WYCLIFFE HALL

STAFF ACCEPTABLE USE POLICY

Most internet services in the Hall are provided to the Hall by the University for academic and education purposes. This means that anyone who wishes to connect their computer to the Hall network must agree to abide by the following rules.

The full set of the University rules concerning network access can currently be found at *http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml*. The important parts of these rules are:

6 6.2 Any password, authorisation code, etc. given to a user will be for his or her use only, and must be kept secure and not disclosed to or used by any other person.
...

7 Users are not permitted to use university IT or network facilities for any of the following:
- 7.1 any unlawful activity;
- 7.2 the creation, transmission, storage, downloading, or display of any offensive, obscene, indecent, or menacing images, data, or other material, or any data capable of being resolved into such images or material [with exceptions only for bona fide, pre-authorised, research subject to lots of conditions];
- 7.3 the creation, transmission, or display of material which is designed or likely to harass another person in breach of the University's Code of Practice on Harassment;
- 7.4 the creation or transmission of defamatory material about any individual or organisation;
- 7.5 the sending of any e-mail that does not correctly identify the sender of that e-mail or attempts to disguise the identity of the computer from which it was sent;
- 7.6 the sending of any message appearing to originate from another person, or otherwise attempting to impersonate another person;
- 7.7 the transmission, without proper authorisation, of e-mail to a large number of recipients, unless those recipients have indicated an interest in receiving such e-mail, or the sending or forwarding of e-mail which is intended to encourage the propagation of copies of itself;
- 7.8 the creation or transmission of or access to material in such a way as to infringe a copyright, moral right, trade mark, or other intellectual property right;
- 7.9 private profit, except to the extent authorised under the user's conditions of employment or other agreement with the University or a college; or commercial purposes without specific authorisation;
- 7.10 gaining or attempting to gain unauthorised access to any facility or service within or outside the University, or making any attempt to disrupt or impair such a service;
- 7.11 the deliberate or reckless undertaking of activities such as may result in any of the following: (*a*) the waste of staff effort or network resources, including time on any system accessible via the university network; (*b*) the corruption or disruption of other users' data; (*c*) the violation of the privacy of other users; (*d*) the disruption of

the work of other users; (*e*) the introduction or transmission of a virus into the network;

…

13 13.5 Participation in distributed file-sharing networks is not permitted [with exceptions only for bona fide, pre-authorised, research subject to lots of conditions]...

Particular attention is drawn to 13 (5). This means that distributed file sharing is not permitted under any circumstances and this means that file sharing programs, including but not limited to (BitTorrent, Kazaa, eMule, uTorrent, Limewire, Thunder, Vuze and Ares) should never be used on this network.

Mobile Devices

Mobile devices represent a significant risk to information security and data security. If the appropriate security applications and procedures are not applied they can be a conduit for unauthorised access to the organisations data and IT infrastructure. This can subsequently lead to data leakage and system infection. The College has a requirement to protect its information assets in order to safeguard its users, intellectual property and reputation.

1. In line with the Colleges rules and regulations with regard to the security of assets, the security of the mobile devices purchased by the College is the responsibility of the assigned user. The assigned user must read and have agreed to abide by this policy.
2. Standard mobile devices for staff will be acquired via the Domestic Bursary after approval by the individual service managers and in consultation with the IT department. The Domestic Bursary will use the College's approved supplier for standard phones with network (carrier) contracts.
3. Personal calls made by a mobile device provided by the College should only be used in emergency situations and call time kept to a minimum. In the light of download limits on devices and possible excess charges on particular tariffs, the Domestic Bursary and IT Manager will liaise to ensure that the correct SIM and tariff are procured. Any abuse or extensive use of the mobile device for personal use will be treated as misconduct. In cases where a mobile device is used as a team phone, the manager of the team must take overall responsibility.
4. A considerable amount of software is now available for smart-phones, in particular for iPhones and android devices. Those issued with smart-phones must take responsibility for any additional software that they install and any costs associated with such software, e.g. iTunes. The IT department cannot take responsibility for the effects on the operation of any device unless IT staff has been consulted beforehand.
5. Mobile devices in need of repair must be returned to the IT department who will check to see if a repair can be made; if this is not possible or cost-effective then the telephones will be returned to the Domestic Bursary who will return it to the suppliers for repair or replacement as appropriate. It must be noted that manufacturers warranties do not normally cover damage caused by misuse, water or neglect, and that the cost of such repairs could be borne by the assigned user.
6. Mobile device firmware should be kept up to date using the manufacturers website or for installed software, the relevant provider e.g. Apple in the case of iTunes. At a minimum network patches should be checked regularly and applied when available. In the case of tablet devices, these may need to be taken back to the IT department for the work to be carried out. Devices must not be connected to any PC which does not have up-to-date anti-virus software and enabled anti-malware protection. If users need to add personal email accounts on their devices, to segment work from personal, they should use a different app for each account (e.g. Mobile mail program/outlook for business and Yahoo mail, google mail app, web login for personal). They must take particular care to ensure that any College data is not sent through their personal email system.
7. The IT department reserves the right to perform a full remote wipe to all devices configured for access to College or the University systems (if the device is owned by the College) to ensure protection of the Colleges data.
8. Devices should not be "jailbroken", i.e., not have any software/firmware installed which is designed to gain access to any unintended functionality. (**To jailbreak a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorised software.)
9. The assigned user will be responsible for payment of any mobile fines incurred (data or roaming charges), however, it is Ultimately the colleges responsibility to keep all data safe under any new

government guidelines.

10. Devices must store any user-saved passwords in an encrypted password store.
11. The assigned user must not leave their mobile device in unlocked offices.
12. The assigned user must ensure that their mobile device is left out of sight in locked vehicles.
13. The assigned user must not lend their mobile device to any person not employed by the College. If a mobile telephone is lent or swapped by users for more than a quick phone call, then the appropriate line manager must be informed.
14. The assigned user must take appropriate precautions not to reveal sensitive information when making a phone call in public.
15. When the assigned user leaves the employment of the College, unless agreement is given for the user to purchase the mobile device, the mobile device must be returned with its charger, user manual and any other parts to the IT department. If the device is to taken/given to an employee, then the college reserves the right to take the device off the current college mobile phone supplier account and to reset the device to factory defaults.
16. The IT department will provide procurement information, best practices, support and maintenance for all mobile devices, excluding standard mobile phones. The Colleges mobile phone supplier should be able to provide reports giving usage and costs when and if needed. The Domestic Bursary will alert managers of any visible misuse for further investigation.

Please be aware that computers on a high bandwidth network such as ours are a prime target and new vulnerabilities are discovered every day. You are encouraged to keep your machines protection software updated and to take great care when opening email attachments. The IT Manager will advise you on sensible precautions if necessary

In order to gain Internet access, you will be required to sign acceptance of this policy upon arrival at Wycliffe Hall.

WYCLIFFE HALL

WYCLIFFE HALL NETWORK ACCEPTABLE USE POLICY 2018

I _____ (please print name) have read and understood the JANET* rules, the Oxford University rules, and the Hall IT rules, and agree to abide by them. I accept responsibility for all use of the network made by or through computers which I connect to the Hall's network.

* *(Joint Academic NETwork)*

Signed: _____ **Date:** _____

Building: _____ **Room /Flat No:** _____