IMPORTANT:
THIS DOCUMENT IS UNDER REVIEW

Once finalised and approved, the Code of Practice will be replaced by an Acceptable use of IT policy.

Codes of Practice for IT Users

(Staff & Students)

Codes of Practice

Code of Practice
Telephone, E-Mail and Internet Usage(Staff)

Introduction

The ability of staff to use external e-mail and to access the Internet provides new opportunities for the College as it facilitates the gathering of information and communication with fellow employees, customers and other contacts. However, Internet and e-mail access opens up the College to new risks and liabilities. It is therefore essential that staff read these guidelines and make themselves aware of the potential liabilities involved in using e-mail and the Internet. Staff should also be aware that the usage of any college equipment may be monitored in accordance with section 8 of the IT Security Policy.

1. General Points

1.1 Use of e-mail and the Internet is primarily for work-related purposes.

1.2 The College may monitor any aspects of its telephone and computer system that are made available to staff, and may also monitor, intercept and/or record any communications made, including telephones, e-mail or Internet communications. The College will ensure compliance in line with the Regulation of Investigatory Powers (RIP) Act 2000, and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. In addition, the College wishes to inform staff that Closed Circuit Television (CCTV) is in operation for the protection of staff and students.

1.3 The college network is a private network and includes all IT equipment connected to it. All staff have the responsibility for ensuring that only college owned and installed IT equipment is used within college premises, with the exception of WiFi devices. If staff wish to use equipment owned by them it must first be tested and configured by the ICT support team.

1.4 Telephone, computers, e-mail and online texting accounts are the property of the College and are designed to assist in the performance of your work. Staff should, therefore, have no expectation of privacy in any e-mail sent or received, whether it is of a business or personal nature.

1.5 It is inappropriate use of the Internet, email and other electronic communication tools for staff to access, download or transmit any material which might reasonably be considered to be obscene, abusive, sexist, racist or defamatory. Staff should be aware that such material may also be contained in jokes sent by e-mail. Such misuse of electronic systems will be considered as misconduct and will, in certain circumstances, be treated by the College as gross misconduct. The College reserves the right to use the content of any employee electronic correspondence in any disciplinary process.

1.6 Use of peer-to-peer programs such as Lime Wire or Bit Torrent or download accelerators are prohibited under any circumstances.

1.7 You are the custodian of the college equipment. Care must be taken at all times to ensure the security of the equipment, software, data and passwords.

1.8 At the termination of your employment with the college, or in the case of secondment or long term sickness you will be required to surrender all college IT and telephony equipment. The data files/emails residing on all such equipment belong to the college. All efforts will be made to provide you with copies of these files if it is deemed not to be prejudicial to the college.

1.9 Whilst driving on college business:

Mobile phones should be switched off whilst driving.

If you need to make an outgoing call or pick up messages, pull over to a safe place, and use the phone whilst safely parked

Use the voicemail or message service to monitor incoming calls.

1.10 Instant electronic messages (such as Moodle Mobile texting) should only be sent during College hours (7.30am – 9.30pm) and are to be used for important, course related alerts only.

2. Use of e-mail

2.1 E-mails should be drafted with care. Due to the informal nature of e-mail, it is easy to forget that it is a permanent form of written communication and that material can be recovered even when it is deleted from your computer.

2.2 Staff should not make derogatory remarks in e-mails about employees, students, competitors or any other person. Any written derogatory remark may constitute libel.

2.3 Try not to create e-mail congestion by sending trivial messages or unnecessarily copying e-mails. Staff should regularly delete unnecessary e-mails to prevent over-burdening the system.

2.4 Make hard copies of e-mails which you need to retain for record keeping purposes.

2.5 Staff may want to obtain e-mail confirmation of receipt of important messages. You should be aware that this is not always possible and may depend on the external system receiving your message. If in doubt, ask ICT Services to confirm receipt of important messages.

2.6 Reasonable private use of e-mail is permitted but should not interfere with your work. The contents of personal e-mails must comply with the restrictions set out in these guidelines. Excessive private use of the e-mail system during working hours may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct.

2.7 By sending e-mails on the College's system, you are consenting to the processing of any personal data contained in that e-mail and are explicitly consenting to the processing of any sensitive personal data contained in that e-mail. If you do not wish the College to process such data you should communicate it by other means.

2.8 The use of the 'All Staff' e-mail account is restricted to business purposes only. If any member of staff wishes to communicate to all college staff for a personal reason then a draft of the email must be submitted to the Director of ICT who will publish it on your behalf if it is deemed appropriate.

2.9 Any e-mails sent outside the College will be accompanied by the College's standard disclaimer notice which currently contains the following statement:-

> "The information or opinions in this message (including any attachments) are those of the author and are not necessarily those of Hertford Regional College,

which disclaims responsibility for loss or damage arising from its use to the maximum extent permitted by law. E-mail messages sometimes go astray. If you have received this message in error, we'd be grateful if you would notify the originator immediately and delete the message without copying, altering or disclosing its contents. E-mails to or from Hertford Regional College may be monitored by the College in accordance with its current policy"

3. Use of the Internet

3.1 Reasonable private use of the Internet is permitted but should be kept to a minimum and should not interfere with your work. Excessive private access to the Internet during working hours may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct.

3.2 The sites accessed by staff must comply with the restrictions set out in these guidelines. Accessing inappropriate sites may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct.

3.3 The College do not police the use of external Web 2.0 and Social Networking web sites such as MySpace, Facebook and Blogger. However, if such sites are used inappropriately - e.g. to defame any member of staff or student, or to publish offensive imagery – disciplinary procedures may be invoked.

4. Copyright and downloading

4.1 Copyright applies to all text, pictures, video and sound, including those sent by e-mail or on the Internet. Files containing such copyright protected material may be downloaded, but not forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate.

4.2 Copyrighted software must never be downloaded. Such copyrighted software includes screen-savers.

4.3 Excessive downloading of bit-mapped images and multimedia files is to be avoided wherever possible.

4.5 College staff should not import non-text files or unknown messages on to the College's system without having them scanned for viruses. If you have not been properly trained to scan for viruses, do not import such items at all.

4.6 College staff must never engage in political discussions through outside newsgroups using the College's computer system.

5. General computer usage

5.1 You are responsible for safeguarding your password for the system. For reasons of security, your individual password should not be printed, stored on-line or given to others. User password rights given to staff should not give rise to an expectation of privacy.

5.2 Your ability to connect to other computer systems through the network does not imply a right to connect to those systems or to make use of those systems unless authorised to do so. You should not alter or copy a file belonging to another user without first obtaining permission from the creator of the file.

6. ICT Services

6.1 The ICT Services Section is there to assist you. If you require any information or help about the use or set up of your computer you should contact the ICT Helpdesk on x3000.

7. Code of Practice Awareness and Disciplinary Procedures

7.1 Failure of an individual member of staff to comply with this Code of Practice may lead to the instigation of the relevant disciplinary procedures and, in certain circumstances, legal action.

Code of Practice

Acceptable Use of Information Technology (IT) Facilities (Students)

If you use any College IT Facility you are automatically agreeing to comply with the terms of this Code of Practice.

1. Use of IT facilities, such as the network, computers, printers and the facilities associated with them e.g. software, data, email, internet, bulletin boards, data bases must be for College work, or other **authorised** use only. No 'private' work is permitted.

2. You are permitted to use the college IT equipment in accordance with any local conditions pertaining to that room or area. IT equipment not owned or installed by the college must not, under any circumstance, be connected to the college network.

3. All files created or stored by you on College IT facilities may, in the instance of suspected wrong doing, be subjected to inspection by College IT Technical Staff. Where evidence is found of misuse or of the illegal use of material they will be subject to removal and deletion.

4. You must comply with any local rules in force applicable to IT facilities provided by the College e.g. in Libraries and ILT Centres.

5. Specifically you must not:-

a) disclose to others your login name/password combination(s) or access, or attempt to access, computers at the College or elsewhere for which permission has not been granted

b) eat or drink in any IT facility

c) use or produce materials or resources to facilitate unauthorised corruption, changes, malfunction or access to any College or external IT facilities.

d) knowingly introduce a real, or hoax virus onto College IT systems

e) display, store, print or transmit images or text which could be considered offensive e.g. material of a sexual, pornographic, paedophilic, sexist, racist, libellous, threatening, defamatory or terrorist nature, or likely to bring the College into disrepute.

f) forge email signatures and/or headers, initiate and/or forward ‘chain’ or ‘junk’ or ‘harassing’ mail.

g) play unauthorised games, gamble or use unauthorised ‘chat-rooms’.

h) use, download, copy, store or supply copyright materials including software and retrieved data other than with the permission of the Copyright holder or under the terms of the license held by the College.

i) use a mobile phone to make voice calls in classrooms and other learning areas, e.g. Learning Centres. Mobile phones must be set to *silent* in all learning areas. The use of SMS/ MMS messaging in classrooms is prohibited without prior tutor authorisation.

6. The College cannot police the student use of external Web 2.0 and Social Networking web sites such as MySpace, Facebook and Blogger. However, if such sites are used inappropriately - e.g. to defame any member of staff or another student, or to access or publish offensive imagery – College disciplinary procedures may be invoked. Each college IT centre or room has its own rules regarding access to such sites – you need to ensure that you are aware of these local rules when using these centres.

7. When holding data on computers about living individuals, you must register that data and its uses, and treat it as required by the Data Protection Act 1998.

8. Whilst the College takes appropriate security measures against unauthorised access to, alteration, disclosure, destruction or accidental loss of personal and other data, it cannot and does not give any warranties or undertakings to you about security, confidentiality or integrity of data, personal or other. Make sure that you back-up your files!

Breaking these conditions may lead to College disciplinary procedures being invoked, with penalties which could include suspension from the use of College IT facilities for extended periods. Serious cases may lead to expulsion from the College and may involve civil or criminal action being taken against the user.

Code of Practice
Use of Software

1. Introduction

1.1 Hertford Regional College supports the aims of the Federation Against Software Theft (FAST) and is committed to the principle of full software compliance.

2. Use of Software

2.1 The College has licensed copies of computer software from a variety of providers. Licensed and registered copies of software programs have been placed on computers within the College and appropriate backup copies made in accordance with the licensing agreements. No other copies of this software or its documentation can be made without the express written consent of the software publisher. All software purchases, or systems installations must be authorised by the Director of ICT. Central inventories of all College software assets shall be maintained. Details of these assets will be recorded on procurement and on disposal. On disposal, all software media shall be rendered non re-usable i.e. broken or cut

2.2 The College will provide copies of legally acquired software to meet all legitimate needs in a timely fashion and in sufficient quantities for all of our computers. The use of software obtained from any other source presents security and legal threats to the College, and such use is strictly prohibited, without prior authorisation of the Director of ICT.

2.3 The College provides standard screensavers for all users.

2.4 In some cases, the license agreement for a particular software program may permit an additional copy to be placed on a portable computer or home computer for business purposes. Staff and/or students will not make such additional copies of software or documentation for the software without the approval of ICT Services.

2.5 The unauthorised duplication of copyrighted software or documentation is a violation of the law and is contrary to established Codes of Conduct for College staff and/or students. Staff and/or students who make, acquire, or use unauthorised copies of

computer software or documentation will be subject to disciplinary procedures, in line with College policy, including potential termination of employment or studies.

2.6 The College reserves the right to protect its reputation and its investment in computer software by enforcing strong internal controls to prevent the making or use of unauthorised copies of software. These controls include frequent and periodic audits of software use, announced and unannounced audits of College computers to assure compliance, and the immediate removal of any software found on College computers for which a valid license or proof of license cannot be determined. Disciplinary action may be instituted in the event of an employee or student's violation of this policy.

Code of Practice

Virus Protection and Firewall Policy

1. Introduction

1.1 To facilitate learning, teaching and administration the College provides staff, students with access to the internet via a connection to an Internet Service Provider (ISP) . One disadvantage of this is that others from outside the College may attempt to obtain unauthorised access to the College network (a process known as hacking), or may deliberately introduce a virus onto the network potentially causing severe disruption to College business. There is also a similar risk from internal hacking or virus introduction (whether deliberate or accidental). Therefore to preserve the integrity of our systems and the confidentiality of our data, we must have controlled access to the College network, and the College network shall be provided with maximum protection against virus attack.

1.2 A firewall shall be placed between College systems and the internet ensuring that access is provided only to those who are authorised. In the case of College systems holding very sensitive data, separate controls may also be required to prevent internal hacking.

1.3 All access to the internet shall be through our ISP. Any computers with modems within the College shall be strictly limited and prior approval from the Director of ICT is required.
Proprietary virus protection software shall be installed on all workstations and servers. This will be regularly updated to both prevent the introduction of viruses from external sources and internally via external storage media e.g. floppy/Zip discs

2. Virus Protection

2.1 Every College computer (servers, workstations, laptops, and other devices e.g. Palm Tops) will have standard College virus protection software installed on commissioning by ICT services.

2.2 Staff and students are not allowed to connect personal workstations, or other equipment, to the College network without prior authorization from ICT Services. The workstation will routinely be checked for potential virus threats

2.3 Portable storage media e.g. floppy discs, CD ROM's, shall not be used on College computers without prior checking for viruses.

3. Firewall

3.1 The overall purpose of the firewall is based on the following.

a) The prevention of unwanted traffic on the insecure external network getting access to the secure private network.

b) The separation of those applications that need to gain access to the secure private network from computers that require maximum protection e.g. E-Mail and Internet.

c) Prohibiting access to those who are not expressly permitted provides a more precise control than permitting access to those who are not expressly prohibited.

3.2 To meet the security challenge posed by the internet and hackers the College adopts the following approach on the firewall:-

(i) To filter out use of undesirable internet based material, we will implement a web filtering procedure which complies with internationally recognised standards.

(ii) Additionally we will block any specific addresses identified by College staff and students, with authorisation of the Director of ICT.

(iii) We will block TelNet, Chat lines and internet relay chat as a matter of normal practice and any other service as may be deemed necessary to preserve security or bandwidth.

Code of Practice

PHYSICAL SECURITY OF IT SYSTEMS

1. Introduction

1.1 It is just as important to maintain the physical security of software and hardware as it is to ensure the security of information contained within the College's ICT systems. Loss of computers, file servers or storage media can have a significant damaging effect on learning, teaching, and administration, through loss of data and in the cost of replacing the hardware. Theft of hardware can also result in data falling into the hands of those not entitled to receive it, hence the loss of intellectual property and, in the case of personal data, the possibility of a court case through failure to ensure the security of that data under the Data Protection Act 1998.

2. Security of Premises

2.1 While it is difficult to make premises in a College environment completely secure, buildings and some offices are now equipped with keypad locks which provide a level of protection against opportunist intruders, so long as they are used intelligently by those who have a right of access.

2.2 In order to reduce the risk of theft, the following rules should be followed:

a) offices or other rooms which house valuable equipment should not be left unattended with the door unlocked, or (on the ground floor) with windows open;

b) when entering a locked building the door should be closed securely behind you and you should not allow access to anyone who tries to 'tail-gate' behind you;

c) keep an eye open for anyone who appears to be loitering in the vicinity of a locked door, challenge them and report any suspicions to Receptionist who will contact the Duty Principal.

d) where buildings/offices are secured by keypad locks, do not give away details of PIN/keypad numbers;

e) valuable equipment or equipment storing valuable data should not be located in a vulnerable location such as just inside the window of a ground floor office or near a fire escape; curtains and blinds should be closed at night and equipment which can be seen from the outside should be covered.

3. Security of Equipment

3.1 In order to ensure that computing equipment itself is secure:

(a) All computer equipment with a value of more than £500 will be clearly marked as property of Hertford Regional College, security tagged and recorded on a central inventory. This will be done as soon as possible after the installation and set-up of the equipment;

(b) ICT Services will carry out a risk assessment in relation to the cost of replacing the equipment and the value of the data stored on it in order to determine what additional security measures need to be taken, such as marking, cable restraint, lock-down fixtures, alarms, and arrange fitting as soon as possible.

(c) ICT Services will dispose of any computer packaging as quickly and as discretely as possible in order not to advertise the arrival of new equipment.

3.2 For college equipment used off-site such as a laptop PC:

(a) All reasonable steps must be taken to ensure the security of the item. It must not be left in any location that is deemed to present a risk of theft or damage such as leaving the item in the boot of your car overnight.

(b) Any equipment required to be taken off-site that is not deemed to be portable and not allocated specifically to you must have the agreement of ICT before the equipment is moved.

4. Security of Data

4.1 All master copies of software will be held in a central secure storage area.

4.2 Any media containing data which has been backed up will be held securely ie. in a locked container, drawer or cupboard, and placed in a location commensurate with ensuring business continuity ie. away from the area where that data is normally processed.

4.3 Before disposal of computing equipment we will ensure that any data held on the hard disk is destroyed by an approved method.

Code of Practice

Access to Data on College Computerised Administration Systems

1. Introduction

1.1 Access to the applications, data and computer services associated with the College Computerised Administration Systems (Student Record, Finance Record, Personnel and Payroll Databases) will be controlled on the basis of business requirements to prevent unauthorised access to College applications and data.

1.2 Authorisation to access shall be determined by the Director of ICT in conjunction with the relevant System Access Manager.

1.3 The System Administrator will install and maintain software applications on the relevant system, be responsible for operational system security and data backup.

2. Software Applications Management

2.1 Software applications that can access data held on College Computerised Administration Systems shall only be installed with the authority of the relevant System Access Manager or Director of ICT.

2.2 The System Administrator will install and maintain software applications on the relevant system.

2.3 The System Administrator will maintain change control procedures to minimise the corruption of the systems. These include only accepting changes submitted by authorised personnel, applying upgrades and changes according to the suppliers instructions, ensuring system documentation is updated for each change, maintaining relevant version control for all software updates and minimising downtime and business disruption.

2.4 The facility to connect remotely to systems shall be authorised by the System Access Manager. Connections by remote systems and users (e.g. software maintenance contractors) shall be set up by the System Administrator. Modems shall be turned off by default and only enabled for sessions under the control of the System Administrator.

2.5 System Administrators shall maintain an access log and an audit trail of security events that is reviewed at regular intervals.

3. User Access Management

3.1 The System Access Manager shall determine that the level of access granted to a user is appropriate for the job role and consistent with the College IT Security policy.

3.2 Users with access to sensitive data will be required to sign undertakings that they understand the conditions of access.

3.3 Users with high privileges for special purposes (e.g. DBA) will be assigned a different user identity for privilege and normal business use.

3.4 When users leave the College their access rights will be removed.

3.5 When employees change jobs within the College their access rights will be reviewed and changed as necessary.

3.6 A periodical check will be made for redundant user identities and they will be removed.

3.7 System Administrators shall ensure that passwords shall not be visible at logon and be stored on the system in an encrypted form. Line managers shall apply for an individual user identity and password for all of their relevant staff. Passwords shall be generated by the System Administrator and conveyed to the user in a secure manner. System Administrators shall enforce annual changes of passwords. For users who have write access to college data systems the change of password will be once per term.

4. User Responsibilities

4.1 Users shall not attempt to gain access to applications, data or computer services that they do not have authorisation to access.

4.2 Users should at all times abide by the requirements of confidentiality set out in the Data Protection Act 1998.

4.3 Users shall maintain the confidentiality of passwords at all times. Users should not divulge their own passwords or log in someone with it, without the express permission of their line manager.

4.4 Passwords shall not be included in any automated logon procedures.

4.5 Users with more than one user identity shall use the appropriate one for each specific session.

4.6 Active sessions shall be terminated when finished and not left open by default for convenience.

4.7 Equipment shall be left in a secure status at the end of the working day by a controlled shutdown and power off.

4.8 Users shall report, as soon as possible, any suspected security incident to their line manager who should inform the System Access Manager.

Code of Practice
Review of IT Security

1. Process

1.1 Regular reviews will be carried out to ensure compliance with the overall Security Policy and Codes of Practice. The reviews will include ICT systems and providers, information and data owners, users and management.

1.2 All software resident on every workstation in the College will be audited using a proprietary software auditing tool. A reconciliation against licences held will be periodically undertaken. Any software without a current licence will be removed.

1.3 Regular tests will be carried out on both the firewall and network as a whole to expose potential weaknesses in terms of both virus attack and hacking.

1.4 All Codes of Practice for staff and students will be reviewed to ensure that they are fit for purpose

1.5 Any security breach will be subject to an investigation by a team comprising of the Director of IT, Technical Manager, MIS Manager. This team will report their findings to the SMT including any recommendations for preventing further security breaches.