



FYLING HALL SCHOOL

Acceptable Use Policy (AUP)

Last updated 10 April 2008

Fyling Hall Acceptable Use Policy (AUP)

COMPUTING FACILITIES

Users are encouraged 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. Users can access internal systems including school email, from outside the school via the users' website at <http://users.fylinghall.org>

USE OF TECHNOLOGY

Technology that can be used to store, transmit or manipulate data, such as media rich phones, MP3 players, Personal Digital Assistants (PDAs) and USB media, should be used responsibly and in accordance with this Acceptable Use Policy, even when not used with school equipment.

ACCOUNT SECURITY

Users are responsible for the protection of their own network account and should not divulge passwords to anybody including members of staff. Passwords must be complex; a minimum of 6 characters, which must include a combination of uppercase and lowercase letters, numbers and punctuation marks. 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: Attempt to download, store or install software to school computers. Attempt to introduce a virus or malicious code to the network. Attempt to bypass network or system security. Attempt to access another user's account. Attempt to gain access to an unauthorised area or system. Attempt to use any form of hacking/cracking software or system. Connect any device to the network that acts as a Wireless Access Point (WAP), bridge or router. Connect any device to the network that has access to the Internet via a connection not provided by the school. 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, brings the name of the school in to disrepute. 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 and network use. The use of public chat facilities is not permitted. Users 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. Users should ensure that they are not breaking copyright restrictions when copying and using material from the Internet.

EMAIL

Automated software scans all email and removes content that could compromise the integrity of the computer systems or contain unsuitable/offensive content. Pupils are not allowed to use email during lessons, unless the teacher for that lesson has permitted its use. If a user receives an email from an unknown person or that is offensive or upsetting, the relevant housemaster or a member of

the IS department should be contacted. Do not delete the email in question until the matter has been investigated. Sending or forwarding chain emails is not acceptable. Sending or forwarding emails to a large number of recipients is acceptable only for a good reason. Before doing so, the user must obtain permission from the Network Manager. Do not open attachments from senders you do not recognise, or that look suspicious. Users should periodically delete unwanted sent and received emails. Pupils may only use the email facilities provided by the School.

INSTANT MESSAGING / SOCIAL NETWORKING

The use of Web-based Instant Messaging (IM), and some social networking (SN) sites is allowed. Pupils are not allowed to use these facilities during lessons or during prep time, unless the teacher for that lesson has permitted its use. If a user receives a message from an unknown person, or which is offensive or upsetting, the relevant housemaster or a member of the IT department should be contacted. Copy and save the message until the matter has been investigated. Only communicate with people on your Contact or Buddy List. Do not accept requests to join your contact list from people you do not already know. Never accept files or downloads from people you do not know, or that looks suspicious. Do not use a screen-name that is offensive, or gives away additional personal information. Do not add unnecessary personal information to your profile or account details. Do not add or allow your profile, screen-name or contact information to be shown in online public directories.

PRIVATELY OWNED COMPUTERS

Personal laptops and desktops are allowed to be connected to the school network. They are subject to this Acceptable Use Policy. All computers must, for their own protection, have Antivirus software installed, which can be provided by the school.

PRIVACY AND PERSONAL PROTECTION

Users must, at all times, respect the privacy of others. Users should not forward private data without permission from the author. Users should not supply personal information about themselves or others via the web, email or IM/SN. Users must not attempt to arrange meetings with anyone met via the web, email or IM/SN. 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 Acceptable Use Policy or school guidelines are not being followed.

DISCIPLINARY PROCEDURES

Those who misuse the computer facilities and break the Acceptable Use Policy will be subject to disciplinary procedures. Email support@fylinghall.org 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 IT department. Faulty equipment should be reported to the IT department in person or by sending an email to support@fylinghall.org. Users should not attempt to repair equipment themselves.