

## Acceptable Use Policy for Wadham IT

### General Rules

1. All individuals wishing to make use of Wadham College IT facilities must abide by this document. Wadham IT facilities include networking, shared IT facilities such as the computer room, and college-owned IT equipment allocated to an individual user.
2. All users of College IT facilities must abide by the terms & conditions of all relevant UK legislation, ICTC Regulations<sup>[1]</sup>, the JANET Acceptable Use Policy<sup>[2]</sup>, and any additional conditions required by OUCS. Clarification should be sought from the IT manager if users are unclear as to the position towards any service, application or activity. *Members of the University should note that computer misuse is regarded as a serious matter which may warrant disciplinary action.* Many of the rules specified here for Wadham IT facilities simply restate requirements for connection to the Oxford University network; please note that many of these rules are much more restrictive than would be expected for an ordinary domestic ISP.
3. Access to IT equipment and resources is provided for bona fide use and it is expected that all users (and any PCs or devices they own) will behave in a considerate and socially acceptable manner. It is forbidden to enumerate or access devices or services to which the user has no legitimate need, to access or circumvent network devices or policies, to intercept network traffic, or to hide or disguise the user's identity (or imitate another user's identity).
4. Users are not permitted to "extend or amend" network or service coverage, nor provide it to others. Wireless Access Points, Powerline Ethernet, and connections between the college network and any other network are forbidden (except where installed by Wadham IT for infrastructure purposes). Use of network(ed) devices such as switches, routers [which must not have wireless capabilities], games consoles or hosting of any servers/services must be approved by the IT Manager. Users found to break this rule will be reported to the Dean who will treat the matter as a breach of College discipline.
5. The network is provided primarily for academic purposes. The use of peer to peer (p2p) software is permitted but bandwidth utilisation is monitored. Excessive use may lead to a warning, and if that advice is not followed the breach will be reported to the Dean who will treat the matter as a breach of College discipline. The network must not be used to violate copyright. If copyright violation notices are received through IT Services, the associated costs will be recovered from those responsible, and the breach will also be reported to the Dean who will treat the matter as a breach of College discipline. Internet telephony (VoIP) must comply with IT Services guidelines and Skype can only be used on the College network if it is configured as required by IT Services.
6. Users must ensure that their computers are maintained in a secure fashion. This includes keeping the operating system and applications updated as necessary. Antivirus software must be installed and kept up to date on those platforms that require it.

### Security and Privacy Issues

7. Users should note that Wadham IT undertakes various measures to manage the network. These activities are undertaken from the point of view of the network; they do not involve examining files on your computer itself. These include:
  - 7.1 statistical monitoring and some analysis of network traffic, to assess the utilisation of the network and note possible problems, as well as to enforce elements of this AUP (e.g. 4 and 5 above)
  - 7.2 periodic unannounced vulnerability testing of PCs, to ensure that as far as possible the network does not contain computers with known security issues that could pose a threat to other users of the network

**8 (This policy is in place until an expected update of the university ICTC regulations, and will be reviewed then).**

Where Wadham IT staff have potential access to a user's private data held on college-owned IT equipment, they will not access that data without the user's explicit consent, except under specific rules below. When users' consent to access private data is sought, it must be given explicitly, and the user must explicitly state that there is no data to be accessed which is potentially infringing on the privacy of third parties. Data may be impounded while permission to access it is sought.

- 8.1 A relevant college officer makes the case that this access is necessary in pursuit of college policy;
  - 8.2 That case is approved by the Warden;
  - 8.3 In the event that the Warden is absent or involved as either the "user" or the "relevant college officer", the Sub-Warden may approve; in the event of the absence or involvement of both, the case must be approved by at least three college officers apart from the college officer making the case for access.
  - 8.4 If possible, the data will be accessed only in the physical presence of the approving officer(s).
  - 8.5 All involved will make every endeavour to ensure that, as far as possible, access is only to material relevant to the specific case made, and particular attention is paid to avoid accessing data held on third parties.
  - 8.6 These guidelines attempt to follow the ICTC regulations Sections 15-17 and applicable statutes; in the event of changes to the rules they will be reviewed.
- 9 In the event that Wadham IT have concerns about the security or use of a computer on the network, access to the network may be blocked and will not be restored until those concerns have been allayed.
- 10 If you are concerned that your privacy may have been breached contrary to this AUP, you should speak in the first instance to either the Fellow Computer Officer or the Warden.
- 11 Wadham IT may install administration accounts on college-owned computers in order to upgrade or audit installed software or amend the configuration. Where there is a user with sole use of such a computer, the user will be notified of such access, which will never involve the inspection of private data.
- 12 If you are concerned about the privacy of data held on your computer, Wadham IT will be happy to advise on security measures to take. However, two particular points are worthy of emphasis:
- 12.1 Email is not an intrinsically secure or private form of communication. Emails should contain no information you would not be happy to send on a postcard; more secure information, if sent by email, should be encrypted.
  - 12.2 The security of any information held on networked computers can never be guaranteed. Data which is particularly sensitive should not be held unencrypted on a networked computer; encryption, and perhaps even physically separate storage in a physically secure location, will be necessary for the most sensitive data. Again, Wadham IT will be happy to advise if notified of especially sensitive information.

#### References

- [1] <http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml>
- [2] <https://community.ja.net/library/acceptable-use-policy>