Acceptable use policy

Computer, tablet and internet use are a daily occurrence within schools and when used correctly can enhance learning within the classroom and school environment. However all users must use the technology and systems according to this policy to ensure no harm comes to them or others around them when using the school system.

Networked resources, including internet access, are potentially available to students and staff in the school. All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and/or retrospective investigation of the user's use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

These networked resources 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.

The school expects that staff will use new technologies as appropriate within the curriculum and that staff will provide guidance and instruction to pupils in the use of such resources. Independent pupil use of the internet or the school's intranet will only be permitted upon receipt of signed permission and agreement forms as laid out below. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Conditions of use

Personal responsibility

Access to the networked resources is a privilege, not a right. Users are responsible for their behavior and communications. Staff and 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 member of staff responsible.

Acceptable use

Users are expected to utilise the network systems in a responsible manner. It is not possible to set a complete set of rules about what is and what is not acceptable but the pages on network expectations and privacy together with unacceptable use provides some guidelines on the matter

Network use expectations and privacy

Users are expected to abide by the rules of network expectations. These rules include, but are not limited to, the following:

- Be polite – never send or encourage others to send abusive messages.

- 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.

- Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.

- Privacy – do not reveal any personal information (for example home address, telephone number) about yourself or other users. Do not trespass into other users' files or folders, without permission.

- Password – do not reveal your password to anyone.

- Electronic mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities.

- Disruptions – do not use the network in any way that would disrupt use of the network by others.

- Pupils will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.

- Staff or students finding unsuitable websites through the school network should report the web address to the member of staff responsible.

- Do not introduce 'CDs' or 'pen drives' into the network without having them checked for viruses.

- 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.

- 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 or intranet does not occur.

Unacceptable use

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

- Users must log in with their own user ID and password, where applicable, and must not share this information with other users, unless permission is given.

- Users finding machines logged on under other user's username should log off the machine whether they intend to use it or not.

- Accessing or creating, transmitting, displaying or publishing any material (for example images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety. The County Council have filters in place to block emails containing language that is or may be deemed to be offensive.

- Accessing or creating, transmitting or publishing any offensive material.

- Transmitting unsolicited material to other users (including those on other networks).

- Unauthorised access to data and resources on the school network 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.

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 member of staff responsible immediately if a security problem is identified. Do not demonstrate this problem to other users. Users must log in 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.

Physical security

Staff users are expected to ensure that portable ICT equipment such as laptops, tablets, digital still and video cameras are securely stored when they are not being used.

Willful 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

Full names alongside images of pupils (for example in photographs, videos, web broadcasting, TV presentations, and web pages) must not be published under any circumstances. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or other online sites.

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