for the procurement of the device. 4. The costs of the Smartphone or mobile device (including tablets) will come out of the IT budget - a budget increase will need to be agreed, which will cover the number of smartphones to be made available. The cost of the mobile connection (mobile phone sim) and monthly connection costs will be passed through the Domestic Bursary for sign off. The cost will then be apportioned through the Treasury to the relevant department.

4. Implementation

4.1. Technical Requirements. Devices must use the following Operating Systems: Android 2.2 or later, IOS 4.x or later, or the Blackberry OS.

Devices must store any user-saved passwords in an encrypted password store.

The users must configure their devices with a secure password that complies with the Security Policy (Appendix B). This password must not be the same as any other credentials used within the organisation.

All passwords for devices should be shared with the IT Manager to hold in a secure location.

4.2. Security Aspects. Users must only load data essential to their role onto their mobile device(s).

The assigned user must ensure that their mobile device is protected against unauthorised use. This can be assured by either the use of a PIN/Security code or by locking the keyboard. Full details will be given in the relevant mobile user manual.

The assigned user must not leave their mobile device in unlocked offices.

The assigned user must ensure that their mobile device is left out of sight in locked vehicles.

The assigned user must not lend their mobile device to any person not employed by the College. If a mobile telephone is lent or swapped by users for more than a quick phone call, then the appropriate line manager must be informed.

The assigned user must take appropriate precautions not to reveal sensitive information when making a phone call in public.

When the assigned user leaves the employment of the College, the mobile device must be returned with its charger, user manual and any other parts to the IT department.

Any instance of loss or theft of a mobile device must be reported immediately to the IT department.

Mobile devices in need of repair must be returned to the IT department who will check to see if a repair can be made; if this is not possible or cost-effective then the telephones will be returned to the Domestic Bursary who will return it to the suppliers for repair or replacement as appropriate. It must be noted that manufacturers warranties do not normally cover damage caused by misuse, water or neglect, and that the cost of such repairs could be borne by the assigned user.

Care should be taken when installing third party applications. Please check with the IT department if you are unsure before you install any extra applications.

Mobile device firmware should be kept up to date using the manufacturers website or for installed software, the relevant provider e.g. Apple in the case of iTunes. At a minimum network patches should be checked regularly and applied when available. In the case of tablet devices, these may need to be taken back to the IT department for the work to be carried out. Devices must not be connected to any PC which does not have up-to-date anti-virus software and enabled anti-malware protection. Users must not configure personal email accounts on their devices. They must take particular care to ensure that any College data are not sent through their personal email system.

The IT department reserves the right to perform a full remote wipe to all devices configured for access to College or the University systems (if the device is owned by the College) to ensure protection of the Colleges data.

All devices should be security marked in case the device is lost. Their serial numbers and other identifying information must be recorded by IT centrally. Owners must be aware that even if a lost device is recovered, the data on it may have been copied in the meantime.

Devices should not be "jailbroken", i.e., not have any software/firmware installed which is designed to gain access to any unintended functionality. (**To jailbreak a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorised software.)

4.3. Breaches of Policy. Any investigation of alleged equipment abuse will be properly conducted by line managers (escalating as appropriate) and any consideration of disciplinary action will be instigated in accordance with the College's disciplinary procedures.

4.4. Dissemination of the Policy. The policy will be available to staff through the College communications channels, i.e. team briefings and the website. Staff awareness of this policy and its content will be further supported by inclusion in the local induction to all new staff who may be allocated a device.

4.5. Support and Key Contacts. The IT department will provide procurement information and best practices, support and maintenance for all mobile devices, excluding standard mobile phones. The Colleges mobile phone supplier will provide reports giving usage and costs. The Domestic Bursary will alert managers of any visible misuse for further investigation.

4.6. Review Date. This policy will be reviewed on an annual basis or sooner if there are any changes in legislation concerning the use of mobile telephones; this will be monitored by the IT department.

5. Reference Documents

Department of Transport (2007).
Road Vehicles (Construction and Use) Regulations 1986, Regulation 104.
University College Security Policy (Appendix B).
Data Protection Act (1998).
British Standards BS 7799-1:2005 Information Technology Security.
Techniques Code of Practice for information Security Management.
Kings College London security Policy.
University of Salford Mobile Devices Security Policy.
NHS Central Lancashire.

6. Glossary

SMS Short Message Service - Short text messages that can be sent to a mobile phone.
Person Identifiable Information Person Identifiable Data is defined as any of the following items: Surname, Forename, Initials, Address, Postcode, Date of Birth, National Insurance Number, University Card number.

9 November 2013