Acceptable Use Policy for Pupils

Computer systems, including Internet access, are potentially available to pupils. All users are required to follow the conditions laid down in the policy whether using school equipment or the students own personal devices (e.g. laptops and mobile phones) and all devices must be used in accordance with the school rules and policies and only when appropriate to do so. Any breach of these conditions may lead to withdrawal of the user's access; monitoring and or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter. Note that personal devices will only be allowed on the network if approved by ICT technical staff.

These computer systems are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. Any expression of a personal view about the school or County Council matters in any electronic form of communication must be endorsed to that effect. Any use of the network that would bring the name of the school or County Council into disrepute is not allowed. Independent pupil use of the Internet or the school's Intranet will only be permitted upon receipt of signed permission and agreement form as laid out below.

Conditions of Use

Personal Responsibility
Access to the computer systems is a privilege, not a right. Users are responsible for their behaviour and communications. Pupils will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuse of the network to ICT support.

Acceptable Use
Users are expected to utilise the computer systems in a responsible manner. It is not possible to set hard and fast rules about what is and what is not acceptable but the following list provides some guidelines on the matter:

Network Etiquette and Privacy
Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

1. Be polite – never send or encourage others to send abusive messages.
2. Use appropriate language – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.
3. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4. Privacy – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other user's files or folders.
5. Password – do not reveal your password to anyone. If you think someone has learned your password then contact ICT support.
6. Electronic mail – Is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Do not send anonymous messages.
7. Disruptions – do not use the network in any way that would disrupt use of the network by others.
8. Pupils will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.
9. Students finding unsuitable websites through the school network should report the web address to ICT support
10. Do not deliberately introduce 'malware' onto the computer system.
11. Do not attempt to visit websites that might be considered inappropriate. (Such sites would include those relating to illegal activity) All sites visited leave evidence in the county network if not on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use).

12. Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
13. Files held on the school's network will be regularly checked by ICT support.
14. It is the responsibility of the User (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of the Internet/Intranet does not occur.
15. Pupils should use the computer system to focus on their learning.

UNACCEPTABLE USE
Examples of unacceptable use include but are not limited to the following:

- Users must login with their own user ID and password, where applicable, and must not share this information with other users. They must also log off after their session has finished.
- Users finding machines logged on under other users username should log off the machine whether they intend to use it or not.
- Accessing or creating, transmitting, displaying or publishing any material (e.g. images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety. (The County Council have filters in place to block e-mails containing language that is or may be deemed to be offensive.)
- Accessing or creating, transmitting or publishing any defamatory material.
- Creating, transmitting or publishing any terrorist or extremist material. Such material may only be accessed when authorised by the Senior Leadership Team for the purpose of legitimate study.
- Receiving, sending or publishing material that violates copyright law. This includes through Video Conferencing and Web Broadcasting.
- Receiving, sending or publishing material that violates Data Protection Act or breaching the security this act requires for personal data.
- Transmitting unsolicited material to other users (including those on other networks and on any social media).
- Unauthorised access to data and resources on the school computer system or other systems.
- User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.

Additional guidelines
- Users must comply with the acceptable use policy of any other networks that they access.
- Users must not download software without approval from ICT support.

Services
There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

Network Security
Users are expected to inform ICT support immediately if a security problem is identified. Do not demonstrate this problem to other users. Users must login with their own user id and password, where applicable, and must not share this information with other users. Users identified as a security risk will be denied access to the network.

Wilful Damage
Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

Media Publications

Written permission from parents or carers will be obtained before photographs of pupils are published. Named images of pupils will only be published with the separate written consent of their parents or carers. (See separate Pupil Image Consent Form).

Publishing includes, but is not limited to:

- the school website, VLE
- the Local Authority web site,
- web broadcasting,
- TV presentations,
- Newspapers.

Pupils' work will only be published (e.g. photographs, videos, TV presentations, web pages etc) if parental consent has been given.