Rules for network access at Pembroke College, Oxford

The College makes it a condition of attachment to the network and remaining attached to the network that the following rules are accepted and observed.

You must read, sign, and return this form to the IT Systems Manager before you can be connected.

(a) You have read and understood the University leaflets and College rules: Rules and Guidelines, Usernames and Passwords, Network Etiquette, About OUCS, and Pembroke College IT/Computing Rules and that you will obey and adhere to those rules and guidelines.

Explanatory note: Please realise that the misuse described in the guidelines as ‘giving your password to someone else, or being otherwise careless with it’ means in addition to its literal interpretation that either not setting a password or setting an easily guessed password can be taken by College or the University to be a breach of the rules.

(b) You agree not to operate a network service without permission of the Dean (advised by the IT Systems Manager).

Explanatory note: One (but not the only) way in which a computer can be ‘hacked’ into is if it allows people other than the owner to connect to it, for instance by running a service such as ftp, WWW, mail, dialin. If there is an academic reason why you need to run a service then contact the IT Systems Manager first to discuss technical details of what you propose. The IT Systems Manager will then contact the Dean who will determine whether such a service can be operated from your own machine. This does not stop you using telnet, ftp, X and so on to connect to your machine; if you wish to allow others to access your machine via the network in any way then contact the College IT Systems Manager before allowing any access. If you wish to have a personal web page use your herald web space, which has the advantage of enhanced security and is available at all times. If you construct a personal web page you should ensure it does not infringe copyright or contain untrue, libellous or slanderous comments.

(c) You agree to run up-to-date Anti-virus software on your computer. If you do not have one you can use the College Anti-Virus Software. This will require you to uninstall any existing Anti-virus software

Explanatory Note: This will be the first thing you do when your computer has been connected to the network. If, at a later date, your machine if found to be without current Anti-virus software your computer will be disconnected from the college network and you will have to pay an additional connection fee to be reconnected.

Installation details can be obtained from the IT Office.

(d) You agree that in the event of an allegation of computer misuse involving your computer, the College IT Systems Manager may, with the permission of the Dean or Master, copy any hard drives attached to your computer. You agree to allow the IT Systems Manager to have immediate physical access to and control of your computer or hard drive in order to make copies.

Explanatory note: In the event of your computer being misused, almost the only way to 'prove' that you had nothing to do with the misuse may be from logs and other files on your computer. It is therefore important that there is a clone copy of any hard drives from the moment misuse is detected. A clone copy of a hard drive is an exact copy of the contents of a hard drive, including existing files and the remains of deleted files. In the event of a serious incident of computer misuse involving a personal computer of a member of College which is attached to the College network, the IT Systems Manager will, with the Dean or Master’s permission, immediately attempt to make two clone copies of a suspect hard drive, one copy of which is sealed and deposited in the College safe until the incident is resolved, the other of which is kept by the IT Systems Manager for test purposes. The original is returned to you. In general terms, this copying procedure will be attempted if there is the possibility that civil liability or a criminal offence is associated with your computer. You will be able to observe the copying procedure whether it is in your room or elsewhere. In order to help you and to help College determine if your computer has been misused and by whom, we have established a Computer Emergency Response Procedure which the College will try to implement but it is possible that in a really serious incident, matters may be taken out of College hands by the Police.
Computer Emergency Response Procedure

The IT Systems Manager will attempt to make the clone copies without the computer owner having an opportunity to alter files. The response procedure will be:

(1) OUCS advise IT Systems Manager of problem or IT Systems Manager detects problem.
(2) IT Systems Manager contacts Computing Fellow and Dean, Bursar or Master. Dean or Master authorises intervention.
(3) The first contact with whoever controls the computer should be a request to make clone copies – copying should be attempted immediately and the computer owner should not, if possible, be left alone with the computer before copies are made.
(4) IT Systems Manager attempts to make clone copies without moving the computer, otherwise the computer may need to be temporarily moved and secured until copies can be made.
(5) Assuming clone copies have been made, the computer is dealt with to prevent continuation of the problem and to allow the owner to continue with academic work. However, pending resolution of the incident, no network access to the College Ethernet is allowed.
(6) When the incident has been dealt with, the two clone drives are reformatted; the owner of the original drive can be present if they wish.

(e) You agree to inform the College IT Systems Manager if you change or add a new operating system to your computer.

(f) You understand that your connection is linked to the MAC address of your computer. If you wish to connect any device with another Ethernet card (and MAC address), you must inform the IT Systems Manager. Changing the MAC address will automatically disable your computer.

(g) You agree that the network connection is for one device only – you agree not to attempt to connect multiple devices with the intention of network access.

Explanatory note: this means no
- Wireless networking devices (apple air port stations etc.)
- Games Consoles (PS2, game cube, Xbox etc.)
- Routing devices ( PC’s with more than one network card, Hubs/Switches etc.)

(i) You agree not to participation in distributed file-sharing networks.

Explanatory note: This means no windows file sharing or programs like Kazaa and LimeWire. The University will automatically disconnect any peer to peer computer activity and will expect the college to take action against.

WARNING

Please also appreciate that computer misuse can lead to penalties ranging from being denied a personal connection to the College network, to being expelled. Civil or even criminal sanctions may also arise from outside College.

I, the undersigned, have read, understood and hereby agree to be bound by the College’s Rules for network access and any amended rules issued from time to time on behalf of the College.

I hereby authorise the College to have complete and unrestricted access to my personal computer in the event that the Dean or Master considers there to have been any misuse of College facilities or a serious breach of these Rules.

Signed:…………………………………………… Date: ……………………………