IT Acceptable Use Policy

Introduction

This document establishes the rules for the acceptable use of the Lincoln College IT facilities and network infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality of the college's network resources and services.

The standards in this document must be adhered to by all individuals granted access to any machine on the network at any time, whether physically present or via remote access. Failure to comply with the policies set forth in this document will result in disciplinary action.

Definitions

"Lincoln College Network" - comprises the network at the main College, Museum Road and Little Clarendon Street, plus any outlying College properties connected to the University network.

"Authorised User" - any person granted authorisation to use any computer or device on the network.

Policy Scope

The Policy applies to any person granted authorisation to use any computer or device on the Lincoln College Network. This includes (but is not limited to) Fellows, staff, students, temporary workers, contractors, vendors and sub-contractors authorised to access the network locally or remotely, for any reason, including email and Internet or intranet web browsing.

Policy

1. All authorised users must conform to the regulations laid out in the University's Regulations and Policies applying to all users of University ICT facilities document at http://www.it.ox.ac.uk/rules.
2. All authorised users must conform to any and all requirements laid out by the following Acts/policies:
    - Computer Misuse Act (1990);
    - Data Protection Act (1998);
    - Chest Code of conduct;
    - Regulation of Investigatory Powers Act (2000);
    - The Counter-Terrorism and Security Act 2015

3. Only desktop computers, laptop computers, Tablets/PDAs, or Internet-capable cellular devices ("Authorised Devices") may be registered for connection to the network. No other devices, including all network equipment (switches, hubs, wireless routers etc) may be attached to the network, either directly or indirectly, unless these have first been approved for connection by the IT Office.
4. Any authorised device that will be connected to the network must be registered through the Lincoln On-line Registration System, to the authorised user of that device.
5. Any device connected to the network must be configured solely as a client. No device may offer services on the network, including (but not limited to) email servers, web servers, ftp servers and wireless access.
6. Peer-to-peer applications may not be used on the network. The only exception to this rule is Skype which must be configured according to the University's guidance.
7. The use/misuse of authorised devices connected to the network is the responsibility of the individual to whom the device has been registered.
8. Authorised users are permitted to use only network and host addresses that have been issued to them by the College
9. Any device connected to the network must run up-to-date anti-virus protection (assuming a/v protection exists for that platform) and be up to date with the appropriate operating system security patches. Updates should be performed daily and at a minimum, must be performed weekly.
10. All authorised users must conform to the regulations laid out in the University's "Regulations and Policies applying to all users of University ICT facilities" document and the College's Information Security Policy.
11. All authorised devices must (where possible) be running a properly-configured firewall program, such as the Windows or MacOS firewalls supplied with the operating system.

System monitoring

Although the College does not actively monitor use of the network as a matter of course, it does keep records of usage of various aspects of the Service. The College reserves the right to monitor use where it believes there has been (or is a significant risk of) misuse, or where monitoring is necessary for the legitimate interests of the College, or for statistical purposes. The College may use such records and recover deleted data for this purpose.

Liability Issues

3.1 Improper statements made when using the Service can give rise to both personal and corporate liability. Users should always exercise caution in the content of any communications, and should at all times comply with the Data Protection Act and the College's own policies.

3.3 When using the Service, you must ensure that you have not inadvertently agreed to terms, made representations or entered into contractual commitments without having obtained proper authority to do so.

Use of College-owned Computers

Attention must be paid to ensuring that published information has relevance to normal professional activities before material is released in the College's name. Where personal views are expressed a disclaimer stating that this is the case should be clearly added to all correspondence. It is the College's expectation that individuals using workplace computers or telephones for either business or agreed personal use will act responsibly in respect of usage costs and the personal time commitments involved. Reasonable and limited use of these services for social and recreational purposes, where not in breach of this policy and other relevant rules or otherwise forbidden, is permitted outside of normal working hours. This is to be viewed as a privilege and if there is evidence of abuse, appropriate disciplinary action may be taken.

The use of the Internet or e-mail to access and/ or distribute material which may be considered offensive, or material that is not work-related, leaves an individual liable to disciplinary action which may lead to dismissal.

The College has the ability to monitor all internet and telecommunications traffic. The College may monitor network use for statistical purposes, security purposes and misuse detection.

The introduction of new software must first of all be checked and authorised by an appropriate member of the College IT support staff before general use will be permitted.

Only authorised staff should have access to the College's computer equipment.

Only authorised software may be used on any of the College's computer equipment.

No software may be brought onto or taken from the College's premises without prior authorisation. Unauthorised copying and/ or removal of computer equipment/ software may result in disciplinary action.

Specific Regulations Relating to Use of Student IT Rooms

- Only the designated user of an account may use it. You must not let other people know your password.
- No changes whatsoever may be made to the software configuration of the computers.
- Logged in workstations must not be left unattended - this is a security risk as well as being selfish.
- College makes NO absolute commitment to preserve **ANY** user's data on the hard disks or server. This includes personal configuration files and mail. Although every effort will be made to ensure data is regularly backed up you must not assume that any of your files will be in your account the next time that you log on. It is the user's responsibility to back up their data.
- No smoking, eating or drinking in the computer rooms.
- College computer equipment may not be used for commercial purposes.
- No illegal activities may be carried out using the College equipment.

- No material which may cause offense is to be stored or printed on the computer equipment, e.g. pornography or other offensive material.
- No hardware or software may be used which compromises the security of the network or the privacy of users.
- Please do not MOVE the computer units on the worktops. This can upset the cabling, potentially compromising the network or preventing a workstation from operating.
- No connections may be changed or made to any of the computer hardware without the specific consent of the IT Office.
- There is no reserving of terminals.
- Personal belongings must not be left in the computer suite
- The copying of licensed software from the system is forbidden.