Exeter College

Information communication technology (ICT) and computer use policy

1. Introduction

IT communications are a key part of the running of the college, and so it is crucial that both Exeter College and its employees adhere to certain standards to protect all parties. It must be remembered at all times that our IT systems and associated facilities are provided principally for purposes directly connected with the work of the College. We aim to take a fair and consistent approach to IT usage among staff, and this policy sets out our rules on what we would deem to be inappropriate use of ICT facilities. It also covers the use of portable equipment, system security, personal use, computer viruses and monitoring.

This policy is not contractual but sets out our current rules and procedures for ICT use.

2. University of Oxford IT policy

Exeter College has subscribed fully to the Oxford University computer usage rules and etiquette, which also cover the use of email and the internet. These rules apply equally to College employees as to all members of the College and University.

A full listing of all the computer usage rules and etiquette can be found at: http://www.ict.ox.ac.uk/oxford/rules/

In particular, attention is drawn to:

- University Policy on Data Protection
- Trade Mark and Domain Name Policy
- University Policy on Security of Information
- Conditions for Connection to Centrally Provided IT Infrastructure

The statute document “Regulations relating to the use of Information Technology facilities” can be found at: http://www.admin.ox.ac.uk/statutes/regulations/196-052.html

3. System security

You should keep any personal passwords confidential and take all reasonable precautions to prevent unauthorised access to the data stored on your machine and on our network. When leaving your machine unattended, lock the screen (“windows key + L”), or log off or power-off, to prevent unauthorised users using your machine in your absence. On leaving your workplace, please ensure that the computer equipment is physically secure from theft, for example by locking the office door or by use of a security cable.

Your passwords should not be disclosed to anyone. You should also ensure that you do not write your passwords down anywhere where they could be easily retrieved by someone else. Passwords may from time to time be reset, computer access withdrawn, or login accounts disabled, especially when someone leaves our employment.

You should never use another person's login account. In the same way, you should not permit any other person to transmit, download, copy, forward or store material using your email address or password.

Be aware when using ICT facilities that your display may be read by other people, including those overlooking you while at work.

You are required to use our computer equipment responsibly, and not to use or modify it in a way that would interfere with, disrupt or prevent anyone else legitimately using these resources.

Ensure you are aware of the access/modification rights of the network drives you use and remember this when saving confidential data, to make certain that only the right people are able to view and edit the files saved. Unauthorised access to data or programs belonging to Exeter College, including attempts to access or modify and intent to access or modify data or programs, will be considered a disciplinary and potentially criminal offence in accordance with the Computer Misuse Act 1990.

Any licence agreement that accompanies software packages should be strictly adhered to. Do not take any unauthorised copies of software for use within the office or outside.

Work protected by copyright must not be downloaded, copied or sent via the Internet or email. Likewise, do not publish or distribute copyright material without due permission from the copyright holder.

4. Portable equipment and remote working

Portable equipment owned by the College may include laptop computers, blackberries, mobile telephones with email capability, etc.

Computer equipment should not be removed from the College without the prior approval of your Head of Department or the Computing Systems Manager. It is particularly emphasised that you must follow agreed back-up procedures to protect any information that you create on any portable device.

When working away from your normal place of work (e.g. travelling, working from home or from a different venue), there are increased ICT security measures that should be adhered to:

- check the location and direction of your display to ensure confidential information is out of view of others
- ensure that data printed is collected and stored securely
- ensure that any systems containing college data are password protected (in the case of computers) or PIN protected (in the case of mobile telephones)

If you are issued with a cellular network ‘dongle’ to enable you to access the Internet while away from your normal workplace, please note that the cost of Internet access can be very high; this is therefore to be used for essential business purposes only, especially if abroad.

If an item of portable equipment is lost or damaged due to an act of negligence, the individual responsible will be expected to fully explain the loss or damage to the satisfaction of the College and may be asked to meet a proportion of the loss or damage, up to and including the full sum involved. These cases will be considered on an individual basis, and it is expected will involve the supervising Head of Department and/or the Bursar, and the Computing Systems Manager.

5. Email

Our email facilities are intended to promote effective and speedy communication on work-related matters. On occasions it will be quicker to action an issue by telephone or face-to-face contact, rather than via protracted email chains of communication. Employees are expected to decide which is the optimum channel of communication to complete their tasks quickly and effectively.

Remember that emails are merely another form of communication. In some instances, they may be the only contact that a recipient has with Exeter College. The style, appearance and content of the email will therefore contribute to the image that is portrayed of the College. Emails are often considered an informal means of communication, but our normal standards of presentation and content equally apply. This includes correct spelling and punctuation, and completing the subject field for each email as appropriate.

When sending messages via email, the content and language used must be professional, concise and directed only to those on a 'need to know' basis. General messages to a wide group should only be used where necessary. Long email trails should be not sent unless absolutely necessary. Messages should only be marked as ‘urgent’ if they warrant immediate action. Read receipts and requests to acknowledge acceptance of an email further add to email traffic and should not be used unless absolutely necessary. Remember, verbal face-to-face contact is another effective means of communication and develops our internal working relationships.

Email is an insecure medium and confidential or sensitive information should where possible be transferred by another means. If email must be used, confidential or sensitive information should not be sent within a message body, but only by use of encrypted attachments, for which the key or password is not included in the same message.

Messages sent by email can give rise to legal action against us. Claims of defamation, or breach of confidentiality or contract could arise from a misuse of the system. Emails should therefore be treated like any other form of correspondence and, where necessary, hard copies retained. Do not make any statements in an email that could intentionally or unintentionally create a binding contract, or make a negligent statement. You should not transmit, copy or forward to third parties any emails sent to you by others without their permission.

Emails, however confidential or damaging, may have to be disclosed to third parties and messages are disclosable in any legal action commenced against us relevant to the issues set out in the email. Even deleted emails may still be recoverable and are regarded as legitimate forms of evidence in court.

If your line of work requires the regular use of email, then you should ensure that an appropriate message is sent automatically to senders if you are away from your place of work for more than one working day. Unless your level of seniority demands it or you are specifically requested to do so, emails are not expected to be read and actioned when you are on any form of leave.

Should you receive an email message that has been wrongly delivered to your email address, you should notify the sender of the message by redirecting the message to that person. If the message contains confidential information, you must not disclose or use that confidential information.

The email system should not be used for spreading gossip or sending nuisance mail, for personal gain or in breach of any of our employment policies on issues such as harassment or bullying. Sending unwanted, abusive, sexist, racist or defamatory emails can constitute harassment and will be treated as a serious disciplinary issue.

Take care before sending or viewing material that you believe may be of a hurtful, suggestive or harassing nature. Remember that it is the view of the recipient of the material that determines whether it is inappropriate, even if the recipient was not the original addressee.

Should you receive an email that contravenes this policy, the email should be brought to the attention of your Head of Department or line manager immediately.

6. Internet use

The vast amount of data that can be found on the Internet can be a useful resource, and its use may be integral to your role. Having access to the Internet demands a level of trust and responsibility, as the websites visited will record your computer system's IP address. In general, it is expected that only fully legal and reputable websites should be used in the course of your work.

You must not use the College systems to access websites offering illegal services or content.

7. Personal use of our IT systems

Reasonable personal use of the email system is acceptable, but it should be clearly understood that while we do not routinely monitor messages, we do reserve the right to monitor and to access any incoming or outgoing messages. Be aware that your messages may be read by other people and do not email anything of a strictly private or confidential nature.

You may use the Internet for viewing non-work-related sites only if this has been agreed in advance with your Head of Department. However, the loading, sending or viewing of the following non-exhaustive list is deemed to be unacceptable and may lead to disciplinary action, including dismissal as a possible outcome:

- pornographic material
- non-licensed material
- suggestive, obscene or offensive material

Furthermore, our systems may not be used for any of the following:

- gambling
- promoting non-business related religious, charitable or political material with the intention to solicit (unless authorised)
- sending or participating in junk mail, spam mail or chain letters
- bringing our name into disrepute, e.g. via social networking websites

This list is not exhaustive, but indicates the sort of usage that we would consider to be unacceptable and that may lead to disciplinary action, including dismissal as a possible outcome.

8. System monitoring

Internet, email and computer usage is continually monitored as part of our ICT operations, providing protection against computer viruses, for ongoing maintenance of the system and when investigating faults.

Internet monitoring and the retrieval of the content of any messages may be employed for the purposes of monitoring whether the use of the system is legitimate, to find lost messages, to retrieve messages lost due to computer failure, to assist in the investigations of wrongful acts, or to comply with any legal obligation.

9. Computer viruses

Unknown files or messages must never be introduced into the system without first being checked for viruses. ALL incoming material should be checked for viruses, whether loaded manually (e.g. from CDs or memory sticks) or transmitted from an external source such as the Internet. Any problems relating to viruses should be reported immediately to your Head of Department or line manager, or directly to the Computing Systems Manager.

Be wary of opening emails from sources you do not know; this is how many viruses are introduced and they could easily spread throughout our systems. Do not respond to junk mail or send out mass warnings regarding new email viruses. Also, please do not forward or respond to chain letter emails. Be particularly careful about opening attachments. Should you open any attachments that produce strange or unexpected results, contact the Computing Department immediately.

10. Implementation, monitoring and review of this policy

This policy will take effect from 1 September 2011. The Governing Body of the College has overall responsibility for implementing and monitoring this policy, which will be reviewed on a regular basis (at least annually) following its implementation and additionally whenever there are relevant changes to our working practices.

Any queries or comments about this policy should be addressed to the HR Officer.

Any breach of this policy will be treated as a disciplinary issue and dealt with through our disciplinary procedure.