Last updated: June 2017

St Cross College

IT Rules

These rules apply to all use of the computing and network equipment in all St Cross College buildings, and they specify what is considered to be unacceptable behaviour and misuse, as well as what may infringe licence terms or may be otherwise illegal. All use of computing facilities is explicitly governed not only by the College rules but also by the University rules as given on the following web page:

http://www.it.ox.ac.uk/rules

The College regards computer misuse as a serious matter which may warrant disciplinary proceedings including fines. Offenders who infringe any of these regulations will be reported to the Dean and in some cases to the Proctors, and will be prevented from using the College computing facilities for a period of time dependent on the severity of the misuse. Misuse of computing and network facilities and unacceptable behaviour include (but are not limited to) the following:

1. Using someone else's username with or without their consent, or generating messages which appear to originate from another person or otherwise attempting to impersonate someone else;
2. Attempting to gain unauthorised access to any facility, account or software, or disregarding the privacy of other people's files;
3. Giving your password(s) to someone else or being otherwise careless with it;
4. Sending messages which are abusive or a nuisance or otherwise distressing (the College and University regulations on Harassment apply);
5. Sending chain mail or hoax virus alerts, or sending unsolicited mass mailings to other users outside of official mailing lists which you are personally responsible for;
6. Software piracy, including infringement of software licences or copyright provisions;
7. The use of peer-to-peer software and/or of any other bandwidth-intensive network communication software is only permitted with the prior approval of the College IT Manager. The use of Skype is permitted only where the University Regulations pertaining to Skype are adhered to as detailed on the following web page:
   http://www.oucs.ox.ac.uk/network/voip/skype.xml
8. Trying to interfere with someone else's use of the facilities or disregarding computer and network etiquette;
9. Using the facilities for commercial gain or any illegal activities;
10. Physically damaging or otherwise interfering with the facilities including deliberately changing hardware, firmware and software set-ups;
11. Using any personal wireless network equipment in any College building, except where explicitly authorised by the College IT Manager in advance. This includes all wireless routers, wireless access points (including airstations), wireless sharing devices and wireless network cards except those that are factory-built into a laptop. The College runs its own wireless networks, which are part of the larger Oxford Wireless LANs. Connections to these networks are permitted, subject to the University's regulations for wireless networking available on the following web page:
    http://www.oucs.ox.ac.uk/network/wireless/rules/

Last updated: June 2017

St Cross Computer Rooms and College Network Rules

i. Unauthorised persons are not permitted to use the facilities or to enter the Computer Rooms;
ii. Smoking, eating or drinking are not permitted in the Computer Rooms at any time;
iii. No material that may cause offence is to be accessed, viewed, stored or printed on the computer equipment, e.g. pornography. Any such breaches will be reported to the Dean for disciplinary action.
iv. All personal computers connected to the wired College network must be up to date with security patches and anti-virus software. The Sophos anti-virus software must be used, unless explicit dispensation from this rule is given by the College IT Manager. All computers must be checked and made secure with the help of by one of the St Cross IT Officers before they can be connected to the College network.
v. Only the IP addresses dynamically allocated to each student for their individual room may be used for connection to the network in College rooms; no other IP addresses, whether with or without others' consent, may be used in substitution for any dynamically allocated IP address(es) for a given student's computers.
vi. All students using the College network must bring their laptops in for updating of the security settings by the College IT Officers at the start of every academic year on the dates advertised each Michaelmas Term.