WYCLIFFE HALL

NETWORK 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 https://governance.admin.ox.ac.uk/legislation/it-regulations-1-of-2002. 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 Hall has a requirement to protect its information assets in order to safeguard its users, intellectual property and reputation.

1. The security of mobile devices is the responsibility of the user. If purchased by the Hall the responsibility is that of the assigned user. All users must read and have agreed to abide by this policy.
2. The Hall may not be responsible and accountable for keeping its data safe, but cannot be held accountable for the payment of any mobile fines (roaming, data charges) incurred, this is the responsibility of the user.
3. Devices must store any user-saved passwords in an encrypted password store.
4. Please do not leave a mobile phone unlocked in a work area.
5. Please ensure that mobile devices are kept out of sight in locked vehicles.
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.
7. Devices must not be connected to any PC which does not have up-to-date anti-virus software and enabled anti-malware protection.
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.)

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 2021

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:** _____