****

**Email and Internet Use Policy**

**1. Introduction**

1.1 Schools are using E‐mail and the Internet more and more to support their activities. This E‐mail and Internet use policy, which will form part of our ICT Security Policy, contains the rules for using the E‐mail and Internet facilities. It applies to all school staff and students who use either or both of these facilities.

1.2 As well as saying what you are not allowed to use E‐mail and the Internet for, the policy also provides guidance on the good practices that you should use, and the practices that you should avoid.

* 1. The school will periodically review the policy in response to guidance issued by the County Council.

**2. Access to Email and Internet services**

2.1 Your connection to E‐mail or the Internet must be authorised (in writing or in electronic form) by your Director of Business & Finance or Senior ICT Technician. All school Internet access will be via an approved Internet Service Provider (ISP). Any variations to this must be authorised in writing by the Headteacher.

2.2 The school E‐mail and Internet facilities are for business use but we will allow staff to use them privately, as long as it is reasonable.  If you use these facilities, you must keep to and not break any of the conditions in this policy.

2.3 You may not attempt to bypass firewalls and access rules in place. This includes not setting up servers of any kind (examples: web, mail, proxy) that are visible to the world outside the school network. In critical situations the system manager reserves the right to disconnect any device or disable any account if it believed that either is involved in compromising the information security of the School.

2.4 The school has the right to monitor E‐mails and Internet use.

2.5 If you intentionally access a computer system or information without permission, you are breaking the law under the Computer Misuse Act 1990.

**3. Code of Conduct Declaration**

3.1 If you use or have access to our E‐mail or Internet facilities, you need to read this policy carefully and make sure that you understand it.  The school will provide appropriate training where required.  You then need to sign the declaration / consent form to confirm that you have read, understood and will keep to the policy.  You must also understand that we may take action against you if you wilfully break the conditions of the policy.

3.2 The school will keep the signed declaration in the IT Support Office.  Sometimes, we may ask you to confirm that you still understand and accept the rules.

**4. Specific Conditions of Use**

**4.1 General prohibitions**

4.1.1 You must not use, or try to use, our E‐mail and Internet facilities to create, distribute or display in any form, any activity that is or may be considered to be against the law or against our rules and policies.  In this context, you are not allowed to use the E‐mail and Internet facilities for reasons that are:

* pornographic or obscene;
* intimidating, discriminatory (for example; racist, sexist or homophobic) or that break our anti‐harassment and equal opportunities policies in any other way;
* defamatory;
* encouraging violence or strong feelings;
* hateful;
* fraudulent;
* showing or encouraging violence or criminal acts;
* unethical or may give the school a bad name; or
* a deliberate harmful attack on systems we use, own or run.

4.1.2 We will only allow you to do the above if:

* it is part of your job to investigate illegal or unethical activities;
* your Headteacher or Director of Business & Finance or Senior ICT Technician asks you to in writing; or
* it is in the public interest.

You must make sure that your Director of Business & Finance or Senior ICT Technician knows what you are doing.  If you find or suspect anyone of using the computer system illegally or unethically, you must report it to your System Manager who will advise your Headteacher or Chair of Governors or Internal Audit.

4.1.3 You must not use the school E‐mail or Internet facilities for time‐wasting activities, such as chain letters, or for sending private E‐mails to everyone on the global address list.

**4.2 Computer viruses**

4.2.1 Under the Computer Misuse Act 1990, it is a criminal offence to deliberately introduce a computer virus to any system.

You must not use the school E‐mail and Internet facilities for:

* Intentionally accessing or transmitting computer viruses or other damaging software; or
* Intentionally accessing or transmitting information about, or software designed for, creating computer viruses.

4.2.2 You must scan any material you receive or download from the Internet to make sure it is virus free.  The school will ensure that virus protection exists on any standalone or locally networked computers that can access the Internet and train you in its use.  You must not E‐mail material that has not been scanned to other users. If you find a virus, or you think the material has one, you must immediately break the connection, stop using the computer and tell your System Manager.

4.2.3 You must always follow the instructions that your Director of Business & Finance or Senior ICT Technician gives you about virus attacks.

4.2.4 If you are not sure how to use the virus protection system, you must get advice from your Director of Business & Finance or Senior ICT Technician.

**4.3 Passwords**

4.3.1 You must not tell anyone your password, apart from authorised staff if required.

4.3.2 You must change your password every half term.

**4.4 Other security**

4.4.1 You must not use or try to use the school facilities for:

* accessing or transmitting information about, or software designed for, breaking through security controls on any system;
* breaking through security controls on any system; or
* accessing, without permission, any E‐mail that is not for you, even if it is not protected by security controls.

**4.5 Publishing information**

4.5.1 You must get authorisation from the Headteacher for any school information that is to be published on the Internet.  All schools have web space available for authoring of their own school web site and virtual learning environment. Images of individuals must have their permission or that of their parent/guardian before publication of the web site. We will not allow the publishing or editing of Web sites which involve advertising, financial reward or are part of a business.

**4.6 Copyright**

4.6.1 It is illegal to break copyright protection. You could break copyright if you download or transmit protected material through E‐mail or over the Internet.

4.6.2 You must not:

* Transmit copyright software from your computer to the Internet or allow any other person to access it on their computer through the Internet; or
* Knowingly download or transmit any protected information that was written by another person or organisation without getting permission from the owner.

*Permission can be sought via e‐mail.*

**4.7 Confidential or sensitive information**

4.7.1 You must not break the conditions of the Data Protection Act 1998 when you use the E‐mail services of the Internet for transmitting information.

*If you need any more advice about these conditions, you should refer to the Policy summary or obtain further information/advice from the Director of Business & Finance or Senior ICT Technician.*

4.7.2 The Internet E‐mail facility is not a secure way of transmitting confidential, sensitive or legally privileged information unless there are special security measures (such as encryption).  Without these security measures, Internet E‐mail is as insecure as a postcard that you send through the normal post.  So, you should make sure that the Internet is suitable for transmitting information that you feel is confidential, sensitive or legally privileged.  If you allow anyone to see this type of information without permission, you may be breaking the law.

4.7.3 If you have to transmit any E‐mail over the Internet that you think contains confidential, sensitive or legally privileged information, no matter what special security measures you take, you are strongly advised to include the following disclaimer in the E‐mail.

*‘This communication contains information which is confidential and may also be privileged. It is for the exclusive use of the addressee. If you are not the addressee please note that any distribution, reproduction, copying, publication or use of this communication or the information in it is prohibited. If you have received this communication in error, please contact us immediately and also delete the communication from your computer’.*

This disclaimer can be set using the ‘autosignature’ facility where this is available.

**4.8 Forums**

4.8.1 There are forums on the Blythe Bridge High School & Sixth Form Virtual Learning Environment (Frog) for discussion, social and personal use. These ‘bulletin boards’ are moderated to ensure appropriate use. The conditions of use in this policy also apply to the bulletin boards.

4.8.2 Neither the school, the LEA nor the County Council is responsible for the content of any material included in the bulletin board or for anything users do because of the material.

**5 Recording internet use**

5.1 You should be aware that use of Internet facilities are logged.

5.2 If you access a prohibited Internet site unintentionally, you must break the connection immediately and report it to your Director of Business & Finance or Senior ICT Technician or Headteacher.  If you do not do this, the school may take action against you.

5.3 You should protect yourself by not allowing unauthorised people to use your Internet Facility.

**6 Email good practice**

6.1 The Acceptable usage policy in the staff handbook contains guidelines that tell you what is and what is not good practice when you use internal or Internet E‐mail services.

**7. E-Safety**

E-Safety aims that children and young people are:

* Safe from maltreatment, neglect, violence and sexual exploitation
* Safe from accidental injury and death
* Safe from bullying and discrimination
* Safe from crime and anti-social behaviour in and out of school
* Secure, stable and cared for.

Much of these aims apply equally to the ‘virtual world’ that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the ‘virtual’ or digital world as would be applied to the school’s physical buildings.

This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

### 7.1 The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

* The Internet
* e-mail
* Instant messaging (<http://www.msn.com>, <http://info.aol.co.uk/aim/>) often using simple web cams
* Blogs (an on-line interactive diary)
* Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
* Social networking sites (Popular [www.myspace.com](http://www.myspace.com) / [www.piczo.com](http://www.piczo.com) / [www.bebo.com](http://www.bebo.com) / <http://www.hi5.com> / [www.facebook.com](http://www.facebook.com))
* Video broadcasting sites (Popular: <http://www.youtube.com/>)
* Chat Rooms (Popular [www.teenchat.com](http://www.teenchat.com), [www.habbohotel.co.uk](http://www.habbohotel.co.uk))
* Gaming Sites (Popular [www.neopets.com](http://www.neopets.com), <http://www.miniclip.com/games/en/>, <http://www.runescape.com/>)
* Music download sites (Popular <http://www.apple.com/itunes/> <http://www.napster.co.uk/> <http://www-kazzaa.com/>, <http://www-livewire.com/>)
* Mobile phones with camera and video functionality
* Smart phones with e-mail, web functionality and cut down ‘Office’ applications.

### 7.2 Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

* An effective range of technological tools;
* Policies and procedures, with clear roles and responsibilities;
* A comprehensive e-Safety education programme for pupils, staff and parents.

### 7.3 Roles and Responsibilities

e-Safety is recognised as an essential aspect of strategic leadership in this school and the Headteacher, with the support of Governors, aims to embed safe practices into the culture of the school. The headteacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to a member of the senior management team.

Our school **e-Safety Co-ordinator** is currently Mrs Owen – SENCO & Designated Child Protection Officer

Our e-Safety Coordinator ensures they keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and through organisations such as The Child Exploitation and Online Protection (CEOP). The school’s e-Safety coordinator ensures the Head, senior management and Governors are updated as necessary.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on e-Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a ‘No Blame’ culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools’ Policy including:

* Safe use of e-mail
* Safe use of Internet including use of [internet](http://safety.ngfl.gov.uk/schools/)-based communication services, such as instant messaging and social network
* Safe use of school network, equipment and data
* Safe use of digital images and digital technologies, such as mobile phones and digital cameras
* Publication of pupil information/photographs and use of website
* eBullying / Cyberbullying procedures
* Their role in providing e-Safety education for pupils
* Staff are reminded / updated about e-Safety matters at least once a year.

### 7.4 How will complaints regarding e-Safety be handled?

The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

* Interview/counselling by tutor / Head of House / e-Safety Coordinator / Headteacher;
* Informing parents or carers;
* Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
* Referral to Local Authority / Police.

Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.