



ICT ACCEPTABLE USE POLICY

(For all users of Information, Communication Technology at St Aldhelm's Academy)

Aims

To ensure that users of our Academy understand the ways in which Information communication technology (ICT) equipment is to be used. This policy ensures that ICT facilities and the Internet are used effectively for their intended purpose, without infringing legal requirements or creating unnecessary risk.

This policy applies to all users and administrators of St. Aldhelm's Academy ICT services and/or infrastructure.

On evidence provided by the Academy, an employee may enter into disciplinary procedures by their employer. At the same time, if a user's conduct and/or action(s) are illegal, the user may become personally liable in some circumstances.

Policy Statement

Staff and the young people are provided with free access to a wide range of ICT provision to enable and assist their work and support their educational development. By using the Academy's provision all users are agreeing to the 'Acceptable Use Policy'. When logging on to any computer in the Academy, users are presented with an informational message that alerts them to the fact that they are bound to the terms in this policy. All users must click OK to show that they agree to the policy before they can continue to use the systems. This action is considered as further agreement to the terms of this policy.

Users are responsible and personally accountable for their use and activity on the Academy's ICT systems. Any use that contravenes this policy will be dealt with by the standard disciplinary routes and may involve withdrawal of ICT user privileges.

Monitoring

The Academy reserves the right to monitor all activity on the Academy network by all users. All forms of electronic data held on the Academy's systems are the property of the Academy. The SLT, Network Manager and any designated staff can access any data stored on the Academy's systems at any time to ensure that the system is being used appropriately. Also at the request of the Principal or a member of the SLT, the ICT Support team will investigate if there has been any breach of this policy by searching files and communications on the Academy's systems. Users should not expect nor assume that their Academy files, emails and Internet activities are private.

Identification of Users

1. All users are given a unique user name and password. This password must be kept secret at all times. Staff should change their password at regular intervals to maintain the security of their files and the data they have access to. The ICT team will, at times force all users to change their passwords. If a young person feels that their password has been compromised they must see the ICT Support Team immediately to have it reset. The ICT Support team

does not know the passwords of any individual user and will only reset the password of a user at their own request.

2. Any activity carried out under the user name of an individual is the responsibility of the named person associated with that user name. It is the users responsibility to ensure that they properly log out of the computer when they have finished using it.
3. Users must not use another person's account or attempt in any way to discover their password.

Unacceptable use

St Aldhelm's Academy expects all users to use ICT facilities and the Internet responsibly and strictly according to the following conditions:

4. Users must not use the Academy's ICT systems for the creation or transmission of obscene, abusive, offensive or indecent images, data or other material or any data of being resolved into obscene or indecent images or material.
5. Users must not use the Academy's ICT systems to harass or bully any other person. Any such activity will be treated the same as physical bullying and will be subject to the same anti bullying policy.
6. Users must not use the academy's ICT systems for the creation of material with the intent to defraud.
7. Users must not use the Academy's ICT systems for the creation or transmission of defamatory material.
8. Users must not bring into the Academy any material that would be considered inappropriate on paper. This includes files stored on CD, DVD or any other electronic storage medium.
9. Under no circumstances should any user of the Academy's ICT systems download, upload or bring into the Academy material that is unsuitable for children or the Academy. This includes any material of a violent, racist or inappropriate sexual nature. The transmission, display, storage or promotion of any such material is a violation of the Computer Misuse Act 1990, and possession of certain types of material can lead to police prosecution.
10. Users must not use the Academy's ICT systems for the creation or transmission of content that promotes extremist activity, including terrorism and weapons.
11. Users must not post any information on websites that could cause any other member of the Academy distress, or bring the Academy into disrepute.
12. Users are responsible for all files that are stored in their storage area and any visits to websites by their user account.
13. Users may not use any of the Academy's ICT systems for financial gain, or any political or commercial activity.
14. Users must not breach the copyright of any materials whilst using the Academy's ICT systems. This includes, but is not exclusive to:
 - a) Not copying, or attempting to copy, any of the Academy's software.
 - b) Not copying the work of another user or engaging in plagiarism.
 - c) Not storing any files in their personal storage area which require copyright permission, and where that permission is not held.
15. Any breach of copyright whilst using the Academy's ICT systems is the individual user's responsibility and the Academy cannot accept any liability or litigation for such a breach.
16. Users must not download copy or attempt to install any software onto Academy computers.
17. Any attempt by a user to compromise the security or functionality of the Academy network and its ICT systems, from either internally or externally, will be considered as 'hacking'. It should be noted that 'hacking' is illegal under the Computer Misuse Act 1990 and is prosecutable under law.

18. Users must not deliberately attempt to gain unauthorised access to networked facilities or services, including any attempt to probe, scan or test the vulnerability of the system or network.
19. Users must not connect any network-enabled personal device to the Academy's network without the express permission of the SLT.
20. All machines physically connected to the Academy's ICT network, not from home, must have an appropriate, fully functioning and up to date antivirus software protection.
21. Users must not carry out any of the following deliberate activities:
 - a) Wasting staff effort or networked resources, including time on end systems and the effort of staff involved in the support of those systems.
 - b) Corrupting or destroying other users' data.
 - c) Violating the privacy of other users.
 - d) Disrupting the work of others.
 - e) Denying service to other users (for example, by deliberate or reckless overloading of access links or switching equipment.).
 - f) Continuing to use an item of networking software or hardware after the Academy has requested that use cease because it is causing disruption to the correct functioning of the Academy's ICT systems.
 - g) Other misuse of the Academy's ICT and networked resources, such as the introduction of viruses or other harmful software to the Academy's ICT systems.
 - h) Unauthorised monitoring of data or traffic on the Academy's ICT network or systems without the express authorisation of the owner of the Academy's network or systems.
22. When accessing any of the Academy's systems from home or an external location, this policy still applies.
23. When accessing another network from the Academy's ICT network, any breach of the acceptable use policy of that network will be regarded as unacceptable use of the Academy's ICT systems.
24. The Academy wishes to encourage all users to use the Internet, however it is provided for Academy business and any non Academy use of the Internet must be carried out in the user's free time.
25. The Academy cannot be held responsible for any failed personal financial transaction that may happen whilst using the Academy's ICT systems.
26. Any attempt to circumvent the Academy's firewall and Internet filtering systems will be treated as a breach of this policy. This includes the use of proxy servers and websites to bypass the Internet filtering system. Such activity will be subject to the standard disciplinary procedures and could mean removal of access to the Academy's systems or Internet access.
27. There is a wealth of information on the Internet; however due to the open nature of the Internet, a lot of material is either illegal or unacceptable. Any user that thinks inappropriate or illegal material is being accessed must report it to their teacher, line manager or the ICT Support team. Any user found accessing such material will be subject to the Academy's disciplinary procedures.

This policy will be reviewed annually.

