Information Technology (IT) Acceptable Use Policy

Applicable to all students, faculty, staff and visitors of Harlaxton College

1. Introduction

The College seeks to promote and facilitate the proper and extensive use of Information Technology in the interests of learning and research. Whilst the tradition of academic freedom will be fully respected, this also requires responsible and legal use of the technologies and facilities made available to students and staff of the College.

This Acceptable Use Policy is intended to provide a framework for such use of Harlaxton College's IT resources. It applies to all computing, telecommunication, and networking facilities provided by the College and should be interpreted such that it has the widest application. This policy encompasses new and developing technologies, as well as those that are older and more established.

Members of the College and all other users of the College's facilities are bound by the provisions of this Acceptable Use Policy. They are also bound by such other policies as are published via the College on its website or in printed form. It is the responsibility of all users of Harlaxton College's IT services to read and understand this policy.

2. Purpose of Use

College IT resources are provided primarily to facilitate a person's essential work as an employee or student or other role within the College. The College's fixed and wireless network facilities are also intended to help enhance the wider experience of students attending the College. No use of any IT service should interfere with another person's duties or studies or any other person's use of IT systems, nor bring the College into disrepute, in any way.

While using College IT facilities in an office, library or classroom, uses for non-work-related purposes, such as personal electronic mail or recreational use of the World Wide Web including social networking sites, are understood to enhance the overall experience of an employee or student but are not an absolute right. Priority to such College-owned facilities must always be granted to those needing facilities for academic or other essential work.

College e-mail addresses and associated College e-mail systems must be used for all official College business, in order to facilitate auditability and institutional record keeping. All staff and students of the College must regularly read their College e-mail.

Commercial work for outside bodies, using centrally managed services, requires explicit permission from the Principal; such use, whether or not authorised, may be liable to charge.

3. Authorisation

In order to use the computing facilities of Harlaxton College a person must first be registered. Registration of all members of staff, faculty and registered students is carried out automatically. Others must apply to IT Services. Registration to use College services implies, and is conditional upon, acceptance of this Acceptable Use Policy, for which a signature of acceptance may be required on joining the College. The lack of a signature does not exempt an individual from any obligation under this policy.

The registration procedure grants authorisation to use the core IT facilities of the College. Following registration, a username, password and e-mail address will be allocated. Authorisation for other services may be requested by application to IT Services.

All individually allocated usernames, passwords and e-mail addresses are for the exclusive use of the individual to whom they are allocated, as are individually allocated security certificates. The user is personally responsible and accountable for all activities carried out under their username. The password associated with a particular personal username must not be divulged to any other person, other than to designated members of IT staff for the purposes of system support. Other facilities are available for situations where staff need to share e-mail. Attempts to access or use any username, e-mail address or certificate, which is not authorised to the user, are prohibited. No one may use, or attempt to use, IT resources allocated to another person, except when explicitly authorised by the provider of those resources.

All users must correctly identify themselves at all times. A user must not masquerade as another, withhold their identity or tamper with audit trails. A user must take all reasonable precautions to protect their resources. In particular, passwords used must adhere to current password policy and practice.

4. Privacy

It should be noted that systems staff, who have appropriate privileges, have the ability, which is occasionally required, to access all files, including electronic mail files, stored on any computer which they manage. It is also occasionally necessary to intercept network traffic. In such circumstances appropriately privileged staff will take all reasonable steps to ensure the privacy of service users. The College fully reserves the right to monitor e-mail, telephone and any other electronically-mediated communications, whether stored or in transit, in line with its rights under the Regulation of Investigatory Powers Act (2000). Reasons for such monitoring may include the need to:

- ensure operational effectiveness of services,
- prevent a breach of the law, this policy, or other College policy,
- investigate a suspected breach of the law, this policy, or other College policy,
- monitor standards.

Access to staff files, including electronic mail files, will not normally be given to another member of staff unless authorised by the Principal, or nominee, who will use their discretion. Such access will normally only be granted in the following circumstances:

- where a breach of the law or a serious breach of this or another College policy is suspected,
- when a documented and lawful request from a law enforcement agency such as the police or security services has been received,
- on request from the relevant Head of Department or Section, where the managers or co-workers of the individual require access to e-mail messages or files, which are records of a College activity, and the individual is unable (e.g. through absence) to provide them.

The College sees student privacy as desirable but not as an absolute right, hence students should not expect to hold or pass information, which they would not wish to be seen by members of staff responsible for their academic work. In addition to when a breach of the law or of this policy is suspected, or when a documented and lawful request from a law enforcement agency such as the police or security services has been received, IT staff are also authorised to release the contents of a student's files, including electronic mail files, when required to by any member of staff who has a direct academic work-based reason for requiring such access.

After a student or member of staff leaves the College, files which are left behind on any computer system owned by the College, including servers, and including electronic mail files, will be considered to be the property of the College. When leaving the College, staff should make arrangements to transfer to colleagues any e-mail or other computer-based information held under their personal account, as this will be closed on their departure.

5. Behaviour

No person shall jeopardise the integrity, performance or reliability of computer equipment, software, data and other stored information. The integrity of the College's computer systems is put at risk if users do not take adequate precautions against malicious software, such as computer virus programs. All users of College IT services must ensure that any computer, for which they have responsibility, and which is attached to the College network, is adequately protected against viruses, through the use of up to date antivirus software (**any exceptions to this must be approved explicitly by IT Services**), and has the latest tested security patches installed. Reasonable care should also be taken to ensure that resource use does not result in a denial of service to others.

Conventional norms of behaviour apply to IT-based media, just as they would apply to more traditional media. Within the College setting, this should also be taken to mean that the tradition of academic freedom will always be respected. The College, as expressed in its Equal Opportunities Policy, is committed to achieving an educational and working environment which provides equality of opportunity, and freedom from discrimination on the grounds of race, religion, sex, class, sexual orientation, age, disability or special need.

Distributing material, which is offensive, obscene or abusive, may be illegal and may also contravene College codes on harassment. Users of College computer systems must make themselves familiar with, and comply with, the College's policies on harassment and bullying.

No user shall interfere or attempt to interfere in any way with information belonging to or material prepared by another user. Similarly, no user shall make unauthorised copies of information belonging to another user. The same conventions of privacy should apply to electronically held information as to that held on traditional media such as paper.

For specific services the College may provide more detailed guidelines, in addition to the policies provided in this Acceptable Use Policy. In particular, users of the College's wireless network must adhere to the detailed advice provided by the Wireless Network Acceptable Use Policy.

Users of services external to the College are expected to abide by any policies, rules and codes of conduct applying to such services. Any breach of such policies, rules and codes of conduct may be regarded as a breach of this Acceptable Use Policy and be dealt with accordingly. This includes social networking sites, blog and wiki services, bookmarking services and any other external services, including those described as Web 2.0 or otherwise. The use of Harlaxton College credentials to gain unauthorised access to the facilities of any other organisation is similarly prohibited.

6. Definitions of Acceptable & Unacceptable Usage

Unacceptable use of College computers and network resources may be summarised as:

- the retention or propagation of material that is offensive, obscene or indecent, except in the course of recognised research or teaching that is permitted under UK and international law; propagation will normally be considered to be a much more serious offence;
- intellectual property rights infringement, including copyright, trademark, patent, design and moral rights, including use internal to the College;
- causing annoyance, inconvenience or needless anxiety to others;
- defamation (genuine scholarly criticism is permitted);
- unsolicited advertising, often referred to as "spamming";
- sending e-mails that purport to come from an individual other than the person actually sending the message using (e.g., a forged address);

- attempts to break into or damage computer systems or data held thereon;
- actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software;
- attempts to access or actions intended to facilitate access to computers for which the individual is not authorised;
- using the College network for unauthenticated access;
- unauthorised resale of College services or information.

These restrictions should be taken to mean, for example, that the following activities will normally be considered to be a breach of this policy (potential exceptions should be discussed with IT Services):

- the downloading, uploading, distribution, or storage of music, video, film, or other material, for which you do not hold a valid licence, or other valid permission from the copyright holder;
- the publication on external websites of unauthorised recordings (e.g. of lectures);
- the distribution or storage by any means of pirated software;
- connecting an unauthorised device to the College network (i.e. one that has not been configured to comply with this policy and any other relevant regulations and guidelines relating to security and acceptable use);
- circumvention of network security and/or access control;
- monitoring or interception of network traffic, without permission;
- probing for the security weaknesses of systems by methods such as port-scanning, without permission;
- associating any device to network Access points, including wireless, for which you are not authorised;
- non-academic activities which generate heavy network traffic, especially those which interfere with others' legitimate use of IT services or which incur financial costs;
- excessive use of resources such as filestores, leading to a denial of service to others, especially when compounded by not responding to requests for action;
- frivolous use of College owned computer labs, especially where such activities interfere with others' legitimate use of IT services;
- opening an unsolicited e-mail attachment, especially if not work or study-related;
- the deliberate viewing and/or printing of pornographic images;
- the passing on of electronic chain mail;
- posting of defamatory comments about staff or students on social networking sites;
- the creation of web based content, portraying official College business without express permission or responsibility;
- the use of College business mailing lists for non-academic purposes;
- the use of CDs, DVDs, and other storage devices for copying unlicensed copyright software, music, etc.;
- the copying of other people's web site, or other, material without the express permission of the copyright holder;
- the use of peer-to-peer and related applications within the College. These include, but are not limited to, Ares, BitTorrent, Direct Connect, Morpheus, KaZaA;
- Plagiarism (i.e. the intentional use of other people's material without attribution).

Other uses may be unacceptable in certain circumstances. In particular, users of the Colleges fixed and wireless network should not provide any services to others via remote access. The installed machine on each network access point must be a workstation only and not provide any server-based services, including, but not limited to, Web server, FTP server, IRC, Streaming Media server, peer-to-peer facilities, or e-mail services.

It should be noted that individuals may be held responsible for the retention of attachment material that they have received, via e-mail that they have read. Similarly, opening an attachment, received via unsolicited e-mail, especially if clearly unrelated to work or study, which leads to widespread virus infection, may result in disciplinary action being taken.

Acceptable uses may include:

- personal e-mail and recreational use of Internet services, as long as these are in keeping with the framework defined in this policy document and do not interfere with one's duties, studies or the work of others;
- advertising via electronic notice boards, intended for this purpose, or via other College approved mechanisms

However such use must not be regarded as an absolute right and may be withdrawn if abused or if the user is subject to a disciplinary procedure.

7. Legal Constraints

Introduction

Any software and/or hard copy of data or information which is not generated by the user personally and which may become available through the use of College computing or communications resources shall not be copied or used without permission of the College or the copyright owner. In particular, it is up to the user to check the terms and conditions of any licence for the use of the software or information and to abide by them. Software and/or information provided by the College may only be used as part of the user's duties as an employee, faculty member or student of the College or for educational purposes. The user must abide by all the licensing agreements for software entered into by the College with other parties, noting that the right to use any such software outside the College will cease when an individual leaves the institution. Any software on a privately owned computer that has been licensed under a College agreement must then be removed from it, as well as any College-owned data, such as documents and spreadsheets. When a computer ceases to be owned by the College, all data and software must be removed from it, in accordance with the College's policies and contractual obligations.

In the case of private work and other personal use of computing facilities, the College will not accept any liability for loss, damage, injury or expense that may result.

The user must comply with all relevant legislation and legal precedent, including the provisions of the following Acts of Parliament, or any re-enactment thereof:

- Copyright, Designs and Patents Act 1988;
- Malicious Communications Act 1988;
- Computer Misuse Act 1990;
- Criminal Justice and Public Order Act 1994;
- Trade Marks Act 1994;
- Data Protection Act 1998;
- Human Rights Act 1998;
- Regulation of Investigatory Powers Act 2000;
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000;
- Communications Act 2003;
- Criminal Justice and Immigration Act 2008.

See below for a summary of the main points. Further advice should be obtained through IT Services in the first instance.

Copyright, Designs and Patents Act 1988

This Act, together with a number of Statutory Instruments that have amended and extended it, controls copyright law. It makes it an offence to copy all, or a substantial part, which can be a quite small portion, of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, sound, moving images, TV broadcasts and many other media.

Malicious Communications Act 1988

Under this Act it is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person. Additionally under the Telecommunications Act 1984 it is a similar offence to send a telephone message, which is indecent, offensive, or threatening.

Computer Misuse Act 1990

This Act makes it an offence

- to erase or amend data or programs without authority;
- to obtain unauthorised access to a computer;
- to "eavesdrop" on a computer;
- to make unauthorised use of computer time or facilities;
- maliciously to corrupt or erase data or programs;
- to deny access to authorised users.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:-

- use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- display any writing, sign or other visible representation which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Trade Marks Act 1994

This Act provides protection for Registered Trade Marks, which can be any symbol (words or images) or even shapes of objects that are associated with a particular set of goods or services. Anyone who uses a Registered Trade Mark without permission can expose themselves to litigation. This can also arise from the use of a Mark that is confusingly similar to an existing Mark.

Data Protection Act 1998

The College has a comprehensive Data Protection Policy, of which the following statement is a summary.

Harlaxton College is committed to a policy of protecting the rights and privacy of individuals (includes students, faculty, staff and others) in accordance with the Data Protection Act. The College needs to process certain information about its staff, faculty, students and other individuals it has dealings with for administrative purposes (e.g. to recruit and pay staff, to administer programmes of study, to record progress, to agree awards, to collect fees,

and to comply with legal obligations to government). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

The policy applies to all staff, faculty and students of the College. Any breach of the Data Protection Act 1998 or the College Data Protection Policy is considered to be an offence and in that event, Harlaxton College's disciplinary procedures will apply. As a matter of good practice, other agencies and individuals working with the College, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that staff who deal with external agencies will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy.

Human Rights Act 1998

This act does not set out to deal with any particular mischief or address specifically any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the context of the College, important human rights to be aware of include:

- the right to a fair trial;
- the right to respect for private and family life, home and correspondence;
- freedom of thought, conscience and religion;
- freedom of expression;
- freedom of assembly;
- prohibition of discrimination;
- the right to education.

These rights are not absolute. The College, together with all users of its IT services, is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations which arise from other relevant legislation.

Regulation of Investigatory Powers Act 2000

The Act states that it is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic (including telephone) communications is permitted, in order to:

- establish the facts;
- ascertain compliance with regulatory or self-regulatory practices or procedures;
- demonstrate standards, which are or ought to be achieved by persons using the system;
- investigate or detect unauthorised use of the communications system;
- prevent or detect crime or in the interests of national security;
- ensure the effective operation of the system.

Monitoring but not recording is also permissible in order to:

- ascertain whether the communication is business or personal;
- protect staff.

The College reserves the right to monitor e-mail, telephone, and any other communications in line with its rights under this act. The Lawful Business Practice Regulations allow exceptions to the basic principle of non-interception as stated in the RIPA, and allows interception without consent in certain instances.

Communications Act 2003

This act makes it illegal to dishonestly obtain electronic communication services, such as e-mail and the World Wide Web.

Criminal Justice and Immigration Act 2008

This act increased the penalties for publishing an obscene article. It also introduced fines for data protection contraventions when organisations *'knew or ought to have known that there was a risk that the contravention would occur, and that such a contravention would be of a kind likely to cause substantial distress or damage, but failed to take reasonable steps to prevent the contravention*.'

8. College Discipline

Staff, faculty or students who break this Acceptable Use Policy will find themselves subject to the College's disciplinary procedures. In particular, students should familiarise themselves with the College's Student Handbook and its policies on student conduct and discipline.

The Principal, Vice Principal, Dean of Students or, in the case of a staff member, an individual's departmental manager may take such disciplinary action. Individuals may also be subject to criminal proceedings. The College reserves its right to take legal action against individuals who cause it to be involved in legal proceedings as a result of their violation of licensing agreements and/or other contraventions of this policy.

9. Policy Supervision and Advice

The responsibility for the supervision of this Acceptable Use Policy is delegated to IT Services. They will liaise with the Principal, Vice Principal, Dean of Students, the College Librarian, the Copyright Officer and Heads of Department, as required.

Any suspected breach of this policy should be reported to a member of IT Services staff who will then take the appropriate action within the College's disciplinary framework, in conjunction with other relevant areas of the College. IT Services staff will also take action when infringements are detected in the course of their normal duties. Actions will include, where relevant, immediate removal from online information systems of material that is believed to infringe the law. The College reserves the right to audit and/or suspend without notice any account pending any enquiry. Where necessary, this will include the interception of electronically mediated communications.

This policy is not exhaustive and inevitably new social and technical developments will lead to further uses, which are not fully covered. In the first instance students should address questions concerning what is acceptable to their faculty supervisor; faculty and staff should initially contact their Head of Department or the Principal. Where there is any doubt the matter should be raised with IT Services, whose staff will ensure that all such questions are dealt with at the appropriate level within the College.