Accessible Use of E-Safety

April 2018

As part of the school's ICT programme, we offer pupils access to the Internet. Before being allowed to use the Internet, we require all pupils to pass a test and to obtain parental permission. Access will only be given if you sign and return the enclosed form as evidence of your approval and their acceptance of the school rules on this matter.

Access to the Internet will enable pupils to explore thousands of libraries, databases, and other information plus exchange messages with other Internet users throughout the world. Every effort will be taken by the school to ensure that pupils are only able to access suitable information sources. The school Internet Service Provider operates a filtering system that restricts access to inappropriate materials. However, families should be warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate or potentially offensive. Whilst our aim for Internet use is to further educational goals and objectives, it is always possible that pupils may find ways to access other materials. We believe that the benefits to pupils from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages.

We recognise that parents and guardians of minors have the ultimate responsibility for setting and conveying the standards that their children should follow. We also appreciate this is exercised on a daily basis through the control you exert over your child's access to information sources such as television, telephones, films, radio and other media. During school time, teachers will exercise equal vigilance in guiding pupils only towards appropriate material. However, the school supports and respects each family's right to decide whether or not to apply for access.

We have included below our Acceptable Use of E-Learning Systems Policy, this is a standard policy for use with families.

Networked resources, including Internet access and virtual learning environments are potentially available to pupils and staff both from within the school and from home. All users are required to follow the conditions laid down in this policy. 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.

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, 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 academy, into disrepute is not allowed. If parents wish to complain or make comment about the academy, we would ask that they do so by contacting the Head teacher. The use of Facebook, Twitter and other social media sites are not the forum to air any negative comments about the academy.

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 in this document. 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 behaviour 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 to the class teacher or school office.

Acceptable Use
Users are expected to utilise the network 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 users files or folders.
5. Password – do not reveal your password to anyone. If you think someone has learned your password then contact your class teacher (or the e-learning co-ordinator for staff.)
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. Pupils will not be allowed access to Facebook, Twitter or other social networking sites.
10. Staff or pupils finding unsuitable websites through the school network should report the web address to the class teacher (or the e-learning co-ordinator for staff.)
11. Do not introduce “pen drives” into the network without having them checked for viruses.
12. 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.
13. Unapproved system utilities and executable files will not be allowed in pupils’ work areas or attached to e-mail.
14. Files held on the school’s network will be regularly checked by school staff.
15. 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.

Unacceptable Use
Examples of unacceptable use, both from within school and from home 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 school has 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.
- 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. (See section 9.0 respectively in the WSCC ICT in schools Acceptable Use Protocol guidance).
- 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 such as the VLE..
- 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 the e-learning co-ordinator.

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 their class teacher or e-learning co-ordinator 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.

PHYSICAL SECURITY
Staff users are expected to ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used. Items that need to be left over breaks and lunchtimes for example will need to be physically protected by locks and or alarms.

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.

We realise that the policy is a wordy one and not best suited to all of our pupils, we have to use this policy as it has been agreed with the LA and has been approved by the legal team. We ask that parents speak to their children about good behaviour online, safety and the protection of passwords and personal identity. If you wish your child to have access to the Internet at school and our e-learning products at home and school, please complete the pemission form below. **Help your child to be safe online. Visit www.thinkuknow.co.uk/8_10 for online safety activities from CEOP.**