****

**BISK AUP**

* An **AUP** is an agreement between the student and the district designed to keep students safe online. This agreement allows them to explore the digital world as part of their education, instead of accessing inappropriate or harmful sites, such as bullying, **school** violence, pornography, etc
* The purpose of an **Acceptable Use Policy** (**AUP**) is to communicate in clear language how a district's computer and network resources are to be used so that the environment is safe, secure and reliable. Educational institutions **have** a responsibility to keep their students safe.

The Acceptable Use Policy (AUP) for Internet use is one of the most important documents a school will produce. Creating a workable AUP requires thoughtful research and planning.

**Introduction**

The internet is an essential element of 21st Century life for education and social interaction. The purpose of internet use in school is to promote pupil achievement, to support the professional work of staff and to enhance the school’s management, information and business administration system. Benefits include:

Access to worldwide resources and research materials.

Educational and cultural exchanges between pupils worldwide (Skype for instance).

Access to experts in many fields.

Staff professional development such as access to online learning and forums.

Communication with support services, professional associations and colleagues.

Exchange of curricular and administration data .

The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. Consequently, in delivering the curriculum teachers need to plan to integrate the use of ICT and web based resources including email to enrich learning activities. Effective internet use is an essential life still.

Access to the school’s ICT network and use of ICT facilities owned by the school, including access to the internet, are conditional on observance of the following Acceptance Use Policy. The Aims of this Acceptable Use Policy are to:

Allow all users access to school ICT resources and use of the internet for educational purposes.

Provide a mechanism by which staff and pupils are protected from Internet sites, information, and individuals that would undermine and principles and aims of the school.

Provide rules which are consistent, and in agreement with the Data Protection Act 1984, Computer Misuse Act 1990 and other legislation relevant to the use of computers and electronic data in schools.

Provide rules relating to the use of computers and ICT facilities in school, which are consistent with the general policies of the school.

* Pupils who are to have access to the internet must understand the basic conventions and navigation techniques before going online and accessing material.
* Pupils must have returned a signed consent form before being allowed to use the ICT facilities that involve accessing the internet. The use of the names of pupils or photographs of pupils for the website will require written permission from parents/carers. If a picture is placed on website the child’s full name will not be displayed.
* Pupils must not use the school ICT facilities without supervision of a member of staff. Although use of the ICT facilities and access to the internet will be supervised.

**BISK** is protected by firewall filtering service and can be used as evidence in circumstances where a computer has been used to access such inappropriate material.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the ICT Technician or Co-Ordinator immediately who will, in turn, record the address and report on to the headteacher and internet provider.

Pupils are aware that they must only access those services they have been given permission to use.

Staff and pupils are made aware that the use of computer systems without permission or for inappropriate purpose is a criminal offence (Computer Misuse Act 1990).

**Log in and passwords**

Pupils and staff must not disclose any password or login name given to anyone, or allow anyone else to use a personal account.

Pupils and staff must not attempt to gain access to the school network or any internet resource by using someone else’s account name or password.

Staff and pupils must ensure PC’s, mobile devices and laptops are logged off when left unattended.

General safety and risk assessment

Users must treat with respect equipment and services in school and at other sites accessed through school facilities, and are subject to regulations imposed by the respective service providers. Malicious action will result in immediate suspension from use of the school facilities.

Staff are responsible for sharing the safety issues with their pupils.

**Prevention**

We recognize that the best way to deal with cyber bullying is to prevent it from happening in the first place. By embedding good, safe ICT practice into all our teaching and learning, incidents can be avoided.

We recognize we have a shared responsibility to prevent incidents of cyber bullying, the headteacher has the responsibility for coordinating and monitoring the implementation of anti-cyber bullying strategies.

E-safety

Children and staff are reminded of E-Safety Codes of Conduct. Any work or activity on the internet must be directly related to schoolwork. Children and parents are provided with e-safety sessions which are led in school.

Any work or activity on the internet must be directly related to schoolwork. Private use of the internet (including social networking sites) in school is strictly forbidden.

Staff are discouraged from being members of social networking sites. However, if staff are members, they are reminded of the necessity to keep their profiles secure and to avoid contact with persons (particularly parents/pupils or ex-pupils) related to the school. Staff are reminded that any action or comment that brings the school or colleagues into disrepute or compromises pupil or staff confidentiality will be classed as a disciplinary matter.

* Do no give personal email or postal addresses and telephone numbers of any person.

Under no circumstances give email or postal addresses/telephone numbers/fax numbers of any members of staff or pupils at school.

* Do not download, use or upload any material that is copyright. Always seek permission before using any material from the internet. If in doubt, or you cannot obtain permission do not use the material.

Search engines (such as Google) are not to be used to search for websites or images unless the needs of the lesson specifically demand it.

**School network and Pupil Files**

Always respect the privacy of files of other users. Do not enter the file area of other users without obtaining their permission first. Files to be shared should be saved to the shared area. Pupils can access and save work to their own log on through the server. Do not modify or delete files of other users on the shared areas without obtaining permission from them first.

The ICT coordinator will view any material pupils store on the school’s computers. Storage space on the network is limited. All users are requested to ensure that old unused files are removed from their area at the end of each academic year.

Users accessing software or any services available through school facilities must comply with license agreements or contracts relating to their use and must not alter or remove copyright statements. Some items are licensed for educational or restricted use only.

**Security Guidelines**

**Backups**

Files stored on the network are backed up every evening. This means files can be restored if deleted or lost in error. However, if you create and delete files on the same day then a backup will not be available to restore. Backups are kept securely on the school site in a fire proof room.

**Save Regularly**

It is important to save work regularly (approximately every 10 minutes). The network is reliable but problems do occur i.e. programs crash, power failures. If work is saved regularly and a PC or network does fail for any reason, only the work done since the last save will be lost.

Laptops, USB sticks, Ipads may be taken off site. Staff are to ensure that they are used cautiously when viewing pupil data/information and images and that devices are logged off when left unattended. Images must be transferred to the school network as soon as possible to be removed with the set timescales. Data, images and pupil information must be removed from backups and devices when pupils transfer to another class to avoid records being kept of pupils that are not taught by their former teacher.

**Virus Checks**

All computers in school have anti-virus software, although very new viruses will not be found. If you suspect a virus please report it to the ICT Co-Ordinator straight away.

**Email Usage**

Use of email and communication by email should be treated with the same degree of care that you take if you wrote a letter to the person that you are contacting by email. It cannot be regarded as purely private, only to be seen by the receiver. Email can be stored, forwarded and distributed to large numbers of people at the touch of a button. It is easy to forget that it is a permanent form of written communication and that material can be recovered even if seen to be deleted from the computer.

When using email, staff should:

Not access personal emails in school using school equipment.

Be aware that email is not a secure form of communication and therefore pupils should not send any personal information.

Should not attach large files.

Must not forward email messages onto others unless the sender’s permission is first obtained.

Must not open email attachments from unknown senders or from computers from which virus protection may not be current or activated.

Not send email messages in the heat of the moment and avoid writing anything that may be construed as defamatory, discriminatory, derogatory, rude or offensive.

**Mobile devices**

Pupils are not permitted to bring mobile phones or devices into school. Should there be a need for a child to bring their device in to school this should be turned off and handed to the school office to look after during the school day and collected at 2.55pm.

Mobile phones may not be used to take pictures of pupils and staff (unless class camera provided by the school).

Any inappropriate use of mobile devices such as cyber bulling must be reported to the headteacher.

Staff should only use their mobile phones at appropriate times of the day e.g. break times. During the school day their mobiles should be turned off or set to silent. Staff must not use personal mobile devices or cameras to take images of pupils or staff.

**IPads**

On receipt of the IPad staff are required to read and sign the ‘Staff Mobile Device Policy’.  Staff should not leave the device unattended and must be kept secured when not in use.

Should a member of staff leave the employment of the school, the device must be returned in its original box.

**Legal requirements**

Users must agree to comply with all software license agreements. Do not attempt to copy any software from, or by using school computers. If you have any requirements for using additional software for any reason, please contact the ICT coordinator to discuss. Computer facilities shall not be used to hold or process personal data except in accordance with the provisions of the Data Protection Act.

Copyright Designs and Patents Act – copyright is infringed if a person acquires an unauthorized copy of a computer program. Mere acquisition, without regard to the actual or intended use, constitutes an infringement of the author’s copyright.

**Sanctions**

If staff break the rules as laid down in this policy, they will lose temporary or permanent use of the school systems and may be subject to disciplinary proceedings. If the law has been broken the police will be informed and the school will assist the police with any prosecution.

**Video conferencing and webcams**

The use of webcams to video conference (zoom) will be via firewall which is a filtered service. Publicly accessible webcams are not used in our school setting. Taking images via a webcam should follow the same procedures as taking images with a digital or video camera.

Permission should be sought from parents/careers if their child is engaged in video conferencing with individuals or groups outside of the school. This process should always be supervised by a member of staff.

Managing allegations against adults who work with children and young people

Allegations made against a member of staff should be reported to the headteacher. In the event of an allegation being made against the headteacher, the Chair of Governors should be notified immediately.

Disciplinary Procedure for all school-based staff.

In the event that a member of staff may be seen to be in breach of behavior and good conduct through misuse of online technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behavior and comply with the rules of the governing body.

Additional Information

Please be aware, at such time that you leave **BISK**, your user account and any associated files, your email address and any associated emails will be removed from the school system and will no longer be accessible. The school cannot continue to receive emails sent to your email address.

**Acceptable Use Agreement for Staff**

All adults within the school must be aware of their safeguarding responsibilities when using any online technologies, such as the internet, email or social networking sites. They are asked to sign this agreement so that they provide an example to children and young people for the safe and responsible use of online technologies. This will educate inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

* I know that I must only use the school equipment in an appropriate manner and for professional uses.
* I understand that I need to obtain/check permissions for children and young people before they can upload images to the internet.
* I know that images should not be inappropriate or reveal any personal information of children.
* I have read the procedures for incidents or misuse in the ICT Acceptable Use Policy so that I can deal with any problems that may arise, effectively.
* I will report accidental misuse.
* I will report any incidents of concern for a child’s safety to the headteacher or the nominated Child Protection Officer.
* I know who the nominated Child Protection Officers are.
* I know that I am putting myself at risk of misinterpretation and allegation should I contact children via personal technologies, including my personal email. I know I should use the school email address and telephones to contact parents.
* I know that I must not use the school system for personal use unless this has been agreed by the headteacher.
* I know that I should complete virus checks on my laptop, memory sticks or any other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
* I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
* I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the headteacher or ICT coordinator prior to sharing this information.
* I will adhere to copyright and intellectual property rights.
* I will only install hardware and software I have been given permission for.
* I accept that the use of any technology designed to avoid or bypass the school filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.

Should I be a member of social networking sites, I will keep my profile secure and will avoid contact with parents, pupils and/or ex pupils related to the school. I understand that any action or comment made by myself that brings the school or colleagues into disrepute or compromises pupil or staff confidentiality will be classed as a disciplinary matter.

I have read, understood and agree with this Agreement as I know that by following them, I have a better understanding of e-safety and my responsibilities to safeguard children and young people when using online technologies.

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date: \_\_\_\_\_\_\_\_\_

Name (printed): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_