

UNIVERSITY ACADEMY
HOLBEACH



UNIVERSITY OF
LINCOLN

The University Academy Holbeach

Principal: Steve Baragwanath B.Sc. (Hons.)

ICT Acceptable Use Policy

Networked resources, including Internet access are available to all learners in the school. All users are required to follow the conditions laid down in the policy. Any breach of these conditions will be considered a disciplinary matter and may lead to: the withdrawal of the user's access, an investigation of the user's use of services, and in some instances could lead to criminal prosecution. The school expects that students will use new technologies as appropriate within the curriculum.

COMPUTING FACILITIES

Users are expected in the main to make use of the school's computing facilities for educational purposes. All users are expected to act responsibly and to show consideration to others.

ACCOUNT SECURITY

Users are responsible for the protection of their own network account and should not divulge passwords to anybody. Users should not choose passwords that are easy to guess and should not record these. Users should not logon to or use any account other than their own and should logoff when leaving a workstation, even for just a short period of time.

USE OF FACILITIES

It is not acceptable to:

1. Attempt to download, store or install software to school computers.
2. Attempt to introduce a virus or malicious code to the network.
3. Attempt to bypass network or system security.
4. Attempt to access another user's account.
5. Use another user's account if it has not been logged off.
6. Attempt to gain access to an unauthorised area or system.
7. Connect any device to the network that acts as a Wireless Access Point (WAP), bridge or router.
8. Connect any device to the network that has access to the Internet via a connection not provided by the school.
9. Access, download, create, store or transmit material that is indecent or obscene, could cause annoyance or offence or anxiety to others, infringes copyright or is unlawful and/or brings the name of the school in to disrepute.
10. Engage in activities that waste technical support time and resources.

INTERNET ACCESS

The school's Internet service is filtered to prevent access to inappropriate content and to maintain the integrity of the computer systems. Users should be aware that the school logs all Internet use.

1. The use of public chat facilities is not permitted.
2. Students should not copy and use material from the Internet to gain unfair advantage in their studies, for example in coursework. Such actions may lead to disqualification by examination boards.

3. Students should ensure that they are not breaking copyright restrictions when copying and using material from the Internet.
4. Students agree not to use their own devices to connect to the Internet from outside of school.
5. Staff should take care when downloading resources to their school lap-top as this can have a negative impact on the school network. If in doubt advice should be sought from the ICT Manager.

EMAIL

Automated software scans all email and blocks messages and attachments that could compromise the integrity of the computer systems or contain unsuitable/offensive content.

1. Students are not allowed to use email during lessons, unless the teacher for that lesson has permitted its use.
2. If a student receives an email from an unknown person or that is offensive or upsetting, the relevant teacher or a member of the ICT department should be contacted. Do not delete the email in question until the matter has been investigated.
3. Do not open attachments from senders you do not recognise, or that look suspicious.
4. Students Users should periodically delete unwanted sent and received emails.
5. Staff should only communicate by e-mail with students for work purposes and on the school network. The use of social-networking sites should be avoided.

INSTANT MESSAGING / SOCIAL NETWORKING

1. The use of Instant Messaging (IM), and social networking (SN) sites is NOT allowed.
2. Students should ensure that electronic communications with staff using IM and social networking is not conducted
3. Staff must ensure that electronic communications with students using IM and social networking is not conducted.
- 4.

PRIVATELY OWNED COMPUTERS

Personal laptops and desktops are NOT allowed to be connected to the school network.

PRIVACY AND PERSONAL PROTECTION

1. Users must, at all times, respect the privacy of others.
2. Users should not forward private data without permission from the author.
3. Students should not supply personal information about themselves or others via the web or email.

4. Students must not attempt to arrange meetings with anyone met via the web or email.
5. Students should make sure they have read the school's E-Safety policy.
6. Users should realise that the school has a right to access personal areas on the network. Privacy will be respected unless there is reason to believe that the ICT Acceptable Use Policy or school guidelines are not being followed.

DISCIPLINARY PROCEDURES

Those who misuse the computer facilities and break the ICT Acceptable Use Policy will be subject to disciplinary procedures.

SUPPORT

If you have any questions, comments or requests with regards to the systems in place, please do not hesitate to contact a member of the ICT department. Faulty equipment should be reported to one of the ICT technicians in person or by email as soon as it is discovered. Users should not attempt to repair equipment themselves.