

ICT Acceptable Use Policy

Please read this document carefully, only once it has been agreed to, will access to the Internet and the School's computer systems be permitted. Listed below are the provisions of this agreement. If any pupil violates these provisions, access to services will be denied and the pupil will be subject to disciplinary action.

1. Personal Responsibility

As representatives of the school, pupils are encouraged to take responsibility for reporting any misuse of the network to a staff member. Misuse may come in many forms, but it is commonly viewed as any message(s) sent or received that indicate or suggest, unethical or illegal requests, racism, sexism, inappropriate language, bullying or pornography any use which may be likely to cause offence and other issues described below.

2. Acceptable Use

The use of electronic services must be in support of education and research in accordance with the educational goals and objectives of the School. Pupils are encouraged to take responsibility for this provision at all times when using the electronic information service.

Use of other networks or computing resources must comply with the rules appropriate to that network. Transmission of any material in violation of any United Kingdom, or International, laws is prohibited.

This includes, but not limited to

- Copyrighted material
- Threatening or obscene material
- Material protected by trade laws.

Pupils must acknowledge that they will be held responsible for any unlawful activities they may commit.

Use of commercial activities by for-profit organisations is generally not acceptable unless authorised by the school governing committee.

3. Privileges

The use of the Internet and other electronic services is a privilege and inappropriate use will result in that privilege being withdrawn. The School Deputy Head will rule upon inappropriate use and may deny, revoke or suspend usage.

4. Network Etiquette and Privacy

You are expected to abide by the generally accepted rules of network etiquette. These rules include, but are not limited to the following:

- BE POLITE. Never send or encourage others to send abusive messages.
- USE APPROPRIATE LANGUAGE. Remember that you are a representative of the school on a global public system. You may be alone with your computer, but what you say and do can be viewed by others. Never swear, use vulgarities or any other inappropriate language. Illegal activities of any kind are strictly forbidden.

- **PRIVACY.** Do not reveal any personal information to anyone, especially the home address or personal telephone of yourself or any other pupils.
- **PASSWORD.** Do not reveal your password to anyone. If you think someone has obtained your password, change it and contact a member of staff immediately.
- **ELECTRONIC MAIL.** Electronic Mail (e-mail) may be provided for educational use only, and will be monitored by ICT Network Support and School staff. **Access to external e-mail is strictly prohibited by the School.** Messages relating to, or in support of, illegal activities may be reported to the authorities.
- **DISRUPTIONS.** Do not use the network in any way that would disrupt use of the services by others.

5. Services

Al-Ashraf Primary School makes no warranties of any kind whether expressed or implied, for the network service it is providing. Al-Ashraf Primary School will not be responsible for any damages suffered whilst on this system. These damages include loss of data as a result of delays, non-deliveries, mis-deliveries or service interruptions caused by the system or elements of the system, or your errors or omissions. Use of any information obtained via the network or other information systems is at your own risk. Al-Ashraf Primary School specifically denies any responsibility for the accuracy of information obtained via its Internet services. The school operates a data backup system for the Administrators Office and the ICT departments use only. The ICT department does not maintain regular backups of Students or Staff data. It is the responsibility of the student or staff member to maintain their own data backups of any work etc via the use of USB Flash Drives etc or any other suitable method that has been agreed with the ICT department.

6. Internet Access

The Internet is a valuable resource for pupils to use to gain information relevant to their coursework within the school. However it is necessary for ICT Network Support to limit access to the Internet to protect the pupils from inappropriate material and also to ensure that the Internet does not become a distraction to the pupils whilst in school.

This is achieved by using an Internet filtering system which is regularly updated as new sites appear daily. This system also keeps a record of what sites a pupil has accessed or attempted to access, together with the time, date and workstation ID.

If a pupil is found to be abusing their Internet Access privilege by trying to bypass the security of the system using Proxy servers etc, then their access to the Internet may be removed for a period of time, which will be decided upon by the Principal. If persistent misuse is identified then the pupil may lose access permanently.

7. Security

Security on any computer system is a high priority because there are so many users. If you identify a security problem, notify School Staff at once. Never demonstrate the problem to another pupil. All use of the system must be under your own username and password. Remember to keep your password to yourself. Do not share it with friends. Anyone caught disclosing passwords may have their access denied and may be subject to disciplinary action. Any user identified as a security risk may be denied access to the system and be subject to disciplinary action.

If you have forgotten or believe someone else knows your password then you should consult your teacher or a member of staff to have your password reset. A record of password resets will be kept by ICT Network Support. This data will be strictly limited to the username, date a password was reset and the number of resets performed. ICT Network Support will not keep a record of your password.

If a pupil is found to be deliberately trying to gain unauthorised access to school systems or trying to circumvent or bypass the security measures put in place by the school via the ICT Department will be subject to disciplinary action. In certain instances, where the offence of a more serious nature has taken place, then the school may pass the details onto the police for their investigation.

8. Vandalism

Vandalism is defined as any malicious attempt to harm or destroy any equipment or data of another user or of any other networks that are connected to the system. This includes, but is not limited to, theft, the uploading or creation of computer viruses, the wilful damage of computer hardware, whether connected to the network or not, the unauthorised deletion of data from its place of storage or the defacing of any computer-related hardware.

Anybody determined to have vandalised the system may have their access rights revoked and will have to pay for any damage caused.

9. Online Ordering systems

One of the many facilities available via the Internet is the ability to order goods and services whilst online. This technology is still undergoing development and several questions have been raised with regard to the issue of security of online credit card ordering etc. Because of the security and other ethical issues attached to this facility, Al-Ashraf Primary School has a moral responsibility in this area. It is therefore strictly forbidden for pupils to use the Internet for ordering goods or services regardless of their nature.

10. Electronic Mail

Electronic mail (Email) is widely available via the Internet. The use of any e-mail system apart from the School's own internal e-mail system is strictly forbidden. Pupils are expected to use this facility in a responsible manner. The sending or receiving of any email, which contains any inappropriate material, is strictly forbidden. This material includes, but is not limited to, pornography, unethical or illegal requests, racism, sexism, inappropriate language, any use which may be likely to cause offence. Disciplinary action will be taken in all cases. It is also forbidden to send large volume Emails (Spamming).

Random checks will be performed on users' mailboxes and anybody found to be contravening the rules will have their access to the School's e-mail system removed immediately.

ICT Network Support log all email sent and received within the system to ensure the above points are adhered to. Emails will be kept for the duration of the academic year, at which point all pupil email will be deleted from their mailboxes.

11. Chat Services

Pupils are not permitted to use any form of chat services available on the Internet, this includes, but not limited to, Yahoo! Instant Messenger™, MSN Messenger™, or any web-based chat systems.

12. Forums & Bulletin Board Systems.

Pupils are not permitted to use any form of Forum or Bulletin Board System (BBS) from the school computer network. Any pupil found to be attempting to gain access to such a system from a school computer and/or laptop may face disciplinary action and their ICT privileges suspended or revoked.

13. Miscellaneous

The school computer system is to be used to the sole purpose of educational tasks only. Any pupil using a computer for recreational purposes will be removed from that computer to allow access to anyone requiring it for study or other legitimate use.

No pupil may transfer music and/or video content to local or networked drives. These drives will be checked regularly and any such files will be deleted. Storage of such files not only takes up valuable space, but are also illegal and an infringement of copyright. Any pupil found to be copying copyright material may face disciplinary action and have their access rights revoked for a period of time to be determined by School D.

Access to local or networked drives is for the storage of coursework only. All non coursework related material will be removed by ICT Network Support, this includes, although not limited to: audio/video files and executable files (such as, but not limited to, games, chat programs, applications, etc)

Members of the ICT Network Support will monitor the use of the system and its services. This includes checking the data stored in the personal folders. If it is found that the system is being abused, access may be withdrawn without notice.

Pupils' full names and other details will never be stored together with their pictures in any publicly accessible areas. This includes the School's Internet site and is for the safety of the pupils. Any pupil found displaying such information either internally or externally, will have their access to ICT systems revoked, and face disciplinary procedures.

Pupils found to be posting material on public systems outside of school that may bring Al-Ashraf Primary School and/or its staff into disrepute, or may be deemed offensive and/or defamatory will face disciplinary action by School Management. The matter may also be passed to the Police should the situation warrant such action.