Rules for network access at St John's 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.

(a) You have read and understood the University IT Rules Regulations and policies applying to use of University ICT (and that you will obey and adhere to those rules and guidelines. They are available online at https://www.it.ox.ac.uk/rules

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 College's IT Officers)

Explanatory note *One (but not the only) way in which a computer can be 'hacked' into is if it is allowing people* **other than the owner** *to connect to it, for instance by running a* **service** *such as sshd, ftpd, WWW, or a mail server. If there is an academic reason why you need to run a service then contact one of the College's IT Officers first to discuss technical details of what you propose and then contact the Dean who will determine whether such a service can be operated from your own machine. This does not stop* you *using ssh, ftp, X and so on to connect from* your *machine; if you wish to allow yourself or* others *to access your machine via the network in any way then contact the College's IT Officers before allowing any access. If you wish to have a personal web page this can be put on an IT Services server, 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, libelous or slanderous comments.*

(c) You agree in the event of an allegation of computer misuse involving your computer, the College's IT Officers may with the permission of the Dean or President, copy any hard drives attached to your computer. You agree to allow the College's IT Officers 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, a St John's College IT Officer will, only with the Dean or President's permission, immediately attempt to make two clone copies of a suspect hard drive, one copy of which is sealed and deposited with the College solicitor until the incident is resolved, the other of which is kept by the Senior IT Officer 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 College's IT Officers will attempt to make the clone copies without the computer owner having an opportunity to alter files. The response procedure will be:

(1) IT Services advise College IT Officers of problem or IT Officer detects problem.
(2) A College IT Officer contacts Dean or President who authorise intervention.
(3) The first contact with whoever controls the computer should be a request 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 Officers attempt 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
(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.

(d) You agree to inform the College's IT Officers if you change or add a new operating system to your computer.

(e) You agree not to run a personal wired or wireless router.

Explanatory note *Running a personal router can introduce security vulnerabilities to the network and if badly configured a router can also cause operational problems and stop parts of the network and college wireless system functioning correctly.*

WARNING

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