Statutory Policy

On

ICT Whole School Policy Suite

Drafted by:
Business & Operations Manager
Data Manager
Senior ICT Technician

_____

Date of Approval by Governing Body:
TBC

_____

Signed By Chair of Governors:

_____

Review date:
May 2020

_____

Person(s) Responsible for Day to Day Management:
Business & Operations Manager

_____

Person Responsible for Review:
Business & Operations Manager

BLYTHE BRIDGE HIGH SCHOOL & SIXTH FORM
A FOUNDATION TRUST SCHOOL

Acceptable Use Policy

1. You must always follow the schools e-safety policy in order to keep yourself and others safe online.

2. The work/activity on the Internet must be directly related to your schoolwork. Private use of the Internet including chat software, social networking websites (e.g. Facebook, Twitter, etc…), games or web-based email services (e.g. Hotmail) is strictly forbidden unless given express permission to do so.

3. Any student found to be damaging or interfering with IT equipment or recording systems monitoring IT equipment, will be punished appropriately and may be charged for any costs incurred during repair (see below).

4. Do not disclose any password or login name you have been given **to anyone**. On a network, students will use only their own login and password, which should be kept private. Under no circumstances should a student log into or in any way access another users account.

5. Use of names or photographs of students will require written permission of parent(s)/guardian(s). This can be found in the student planner.

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

7. Under no circumstances should you view, upload or download any material that is likely to be unsuitable for use in schools. This applies to any material of a violent, dangerous, racist or with inappropriate sexual content. If you are not sure about this, or any materials, you must ask a teacher.

8. Always respect the privacy of files of other users. Do not enter the file areas of other students or staff. Work that needs to be accessed in other work areas must only be done by the Senior ICT Technician under the instruction of the Business Manager, in the absence of the Business Manager; the Senior ICT Technician must seek approval from The Headteacher's PA.

9. The IT support department has the right to view any material held on the school network. This right will only be used ethically, for E-Safety reasons and/or at the request of the senior members of staff.

10. Be Polite and appreciate that other users might have different views other than your own. Use of strong language, swearing or aggressive behaviour is not allowed.

11. Do not state anything that could be interpreted as libel.

12. Do not copy any work off the Internet or from other students and try to distribute it as your own (Plagiarism).

13. Under no circumstances is anyone to 'Hack' into any part of the network, or obtain other users logon details by any means.

14. Students will not look at, change or delete other people's files.

15. Under no circumstances should a student create a social media account that in any way impersonates any member of staff, the School or the Sixth Form.

16. All sensitive data stored on portable storage devices such a USB pens or portable hard drives must be stored securely using encryption. A guide to do this is available on the VLE or assistance can be requested from the Senior IT Technician.

17. Failure to comply with these rules will result in one or more of the following

- A ban, temporary or permanent, on the use of the internet facilities or network facilities at school
- A letter informing parents of the nature and breach of rules.
- Appropriate sanctions and restrictions placed on access to school facilities to be decided by the head of year/ICT Coordinator/E-Safety Officer/Headteacher.
- Where damaged has been caused, any expense incurred may be charged to the offender.
- Any other action decided by the head of governors of Blythe Bridge High School and Sixth Form.

BLYTHE BRIDGE HIGH SCHOOL & SIXTH FORM
A FOUNDATION TRUST SCHOOL

Consent Form for BYOD

E-Safety Policy

Please complete, sign and return to the IT Support Office

Name:	***Position:***

Declaration
You must read, understand and sign this form if you use our ICT facilities and services. We will keep the completed form in our signed declarations file.

Declaration
I confirm that, as an authorised user of the School's ICT facilities, I have read, understood and accepted all of the conditions in the E-Safety Policy and BYOD Policy.

Signed:	***Date:***
Device Description:	***MAC Address:***

Notes:

BLYTHE BRIDGE HIGH SCHOOL & SIXTH FORM
A FOUNDATION TRUST SCHOOL

Bring Your Own Device Policy

The use of a device in connection with Blythe Bridge High School and Sixth Form is a privilege granted to stakeholders through approval of the school. Blythe Bridge High School and Sixth Form reserves the right to revoke these privileges in the event that users do not abide by the policies and procedures set out below.

The following policies are aimed to protect the integrity of Blythe Bridge High School and Sixth Form data and ensure it remains safe and secure under Blythe Bridge High School and Sixth Form control. Please note that there may be limited exceptions to these policies owing to device limitations between vendors.

References to the word "device" below includes, but is not limited to, Android, BlackBerry, iPhone, iPad, tablet, Windows mobile or other devices.

Users of Personal Devices must agree to all terms and conditions in this policy to be allowed access to those Blythe Bridge High School and Sixth Form services.

• Irrespective of security precautions mentioned here, you are expected to use your device in an ethical manner and in accordance with the Blythe Bridge High School and Sixth Form E-Safety Policy.
• Your device must lock itself with a PIN (personal identification number set by you)
• If left idle, your device must automatically activate its PIN after a maximum time-out period of 5 minutes
• In the event of a change, loss or theft of your device, you must inform Blythe Bridge High School and Sixth Form within 3 working days so we can update our records and systems.

<u>Tampering</u>

Using your device in ways not designed or intended by the manufacturer is not allowed. This includes, but is not limited to, 'jailbreaking' or 'rooting' your device.

<u>Liability</u>

A personal device can be connected to the Blythe Bridge High School and Sixth Form infrastructure or services, but the user is personally liable for their device and carrier service costs. Users of personal devices are not eligible (except by prior agreement) for reimbursement of expenses for hardware or carrier services.

Access

Employees that purchase a device on their own that is not in line with our standard approved device lists may not be able to or allowed to have their devices added to our network. Users of personal devices are not permitted to connect to Blythe Bridge High School & Sixth Form network without documented consent from the IT support department. Furthermore, Blythe Bridge High School & Sixth Form reserves the right to disable or disconnect some or all services without prior notification.

Disclaimer

Blythe Bridge High School and Sixth Form hereby acknowledge that the use of a personal device in connection with school use carries specific risks for which you, as the user, assume full liability. These risks include, but are not limited to, the partial or complete loss of data as a result of a crash of the operating system, errors, bugs, viruses, downloaded malware, and/or other software or hardware failures, or programming errors which could render a device inoperable.

BLYTHE BRIDGE HIGH SCHOOL & SIXTH FORM
A FOUNDATION TRUST SCHOOL

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.

1.3 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 System Manager. 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 System Manager asks you to in writing; or**
- **it is in the public interest.**

You must make sure that your System Manager 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 It is a crime to deliberately introduce a computer virus, under the Computer Misuse Act 1990. 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 System Manager 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 System Manager.

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 System Manager.

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 and 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 System Manager 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)**
- **Snapchat / Whatsapp**
- **Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)**

- **Social networking sites (Popular www.myspace.com / www.piczo.com / www.bebo.com / http://www.hi5.com / www.facebook.com)**
- **Video broadcasting sites (Popular: http://www.youtube.com/)**
- **Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)**
- **Gaming Sites (Popular 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 & Designate 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-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 LA / 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.

Equipment Loan

Name:

_____

_____

Description:

_____

_____

Contact number:

_____

_____

Blythe Bridge High School and Sixth Form have provided the following equipment for educational purposes and withhold the right to withdraw the equipment at any time.

Item Type	Make and Model	Serial Number
Additional Notes		

The equipment above has been loaned to me by Blythe Bridge High School and Sixth Form. I undertake to look after it with great care and

return it in like condition when it is either no longer required or I no longer work for the School. If the equipment is lost or damaged I will inform the ICT Support Department immediately.

I have read and agree to abide by the above guidelines for the equipment loaned to me.

Device User Signature: _____ Date:_____

Authorised Signature: _____ Date:_____

ICT Security Policy

The objectives of the Policy, which is intended for all school staff, including governors , who use or support the school's ICT systems or data, are to:

- **Ensure the protection of confidentiality, integrity and availability of school information and assets.**
- **Ensure all users are aware of and fully comply with all relevant legislation.**
- **Ensure all staff understands the need for information and ICT security and their own responsibilities in this respect.**

The integrity of the Staffordshire schools' network depends on the security policy implemented by each connected school. Information covers any information, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created.

The school's Senior ICT Technician is responsible for the school's ICT equipment, systems and data with direct control over these assets and their use, including responsibility for access control and protection. The Senior ICT Technician will be the official point of contact for ICT or information security issues.

Responsibilities:

- ✓ **Users of the school's ICT systems and data must comply with the requirements of the ICT Security Policy**
- ✓ **Users are responsible for notifying the Senior ICT Technician of any suspected or actual breach of ICT security. In the absence of the Senior ICT Technician, users should report any such breach directly to the Business Operations Manager or Data Manager.**
- ✓ **Users must comply with the requirements of the Data Protection Act 1998, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988 and the Telecommunications Act 1984.**
- ✓ **Users must be provided with suitable training and documentation, together with adequate information on policies, procedures and facilities to help safeguard systems and data.**
- ✓ **Adequate procedures must be established in respect of the ICT security and implications of personnel changes.**

Physical Security:

- ✓ **As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data.**
- ✓ **Server rooms must be kept locked when unattended.**
- ✓ **Appropriate arrangements must be applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.**

- ✓ **All school owned ICT equipment and software should be recorded and an inventory maintained.**
- ✓ **Uninterruptible Power Supply (UPS) units are recommended for servers and network cabinets.**
- ✓ **Computer monitors should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons.**
- ✓ **Equipment should be sited to avoid environmental damage.**
- ✗ **Do not leave sensitive or personal data on printers, computer monitors or desk whilst away from your desk or computer.**
- ✗ **Do not give out sensitive information unless the recipient is authorised to receive it.**
- ✗ **Do not send sensitive/personal information which may be deemed confidential via e-mail or post without suitable security measures being applied.**
- ✓ **Ensure sensitive data, both paper and electronic, is disposed of properly, e.g. shred paper copies and destroy disks.**

System Security:

- ✗ **Users must not make, distribute or use unlicensed software or data.**
- ✗ **Users must not make or send threatening, offensive or harassing messages.**
- ✗ **Users must not create, possess or distribute obscene material.**
- ✓ **Users must ensure they have authorisation for private use of the school's computer facilities.**
- ✓ **The Senior ICT Technician will determine the level of password control.**
- ✓ **Passwords should be memorised. If passwords must be written down they should be kept in a secure location.**
- ✗ **Passwords should not be revealed to unauthorised persons.**
- ✗ **Passwords should not be obvious or guessable and their complexity should reflect the value and sensitivity of the systems and data**
- ✓ **Passwords should be changed at regular intervals; this is enforced by the ICT network at logon.**
- ✓ **Passwords must be changed if it is affected by a suspected or actual breach of security, e.g. when a password may be known by an unauthorised person.**
- ✓ **Regular backups of data, in accordance with the recommended backup strategy, must be maintained.**
- ✓ **Security copies should be regularly tested to ensure they enable data restoration in the event of system failure.**
- ✓ **Security copies should be clearly marked and stored in a fireproof location and/or off site.**

Virus Protection:

- ✓ **The Senior ICT Technician will ensure current and up to date anti-virus software is applied to all fixed school ICT systems.**
- ✓ **Laptop users must ensure they update their virus protection at least weekly, this is done by simply connecting the device to the schools network.**
- ✓ **The Senior ICT Technician will ensure operating systems are updated with critical security patches as soon as these are available.**
- ✓ **Any suspected or actual virus infection must be reported immediately to the Senior ICT Technician.**

Disposal and Repair of Equipment:

- ✓ **The Senior ICT Technician must ensure any personal data or software is obliterated from a PC if the recipient organisation is not authorised to receive the data.**
- ✓ **It is important to ensure that any software remaining on a PC being relinquished are legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.**
- ✓ **The Senior ICT Technician must ensure the requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed**
- ✓ **The school will ensure that third parties are registered under the Data Protection Act as personnel authorised to see data and such are bound by the same rules as school staff in relation to not divulging the data or making any unauthorised use of it.**
- ✓ **All empty Toner and Ink Cartridges will be disposed in an environmentally friendly manner where possible. As will other ICT consumables such as printer parts and batteries.**

Security Incidents:

All suspected or actual breaches of the ICT security, including detection of computer viruses, must be reported to the Senior ICT Technician or Business Manager in their absence, who should report the incident immediately to Codsall ICT Support/Help Desk.

BLYTHE BRIDGE HIGH SCHOOL & SIXTH FORM
A FOUNDATION TRUST SCHOOL

Mobile Device Policy

- **Blythe Bridge High School and Sixth Form has entrusted you for use with this Mobile Device to aid teaching and learning and expects it to be treated with due care and diligence.**
- **It is your responsibility to ensure that all personal data stored on the device is adequately backed. As data will be lost in the event of hardware failure. We recommend you use the VLE, Email or Remote Desktop where possible in order to ensure your data is stored on the school network.**

- **If a device needs to have its software reinstalled, any and all software and data, over and above that on the machine at the time of issue, will be lost.**

- **Any additional software installed by the user should only be done in compliance with the licensing conditions of that software. It is your responsibility to ensure that the machine remains in a legal state after issue by Blythe bridge High School and Sixth Form and Sixth Form.**

- **Any hardware installed after issue of the device by the school will be the responsibility of the user (e.g. Printers etc…). Ensure only the correct manufacturers' drivers are installed.**

- **Any data stored should be done so in accordance with the Data Protection Act, details of which are stored in the IT office.**

- **You must protect your device with a username/password or equivalent (ie, pin) in order to keep personal data secure. This information must remain secret and not written down and placed with the device.**

- **Under no circumstances should you view, upload or download any material that is likely to be unsuitable for children. This applies to any material of a violent, dangerous or sexual content.**

- **It is your responsibility to keep the device virus free. Please refer to the IT Support Team for assistance, if needed, for best practice on various devices.**

- **Under no circumstances should you use the device to download any software or music illegally either through the use of P2P (peer to peer) clients, bit torrent software or other means. Priority will not be given to infected devices where P2P and/or bit torrent software is installed and/or virus prevention is nonexistent.**

- **The device is configured to allow the use of the Internet within the school. Please be aware of the standard E-Safety policy and follow at all times.**

- **Devices are distributed for staff use. No students/3rd Parties, including family members, are to be allowed to use a staff device unsupervised.**

- **The school will require the return of devices at regular interval for maintenance/servicing purposes, staff must return devices when requested to do so.**

- **All equipment loaned for staff use must be signed for on the** Equipment Loan **or** Mobile Device consent **form.**

- **Blythe Bridge High School and Sixth Form reserves the right to place restrictive access or in extreme cases remove the device if the above is not followed.**

BLYTHE BRIDGE HIGH SCHOOL & SIXTH FORM
A FOUNDATION TRUST SCHOOL

Consent Form for Mobile Device

E-Safety Policy

Please complete, sign and return to the IT Support Office

Name:	***Position:***

Declaration
You must read, understand and sign this form if you use our ICT facilities and services. We will keep the completed form in our signed declarations file.

Declaration
I confirm that, as an authorised user of the School's ICT facilities, I have read, understood and accepted all of the conditions in the E-Safety Policy and Mobile Device Policy.

Signed:	***Date:***
Device Description:	***MAC Address:***

Notes:

E-Safety Policy

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. The School policies will be monitored each year and adapted where necessary to fit in with new technology.

2. Whole School approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at Blythe Bridge High School & Sixth Form:

- An effective range of technological tools (Sophos, Proxy Filters & Impero);
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-Safety education programme for pupils, staff and parents.

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 Senior ICT Technician ensures that the Policy is implemented and compliance with the Policy monitored.

Our school **e-Safety Co-ordinator** is Mrs S Owen

All students, staff and Governors should be familiar with the following ICT policies:

- **ICT. Email Internet Acceptable Use Policy (School Planners, Form rooms and School Website)**
- **ICT. Virtual Learning Policy (AUP on login to Frog – Failure to accept will not allow access)**
- **ICT. Social Media Code of Conduct**
- **ICT. ICT Security Policy**
- **ICT. Acceptable User Policy (Will appear on Network Computers before log on)**
- **ICT. Acceptable Use of Mobile Devices Policy (If issued with school device)**
- **ICT. BYOD Policy (If you have been granted permission to use a personal device at school)**

All policies are made available through the VLE or can be provided on request from IT Support Office.

4. Communications

How will the policy be introduced to pupils?
School planners will contain the relevant ICT policies for students to read and sign to accept they have read and understood them. These will be checked by form tutors and recorded electronically in the IT Support Office for viewing by staff at request.

How will the policy be discussed with staff?
All policies will be made available on the VLE for download and viewing. Any changes to the E-Safety policy will result in new Acceptance forms being signed by staff.

How will parents' support be enlisted?
Parents need to read and sign the ICT section of the Student Planner to state they have read and understood the school ICT policies. This also includes the image consent form. Any further information or useful links to sites such as 'thinkuknow' will be made available on the Parent Portal of the school VLE under the e-Safety section.

5. 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 LA / Police.

Our e-Safety Coordinator acts as first point of contact for any complaint and will work closely with the Head of house and Senior ICT Technician to rectify the issue. Any complaint about staff misuse is referred to the Headteacher.

Acceptable Use Policy

1. You must always follow the schools e-safety policy in order to keep yourself and others safe online.

2. The work/activity on the Internet must be directly related to your schoolwork. Private use of the Internet including chat software, social networking websites (e.g. Facebook, Twitter, etc…), games or web-based email services (e.g. Hotmail) is strictly forbidden.

3. Any student found to be damaging IT equipment will be punished appropriately (see below).

4. Do not disclose any password or login name you have been given **to anyone**.

5. Use of names or photographs of students will require written permission of parent(s)/guardian(s). This can be found in the student planner.

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

7. Under no circumstances should you view, upload or download any material that is likely to be unsuitable for use in schools. This applies to any material of a violent, dangerous, racist or with inappropriate sexual content. If you are not sure about this, or any materials, you must ask a teacher.

8. Always respect the privacy of files of other users. Do not enter the file areas of other students or staff. Work that needs to be accessed in other work areas must only be done by the Senior ICT Technician under the instruction of the Director of Business and Finance, in their absence; the Senior ICT Technician must seek approval from The Headteacher's PA.

9. The IT support department has the right to view any material held on the school network. This right will only be used ethically, for E-Safety reasons and/or at the request of the senior members of staff.

10. Be polite and appreciate that other users might have different views other than your own. Use of strong language, swearing or aggressive behaviour is not allowed.

11. Do not state anything that could be interpreted as libel.

12. Do not copy any work off the Internet or from other students and try to distribute it as your own (Plagiarism).

13. Under no circumstances is anyone to 'Hack' into any part of the network, or obtain other users logon details by any means.

14. Failure to comply with these rules will result in one or more of the following
- A ban, temporary or permanent, on the use of the internet facilities at school
- A letter informing parents of the nature and breach of rules.
- Appropriate sanctions and restrictions placed on access to school facilities to be decided by the Head of House/ICT Coordinator/E-Safety Officer/Headteacher
- Any other action decided by the Chair of Governors of Blythe Bridge High School & Sixth Form.

If you do not understand any part of this document, you must ask the Director of Business and Finance, or the Senior ICT Technician.

PARENT/CARER
I have read and understood the information above:

Name of child _____ Date _____

Parent Name _____ Parent/Carer Signature _____

Blythe Bridge High School
A Foundation Trust School

Virtual Learning Environment (VLE - Frog) Acceptable Use Policy

- **The following policy outlines the terms of use for all users (staff and students) of Blythe Bridge High School & Sixth Form's virtual learning environment (Frog).**
- **All Blythe Bridge High School & Sixth Form staff and students are granted access to Frog to facilitate learning and teaching. Access is conditional upon agreement with school regulations and all relevant UK laws.**
- **Failure to comply may result in loss of privileges. In cases where UK law has been violated, users could face criminal and/or civil liability.**

Acceptable Use
Blythe Bridge High School & Sixth Form expects and requires that its users act responsibly and considerately, and respect the rights of other Frog users at all times.

Unacceptable Use

Any users that infringe the policy, behave inappropriately online, or adversely affect Blythe Bridge High School & Sixth Form's online learning communities will be denied access to Frog. The following constitutes unacceptable use of Frog:

1. **Unauthorised use of another person's login details to gain access to the Frog system.**
2. **Unauthorised reading, copying, modification, or corruption of another users files, communications, or data.**
3. **Attempts to undermine the security or integrity of Frog and related systems/software.**
4. **Posting or using material that infringes copyright and intellectual property rights. If you are unsure whether Blythe Bridge High School & Sixth Form owns a particular licence to reproduce materials, you should contact the Senior ICT Technician or Director of Business and Finance for confirmation.**
5. **Creation or transmission of any materials that are considered offensive, obscene, or indecent.**
6. **Creation and transmission of materials/communications that include profanity, vulgarity, hate speech, disruptive or hostile comments, interpersonal disputes, or threats of violence.**
7. **Discussing or re-posting materials/communications that have been deemed inappropriate and removed by the school.**
8. **Creation and transmission of materials, or taking actions, that interfere with Frog operations.**
9. **Including another user's contact details or personal information in materials/communications without express permission from the individual concerned.**
10. **Refusing to adhere to the schools IT and conduct policies, procedures and agreements.**
11. **Using Frog for commercial purposes or financial gain without express approval from Blythe Bridge High School & Sixth Form.**
12. **Violating the privacy and confidentiality of other users.**

Additional Notes

- **All users are responsible for their activities on the Frog system and for the content of their uploaded materials and communications (via chat rooms, email or discussion forums).**
- **The school aims to remove any inappropriate materials as soon as possible after they are discovered or reported and will deal with inappropriate use or behaviour of Frog swiftly and rigorously within the guidelines of the school's disciplinary procedures.**

I have read and understand the information above:

Name:	**Signature**	**Date**

School Image Consent Form

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make any recordings of your child.

Conditions of use:

1. This form is valid for the period of time your child attends this school. Images of your child will not be used after this time. Please write to the school if you wish to withdraw consent at any time.

2. The images we take will be of activities that show the school and children in a positive light.

3. Embarrassing or distressing images will not be used. The images will not be associated with negative or sensitive issues.

4. We may use group or class photographs or footage with very general labels e.g. 'science lesson'.

5. We will only use images of pupils who are suitably dressed.

6. We will make every effort to ensure that we do not allow images to be taken of any children for whom we do not have permission or who are 'at risk' or disallowed from having their photographs taken for legal or social reasons.

7. We will take all reasonable measures to ensure the images are used solely for the purposes for which they are intended. However we cannot guarantee this and take no responsibility for the way images are used by other websites or publishers or for any consequences arising from publication.

I give permission for my child's image to be taken and used in publicity material for the school, including printed and electronic publications, video and webcam recordings and on websites.	☐
I give permission for images of my child to be used by the news media in printed and/or electronic form and stored in their archives. This might include images sent to the news media by the school and images / footage the media may take themselves if invited to the school to cover an event.	☐
I do not want my child's image used in any publicity.	☐

PARENT/CARER
I have read and understood the information above:

Name of child	Date
Parent Name	Parent/Carer Signature

Acceptable Use Policy

1. You must always follow the schools e-safety policy in order to keep yourself and others safe online.

2. The work/activity on the Internet must be directly related to your schoolwork. Private use of the Internet including chat software, social networking websites (e.g. Facebook, Twitter, etc…), games or web-based email services (e.g. Hotmail) is discouraged during school hours.

3. Any staff member found to be damaging IT equipment will be subject to the rules of the AUP.

4. Do not disclose any password or login name you have been given **to anyone**.

5. Use of names or photographs of students will require written permission of parent(s)/guardian(s). This can be found in the student planner.

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

7. Under no circumstances should you view, upload or download any material that is likely to be unsuitable for use in schools. This applies to any material of a violent, dangerous, racist or with inappropriate sexual content. If you are not sure about this, or any materials, you must ask the technicians.

8. Always respect the privacy of files of other users. Do not enter the file areas of other students or staff.

9. The IT support department has the right to view any material held on the school network. This right will only be used ethically, for E-Safety reasons and/or at the request of the senior members of staff.

10. Be polite and appreciate that other users might have different views other than your own. Use of strong language, swearing or aggressive behaviour is not allowed.

11. Do not state anything that could be interpreted as libel.

12. Under no circumstances is anyone to 'Hack' into any part of the network, or obtain other users logon details by any means.

13. Failure to comply with these rules will result in one or more of the following

- A ban, temporary or permanent, on the use of the internet facilities at school
- Appropriate sanctions and restrictions placed on access to school facilities to be decided by the ICT Coordinator/E-Safety Officer/Headteacher
- Any other action decided by the Chair of Governors of Blythe Bridge High School & Sixth Form.

If you do not understand any part of this document, you must ask the Director of Business and Finance, or the Senior ICT Technician.

Virtual Learning Environment (VLE - Frog) Acceptable Use Policy

- **The following policy outlines the terms of use for all users (staff and students) of Blythe Bridge High School & Sixth Form's virtual learning environment (Frog).**
- **All Blythe Bridge High School & Sixth Form staff and students are granted access to Frog to facilitate teaching and learning. Access is conditional upon agreement with school regulations and all relevant UK laws.**
- **Failure to comply may result in the loss of privileges. In cases where UK law has been violated, users could face criminal and/or civil liability.**

Acceptable Use

Blythe Bridge High School & Sixth Form expects and requires that its users act responsibly and considerately, and respect the rights of other Frog users at all times.

Unacceptable Use

Any users that infringe the policy, behave inappropriately online, or adversely affect Blythe Bridge High School & Sixth Form's online learning communities will be denied access to Frog. The following constitutes unacceptable use of Frog:

13. **Unauthorised use of another person's login details to gain access to the Frog system.**
14. **Unauthorised reading, copying, modification, or corruption of another users files, communications, or data.**
15. **Attempts to undermine the security or integrity of Frog and related systems/software.**
16. **Posting or using material that infringes copyright and intellectual property rights. If you are unsure whether Blythe Bridge High School & Sixth Form owns a particular licence to reproduce materials, you should contact the Senior ICT Technician or Director of Business and Finance for confirmation.**
17. **Creation or transmission of any materials that are considered offensive, obscene, or indecent.**
18. **Creation and transmission of materials/communications that include profanity, vulgarity, hate speech, disruptive or hostile comments, interpersonal disputes, or threats of violence.**
19. **Discussing or re-posting materials/communications that have been deemed inappropriate and removed by the school.**
20. **Creation and transmission of materials, or taking actions, that interfere with Frog operations.**
21. **Including another user's contact details or personal information in materials/communications without express permission from the individual concerned.**
22. **Refusing to adhere to the schools IT and conduct policies, procedures and agreements.**
23. **Using Frog for commercial purposes or financial gain without express approval from Blythe Bridge High School & Sixth Form.**
24. **Violating the privacy and confidentiality of other users.**

Additional Notes

- **All users are responsible for their activities on the Frog system and for the content of their uploaded materials and communications (via chat rooms, email or discussion forums).**
- **The school aims to remove any inappropriate materials as soon as possible after they are discovered or reported and will deal with inappropriate use or behaviour of Frog swiftly and rigorously within the guidelines of the school's disciplinary procedures.**

I have read and understand the above Virtual Learning Environment acceptable usage policy:

Name:	***Signature***	***Date***

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.

1.4 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 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 school 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 that are 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 Senior ICT Technician 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 Senior ICT Technician asks you to in writing; or**
- **it is in the public interest.**

You must make sure that your 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 Senior ICT Technician who will advise your Headteacher or Chair of Governors.

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 It is a crime to deliberately introduce a computer virus, under the Computer Misuse Act 1990. 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 Senior ICT Technician.

4.2.3 You must always follow the instructions that your 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 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 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 and monitored to ensure appropriate use. The conditions of use in this policy also apply to the bulletin boards.

4.8.2 Neither the school, the LA 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 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.piczo.com / www.bebo.com / http://www.hi5.com / www.facebook.com)**
- **Video broadcasting sites (Popular: http://www.youtube.com/)**
- **Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)**
- **Gaming Sites (Popular 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 & Designate 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-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 LA / 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.

BLYTHE BRIDGE HIGH SCHOOL
SIXTH FORM
A FOUNDATION TRUST SCHOOL

E-Safety Policy

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. The School policies will be monitored each year and adapted where necessary to fit in with new technology.

2. Whole School approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at Blythe Bridge High School & Sixth Form:

- An effective range of technological tools (SECURUS, Proxy Filters & Impero);
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-Safety education programme for pupils, staff and parents.

3. Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The Senior ICT Technician ensures that the Policy is implemented and compliance with the Policy monitored.

Our school **e-Safety Co-ordinator** is Mrs S Owen

All students, staff and governors should be familiar with the following ICT policies:

- **ICT. Email Internet Acceptable Use Policy (School Planners, Form rooms and School Website)**
- **ICT. Virtual Learning Policy (AUP on login to Frog – Failure to accept will not allow access)**
- **ICT. Social Media Code of Conduct**
- **ICT. ICT Security Policy**
- **ICT. Acceptable User Policy (Will appear on Network Computers before log on)**
- **ICT. Acceptable Use of Mobile Devices Policy (If issued with school device)**
- **ICT. BYOD Policy (If you have been granted permission to use a personal device at school)**

All policies are made available through the VLE or can be provided on request from IT Support Office.

4. Communications

How will the policy be introduced to pupils?
Student planners will contain the relevant ICT policies for students to read and sign to accept they have read and understood them. These will be checked by form tutors and recorded electronically in the IT Support Office for viewing by staff upon request.

How will the policy be discussed with staff?
All policies will be made available on the VLE for download and viewing. Any changes to the E-Safety policy will result in new Acceptance forms being signed by staff.

How will parents' support be enlisted?
Parents need to read and sign the ICT section of the Student Planner to state they have read and understood the school ICT policies. This also includes the image consent form. Any further information or useful links to sites such as 'thinkuknow' will be made available on the Parent Portal of the school VLE under the e-Safety section.

5. 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 LA / Police.

Our e-Safety Coordinator acts as first point of contact for any complaint and will work closely with the Head of House and Senior ICT technician to rectify the issue. Any complaint about staff misuse is referred to the Headteacher.

ICT Security Policy

The objectives of the Policy, which is intended for all school staff, including Governors , who use or support the school's ICT systems or data, are to:

- **Ensure the protection of confidentiality, integrity and availability of school information and assets.**
- **Ensure all users are aware of and fully comply with all relevant legislation.**
- **Ensure all staff understands the need for information and ICT security and their own responsibilities in this respect.**

The integrity of the Staffordshire schools' network depends on the security policy implemented by each connected school. Information covers any information, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created.

The school's Senior ICT Technician is responsible for the school's ICT equipment, systems and data with direct control over these assets and their use, including responsibility for access control and protection. The Senior ICT Technician will be the official point of contact for ICT or information security issues.

Responsibilities:

- ✓ **Users of the school's ICT systems and data must comply with the requirements of the ICT Security Policy**

- ✓ **Users are responsible for notifying the Senior ICT Technician of any suspected or actual breach of ICT security. In the absence of the Senior ICT Technician, users should report any such breach directly to the Director of Business and Finance or Data Manager.**

- ✓ **Users must comply with the requirements of the Data Protection Act 1998, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988 and the Telecommunications Act 1984.**

- ✓ **Users must be provided with suitable training and documentation, together with adequate information on policies, procedures and facilities to help safeguard systems and data.**

- ✓ **Adequate procedures must be established in respect of the ICT security and implications of personnel changes.**

Physical Security:

- ✓ **As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data.**

- ✓ **Server rooms must be kept locked when unattended.**

- ✓ **Appropriate arrangements must be applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.**

- ✓ **All school owned ICT equipment and software should be recorded and an inventory maintained.**
- ✓ **Uninterruptible Power Supply (UPS) units are recommended for servers and network cabinets.**
- ✓ **Computer monitors should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons.**
- ✓ **Equipment should be sited to avoid environmental damage.**
- ✗ **Do not leave sensitive or personal data on printers, computer monitors or desk whilst away from your desk or computer.**
- ✗ **Do not give out sensitive information unless the recipient is authorised to receive it.**
- ✗ **Do not send sensitive/personal information which may be deemed confidential via e-mail or post without suitable security measures being applied.**
- ✓ **Ensure sensitive data, both paper and electronic, is disposed of properly, e.g. shred paper copies and destroy disks.**

System Security:

- ✗ **Users must not make, distribute or use unlicensed software or data.**
- ✗ **Users must not make or send threatening, offensive or harassing messages.**
- ✗ **Users must not create, possess or distribute obscene material.**
- ✓ **Users must ensure they have authorisation for private use of the school's computer facilities.**
- ✓ **The Senior ICT Technician will determine the level of password control.**
- ✓ **Passwords should be memorised. If passwords must be written down they should be kept in a secure location.**
- ✗ **Passwords should not be revealed to unauthorised persons.**
- ✗ **Passwords should not be obvious or guessable and their complexity should reflect the value and sensitivity of the systems and data**
- ✓ **Passwords should be changed at regular intervals; this is enforced by the ICT network at logon.**
- ✓ **Passwords must be changed if it is affected by a suspected or actual breach of security, e.g. when a password may be known by an unauthorised person.**
- ✓ **Regular backups of data, in accordance with the recommended backup strategy, must be maintained.**

- ✓ **Security copies should be regularly tested to ensure they enable data restoration in the event of system failure.**

- ✓ **Security copies should be clearly marked and stored in a fireproof location and/or off site.**

Virus Protection:

- ✓ **The Senior ICT Technician will ensure current and up to date anti-virus software is applied to all fixed school ICT systems.**

- ✓ **Laptop users must ensure they update their virus protection at least weekly, this is done by simply connecting the device to the schools network.**

- ✓ **The Senior ICT Technician will ensure operating systems are updated with critical security patches as soon as these are available.**

- ✓ **Any suspected or actual virus infection must be reported immediately to the Senior ICT Technician.**

Disposal and Repair of Equipment:

- ✓ **The Senior ICT Technician must ensure any personal data or software is obliterated from a PC if the recipient organisation is not authorised to receive the data.**

- ✓ **It is important to ensure that any software remaining on a PC being relinquished are legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.**

- ✓ **The Senior ICT Technician must ensure the requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed**

- ✓ **The school will ensure that third parties are registered under the Data Protection Act as personnel authorised to see data and such are bound by the same rules as school staff in relation to not divulging the data or making any unauthorised use of it.**

- ✓ **All empty Toner and Ink Cartridges will be disposed in an environmentally friendly manner where possible. As will other ICT consumables such as printer parts and batteries.**

Security Incidents:

All suspected or actual breaches of the ICT security, including detection of computer viruses, must be reported to the Senior ICT Technician, or Director of Business and Finance in their absence, you should report the incident to the Codsall ICT Support/Help Desk, via the Data Manager.

Social Media Code of Conduct

1 Introduction

This code of practice provides employees with guidance to ensure that they are taking the necessary steps to protect themselves and others against Cyber bullying.

It also provides employees with practical guidance on how they can ensure that their conduct in relation to social networking sites and electronic media is accordance with the code of conduct for all Local Government employees as interpreted by Staffordshire County Council in relation to social networking sites and electronic media.

1.1 Guidelines for Social Networking

Online communities can help Blythe Bridge High School & Sixth Form connect with its stakeholders in many ways. At the same time, there are some cautionary lessons that have emerged from participating in online communities. Participants should take note of the following:

- You are legally liable for anything you write or present online. Employees and students can be disciplined by the School for commentary, content, or images that are defamatory, pornographic, proprietary, harassing or that can create a hostile work environment. You can also be sued by School employees, competitors, and any individual or company that views your commentary, content or images as defamatory, pornographic, proprietary, harassing or creating a hostile work environment. No written comment should be made that could be offensive to anyone in any of the seven Equality and Diversity strands: age, disability, gender/transgender, religion or belief, sexual orientation, socio-economic group.
- You are posting content onto the World Wide Web and cannot ensure who does and does not have access to your information.
- Information you post online may continue to stay on the World Wide Web even after you erase or delete that information from pages.
- Before participating in any online community understand that anything posted online is available to anyone in the world.
- Do not post information, photos or other items online that could reflect negatively on you, your family or Blythe Bridge High School & Sixth Form.
- Be discreet, respectful, gracious and as accurate as you can be in any comments or content you post online.

Staff are also referred to the Safeguarding Policy which reminds them that any form of personal relationship between staff and students who are under 18 years of age or are vulnerable adults, is expressly forbidden. This would include any form of personal conversation or comment through the medium of the Internet. Therefore, Staff should not be 'Facebook friends' with any students.

1.2 Guidelines for Blogging

If teaching staff and/or a student own a blogging site the following guidelines should apply.

- Personal blogs should have clear disclaimers that the views expressed by the author in the blog is the author's alone and do not represent the views of the School. Be clear and write in first person. Make your writing clear that you are speaking for yourself and not on behalf of the School.
- Information published on your blog should comply with the School policies. This also applies to comments posted on other blogs, forums and social networking sites.
- Be respectful to the School's other employees, students and competitors.
- Social media activities should not interfere with work commitments.
- Your online presence reflects the School. Be aware that your actions captured via images, posts, or comments can reflect that of the School.
- Do not reference School employees or partners without their express consent.
- Respect copyright laws, and reference or cite sources appropriately. Plagiarism applies online as well.
- Company logos and trademarks may not be used without the written consent of the Director of Business and Finance as set out below.

2.1 Cyber Bullying

Definition: "Cyber bullying is the use of Information and Communications Technology (ICT), particularly mobile phones and internet, deliberately to upset someone else"
[Cyber bullying: Guidance issued by the DCSF 2007]

Staffordshire County Council supports the view that cyber bullying represents a cruel, dangerous and inescapable form of bullying that causes humiliation, stress and trauma to its victims, and so believes that cyber bullying is not acceptable and will not be tolerated.

Blythe Bridge High School & Sixth Form are committed to the view that cyber bullying is never acceptable and is not tolerated

2.2 Legislation

Although bullying is not a specific criminal offence, criminal law exists to prevent certain behaviours. These behaviours may constitute harassment, or cause a fear of violence. Sending indecent, grossly offensive or threatening letters, electronic communications or other articles to another person is illegal

Other legislation protects against the publication of obscene articles or data (e.g. over a school intranet), hacking into someone else's computer, invading their privacy, damaging their reputation or engaging in anti-social acts.

2.3 Protecting yourself against Cyber Bullying

There are simple measures that you can take to safeguard against cyber bullying:

- Being careful about personal information and images posted on the internet
- Not leaving your mobile phone or personal computer around for others to gain access or leaving details on view when left unattended
- Choosing hard-to-guess passwords and not letting anyone else know them
- Being aware of the risks of giving your mobile number or personal e-mail address to others
- Making use of blocking facilities made available by website and service providers
- Not replying or retaliating to a bullying message

- Saving evidence of offending messages
- Making sure you inform others of any mobile phone or online bullying or harassment in accordance with relevant policies.

2.4 What action you can take

- Complaints of cyber bullying 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.
- Cyber bullying complaints will be investigated to obtain any evidence available and you can support this process by:
    - logging any incidents
    - noting the dates, times and content of messages and, where possible, the sender's identity or web address.

Taking an accurate copy of the whole web page address, for example, helps service providers to locate offending material. Such evidence may also be required to show to those who need to know, including police.

Saving evidence of texts and images on the device itself is useful. It is important they are not deleted.

In the non work environment it may be appropriate to report incidents of cyber bullying direct to an internet service provider or mobile phone company. Content may be blocked and / or removed if it is illegal or breaks the provider's own terms and conditions. Some providers issue conduct warnings to users and are able to delete the accounts of those who have broken the rules.

3. Safeguarding

In order to safeguard yourself and potentially vulnerable adults and young people who you may work with you should ensure that your behaviour with regard to social networking sites is consistent with the standards of behaviour expected in normal day to day interactions with vulnerable adults and young people.

Communication that is undertaken via social networking sites is comparable to 'one to one' interaction in other contexts, and individuals should avoid any activity which would lead any reasonable person to question their motivation and intentions.

You are reminded that it is expected that you:

a) Always act in such a way as to promote and safeguard the well being and interests of service users and colleagues.

b) Take all reasonable steps to ensure that relationships with service users and colleagues are such that there can be no suggestion of impropriety whether by word or action.

c) Develop a friendly relationship between employee and service users, with clear boundaries. It is deemed an abuse of that professional relationship for an employee:
    - to enter into an improper relationship with a service user
    - to show favour towards a particular service user
    - to act in a threatening or aggressive manner or to use foul, abusive or profane language
    - to endeavour to exert an undue influence with regard to personal attitudes, opinions or behaviour which is in no way connected to the work of the Service.

d) Take all reasonable steps to ensure that no action or omission on your part or within your sphere of influence is detrimental to the condition or safety of service users

In order to preserve these standards of behaviour it is recommended that you decline any request from an existing or previous service user to be a “friend” on your Social Network Site.

It is inappropriate to request contact with an existing or previous user of the service via this medium or any other form of electronic medium.

It is acknowledged that you may accept a service user as a “friend” unintentionally and where this occurs you are advised to ensure that you remove this access as soon as you become aware of their status. You should do this in a way that does not jeopardise your professional relationship and should inform your Line Manager, if any significant conversation or activity occurs.

All employees are advised to ensure that when setting up social networking sites they should make full use of the range of tools which enable the access to personal information to be restricted.

4 Conclusion

Where no guidelines exist, staff should use their professional judgement and take the most prudent action possible. Consult with the School’s Director of Business and Finance if you are uncertain.

Media contacts about the School, our students, employees, partners, customers and competitors must be referred for co-ordination and guidance to the Director of Business and Finance.

Please note that any activity on School’s internal systems are monitored and recorded. Any external web activity is monitored, recorded and filtered whilst accessed on the school network.

The breach of Social Media Code of Conduct and any content that would adversely affect the School could result in a disciplinary action.

BLYTHE BRIDGE HIGH SCHOOL & SIXTH FORM
A FOUNDATION TRUST SCHOOL

Consent Form For Staff
E-Safety Policy

Please complete, sign and return to the IT Support Office

Name:	**Job Title:**

Staff Declaration
You must read, understand and sign this form if you use our ICT facilities and services. We will keep the completed form in our signed declarations file.

Declaration
I confirm that, as an authorised user of the School's ICT facilities,
I have read, understood and accepted all of the conditions in the E-Safety Policy.

Signed:	**Date:**

Agreement: Purchase of Equipment for Pupil Premium/Pupil Premium Plus Students

Name of Student		**Form**	
		Year	

Name of Parent		**Tel No.**	
Date			

Description of equipment purchased for student		**Serial Numbers**
1		
2		
3		
4		
5		
6		

Declaration

I agree to the safekeeping of the equipment above. Any loss or damage to the equipment will be my responsibility to replace or repair.

Signed:	**Authorising Signature**
Print Name	**Print Name**

Social Media Code of Conduct

1 Introduction

This code of practice provides employees with guidance to ensure that they are taking the necessary steps to protect themselves and others against Cyber bullying.

It also provides employees with practical guidance on how they can ensure that their conduct in relation to social networking sites and electronic media is accordance with the code of conduct for all Local Government employees as interpreted by Staffordshire County Council in relation to social networking sites and electronic media.

1.1 Guidelines for Social Networking

Online communities can help Blythe Bridge High School and Sixth Form connect with its stakeholders in many ways. At the same time, there are some cautionary lessons that have emerged from participating in online communities. Participants should take note of the following:

- You are legally liable for anything you write or present online. Employees and students can be disciplined by the School for commentary, content, or images that are defamatory, pornographic, proprietary, harassing or that can create a hostile work environment. You can also be sued by School employees, competitors, and any individual or company that views your commentary, content or images as defamatory, pornographic, proprietary, harassing or creating a hostile work environment. No written comment should be made that could be offensive to anyone in any of the seven Equality and Diversity strands: age, disability, gender/transgender, religion or belief, sexual orientation, socio-economic group.
- You are posting content onto the World Wide Web and cannot ensure who does and does not have access to your information.
- Information you post online may continue to stay on the World Wide Web even after you erase or delete that information from pages.
- Before participating in any online community understand that anything posted online is available to anyone in the world.
- Do not post information, photos or other items online that could reflect negatively on you, your family or Blythe Bridge High School & Sixth Form.
- Be discreet, respectful, gracious and as accurate as you can be in any comments or content you post online.

Staffs are also referred to the Safeguarding Policy which reminds them that any form of personal relationship between staff and students who are under 18 years of age or are vulnerable adults, is expressly forbidden. This would include any form of personal conversation or comment through the medium of the Internet. Therefore, Staff should not be 'Facebook friends' with any students. If a staff member discovers an imposter account has been made in their name they should report it immediately.

1.2 Guidelines for Blogging

If teaching staff and/or a student own a blogging site the following guidelines should apply.

- Personal blogs should have clear disclaimers that the views expressed by the author in the blog is the author's alone and do not represent the views of the School. Be clear and write in first person. Make your writing clear that you are speaking for yourself and not on behalf of the School.
- Information published on your blog should comply with the School policies. This also applies to comments posted on other blogs, forums and social networking sites.
- Be respectful to the School's other employees, students and competitors.
- Social media activities should not interfere with work commitments.
- Your online presence reflects the School. Be aware that your actions captured via images, posts, or comments can reflect that of the School.
- Do not reference School employees or partners without their express consent.
- Respect copyright laws, and reference or cite sources appropriately. Plagiarism applies online as well.
- Company logos and trademarks may not be used without the written consent of the Business Manager as set out below.

2.1 Cyber Bullying

Definition: "Cyber bullying is the use of Information and Communications Technology (ICT), particularly mobile phones and internet, deliberately to upset someone else"
[Cyber bullying: Guidance issued by the DCSF 2007]

Staffordshire County Council supports the view that cyber bullying represents a cruel, dangerous and inescapable form of bullying that causes humiliation, stress and trauma to its victims, and so believes that cyber bullying is not acceptable and will not be tolerated.

Blythe Bridge High School and Sixth Form are committed to the view that cyber bullying is never acceptable and is not tolerated

2.2 Legislation

Although bullying is not a specific criminal offence, criminal law exists to prevent certain behaviours. These behaviours may constitute harassment, or cause a fear of violence. Sending indecent, grossly offensive or threatening letters, electronic communications or other articles to another person is illegal

Other legislation protects against the publication of obscene articles or data (e.g. over a school intranet), hacking into someone else's computer, invading their privacy, damaging their reputation or engaging in anti-social acts.

2.3 Protecting yourself against Cyber Bullying

There are simple measures that you can take to safeguard against cyber bullying:

- being careful about personal information and images posted on the internet
- not leaving your mobile phone or personal computer around for others to gain access or leaving details on view when left unattended
- choosing hard-to-guess passwords and not letting anyone else know them
- being aware of the risks of giving your mobile number or personal e-mail address to others
- making use of blocking facilities made available by website and service providers
- not replying or retaliating to a bullying message
- saving evidence of offending messages
- making sure you inform others of any mobile phone or online bullying or harassment in accordance with relevant policies.

2.4 What action you can take

- Complaints of cyber bullying 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. Cyber bullying
- complaints will be investigated to obtain any evidence available and you can support this process by:

- logging any incidents
- noting the dates, times and content of messages and, where possible, the sender's identity or web address.

Taking an accurate copy of the whole web page address, for example, helps service providers to locate offending material. Such evidence may be required also to show to those who need to know, including police.
Saving evidence of texts and images on the device itself is useful. It is important they are not deleted.

In the non work environment it may be appropriate to report incidents of cyber bullying direct to an internet service provider or mobile phone company. Content may be blocked and / or removed if it is illegal or breaks the provider's own terms and conditions. Some providers issue conduct warnings to users and are able to delete the accounts of those who have broken the rules.

3. Safeguarding

In order to safeguard yourself and potentially vulnerable adults and young people who you may work with you should ensure that your behaviour with regard to social networking sites is consistent with the standards of behaviour expected in normal day to day interactions with vulnerable adults and young people.

Communication that is undertaken via social networking sites is comparable to 'one to one' interaction in other contexts, and individuals should avoid any activity which would lead any reasonable person to question their motivation and intentions.

You are reminded that it is expected that you:

b) Always act in such a way as to promote and safeguard the well being and interests of service users and colleagues.

b) Take all reasonable steps to ensure that relationships with service users and colleagues are such that there can be no suggestion of impropriety whether by word or action.

c) Develop a friendly relationship between employee and service users, with clear boundaries. It is deemed an abuse of that professional relationship for an employee:

- to enter into an improper relationship with a service user
- to show favour towards a particular service user
- to act in a threatening or aggressive manner or to use foul, abusive or profane language
- to endeavour to exert an undue influence with regard to personal attitudes, opinions or behaviour which is in no way connected to the work of the Service.

d) Take all reasonable steps to ensure that no action or omission on your part or within your sphere of influence is detrimental to the condition or safety of service users

In order to preserve these standards of behaviour it is recommended that you decline any request from an existing or previous service user to be a "friend" on your Social Network Site.

It is inappropriate to request contact with an existing or previous user of the service via this medium or any other form of electronic medium.

It is acknowledged that you may accept a service user as a “friend” unintentionally and where this occurs you are advised to ensure that you remove this access as soon as you become aware of their status. You should do this in a way that does not jeopardise your professional relationship and should inform your Line Manager, if any significant conversation or activity occurs.

All employees are advised to ensure that when setting up social networking sites they should make full use of the range of tools which enable the access to personal information to be restricted.

4 Conclusion

Where no guidelines exist, staff should use their professional judgement and take the most prudent action possible. Consult with the School’s Business Manager if you are uncertain.

Media contacts about the School, our students, employees, partners, customers and competitors must be referred for co-ordination and guidance to the Business Manager.

Please note that any activity on School’s internal systems are monitored and recorded. Any external web activity is monitored, recorded and filtered whilst accessed on the school network.

The breach of Social Media Code of Conduct and any content that would adversely affect the School could result in a disciplinary action.

BLYTHE BRIDGE HIGH SCHOOL & SIXTH FORM
A FOUNDATION TRUST SCHOOL

Consent Form for Staff

E-Safety Policy

Please complete, sign and return to the IT Support Office

Name:	***Job Title:***

Staff Declaration
You must read, understand and sign this form if you use our ICT facilities and services. We will keep the completed form in our signed declarations file.

Declaration
I confirm that, as an authorised user of the School's ICT facilities, I have read, understood and accepted all of the conditions in the E-Safety Policy.

Signed:	***Date:***

BLYTHE BRIDGE HIGH SCHOOL & SIXTH FORM
A FOUNDATION TRUST SCHOOL

Consent Form for Third Parties

E-Safety Policy

Please complete, sign and return to the IT Support Office

Name:	***Job Title:***

Third Party Declaration

You must read, understand and sign this form if you use our ICT facilities and services. We will keep the completed form in our signed declarations file.

Declaration

I confirm that, as an authorised user of the School's ICT facilities, I have read, understood and accepted all of the conditions in the E-Safety Policy.

Signed:	***Date:***

BLYTHE BRIDGE HIGH SCHOOL & SIXTH FORM
A FOUNDATION TRUST SCHOOL

Virtual Learning Environment (VLE - Frog) Acceptable Use Policy

- **The following policy outlines the terms of use for all users (staff and students) of Blythe Bridge High School and Sixth Form's virtual learning environment (Frog).**
- **All Blythe Bridge High School and Sixth Form staff and students are granted access to Frog to facilitate learning and teaching. Access is conditional upon agreement with school regulations and all relevant UK laws.**
- **Failure to comply may result in loss of privileges. In cases where UK law has been violated, users could face criminal and/or civil liability.**

Acceptable Use

Blythe Bridge High School and Sixth Form expects and requires that its users act responsibly and considerately, and respect the rights of other Frog users at all times.

Unacceptable Use

Any users that infringe the policy, behave inappropriately online, or adversely affect Blythe Bridge High School and Sixth Form's online learning communities will be denied access to Frog. The following constitutes unacceptable use of Frog:

25. **Unauthorised use of another person's login details to gain access to the Frog system.**
26. **Unauthorised reading, copying, modification, or corruption of another users files, communications, or data.**
27. **Attempts to undermine the security or integrity of Frog and related systems/software.**
28. **Posting or using material that infringes copyright and intellectual property rights. If you are unsure whether Blythe Bridge High School and Sixth Form owns a particular licence to reproduce materials, you should contact the Senior ICT Technician or Business Manager for confirmation.**
29. **Creation or transmission of any materials that are considered offensive, obscene, or indecent.**
30. **Creation and transmission of materials/communications that include profanity, vulgarity, hate speech, disruptive or hostile comments, interpersonal disputes, or threats of violence.**
31. **Discussing or re-posting materials/communications that have been deemed inappropriate and removed by the school.**
32. **Creation and transmission of materials, or taking actions, that interfere with Frog operations.**
33. **Including another user's contact details or personal information in materials/communications without express permission from the individual concerned.**
34. **Refusing to adhere to the schools IT and conduct policies, procedures and agreements.**
35. **Using Frog for commercial purposes or financial gain without express approval from Blythe Bridge High School and Sixth Form.**

36. **Violating the privacy and confidentiality of other users.**

Additional Notes

- **All users are responsible for their activities on the Frog system and for the content of their uploaded materials and communications (via chat rooms, email or discussion forums).**
- **The school aims to remove any inappropriate materials as soon as possible after they are discovered or reported and will deal with inappropriate use or behaviour of Frog swiftly and rigorously within the guidelines of the school's disciplinary procedures.**

I have read and understand the above Virtual Learning Environment acceptable usage policy:

[Options of Agree or Disagree to be clicked]
[This option will be reset over the summer term or whenever a change to the policy is made]

E-Safety Policy

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. The School policies will be monitored each year and adapted where necessary to fit in with new technology.

2. Whole School approach to the safe use of ICT
Creating a safe ICT learning environment includes three main elements at Blythe Bridge High School & Sixth Form:

- An effective range of technological tools (Sophos, Proxy Filters & Impero);
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-Safety education programme for pupils, staff and parents.

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 Senior ICT Technician ensures that the Policy is implemented and compliance with the Policy monitored.

Our school **e-Safety Co-ordinator** is Mrs S Owen

All students, staff and Governors should be familiar with the following ICT policies:

- **ICT. Email Internet Acceptable Use Policy (School Planners, Form rooms and School Website)**
- **ICT. Virtual Learning Policy (AUP on login to Frog – Failure to accept will not allow access)**
- **ICT. Social Media Code of Conduct**
- **ICT. ICT Security Policy**
- **ICT. Acceptable User Policy (Will appear on Network Computers before log on)**
- **ICT. Acceptable Use of Mobile Devices Policy (If issued with school device)**
- **ICT. BYOD Policy (If you have been granted permission to use a personal device at school)**

All policies are made available through the VLE or can be provided on request from IT Support Office.

4. Communications

How will the policy be introduced to pupils?
School planners will contain the relevant ICT policies for students to read and sign to accept they have read and understood them. These will be checked by form tutors and recorded electronically in the IT Support Office for viewing by staff at request.

How will the policy be discussed with staff?
All policies will be made available on the VLE for download and viewing. Any changes to the E-Safety policy will result in new Acceptance forms being signed by staff.

How will parents' support be enlisted?
This also includes the image consent form. Any further information or useful links to sites such as 'thinkuknow' will be made available on the Parent Portal of the school VLE under the e-Safety section.

5. 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 Sixth Form / 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 LA / Police.

Our e-Safety Coordinator acts as first point of contact for any complaint and will work closely with the Head of Sixth Form and Senior ICT technician to rectify the issue. Any complaint about staff misuse is referred to the Headteacher.

Acceptable Use Policy

1. You must always follow the schools e-safety policy in order to keep yourself and others safe online.

2. The work/activity on the Internet must be directly related to your schoolwork.

3. Any student found to be damaging IT equipment will be punished appropriately (see below).

4. Do not disclose any password or login name you have been given **to anyone**.

5. Use of names or photographs of students will require written permission of parent(s)/guardian(s). This can be found in the student planner.

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

7. Under no circumstances should you view, upload or download any material that is likely to be unsuitable for use in schools. This applies to any material of a violent, dangerous, racist or with inappropriate sexual content. If you are not sure about this, or any materials, you must ask a teacher.

8. Always respect the privacy of files of other users. Do not enter the file areas of other students or staff. Work that needs to be accessed in other work areas must only be done by the Senior ICT Technician under the instruction of the Director of Business and Finance, in their absence; the Senior ICT Technician must seek approval from The Headteacher's PA.

9. The IT support department has the right to view any material held on the school network. This right will only be used ethically, for E-Safety reasons and/or at the request of the senior members of staff.

10. Be Polite and appreciate that other users might have different views other than your own. Use of strong language, swearing or aggressive behaviour is not allowed.

11. Do not state anything that could be interpreted as libel.

12. Do not copy any work off the Internet or from other students and try to distribute it as your own (Plagiarism).

13. Under no circumstances is anyone to 'Hack' into any part of the network, or obtain other users logon details by any means.

14. Failure to comply with these rules will result in one or more of the following
- A ban, temporary or permanent, on the use of the internet facilities at school
- A letter informing parents of the nature and breach of rules.
- Appropriate sanctions and restrictions placed on access to school facilities to be decided by the Head of Sixth Form/ICT Coordinator/E-Safety Officer/Headteacher
- Any other action decided by the Chair of Governors of Blythe Bridge High School & Sixth Form.

If you do not understand any part of this document, you must ask the Director of Business and Finance, or the Senior ICT Technician.

PARENT/CARER
I have read and understood the information above:

Name of child	Date
Parent Name	*Parent/Carer Signature*

Virtual Learning Environment (VLE - Frog) Acceptable Use Policy

- **The following policy outlines the terms of use for all users (staff and students) of Blythe Bridge High School & Sixth Form's virtual learning environment (Frog).**
- **All Blythe Bridge High School & Sixth Form staff and students are granted access to Frog to facilitate learning and teaching. Access is conditional upon agreement with school regulations and all relevant UK laws.**
- **Failure to comply may result in loss of privileges. In cases where UK law has been violated, users could face criminal and/or civil liability.**

Acceptable Use

Blythe Bridge High School & Sixth Form expects and requires that its users act responsibly and considerately, and respect the rights of other Frog users at all times.

Unacceptable Use

Any users that infringe the policy, behave inappropriately online, or adversely affect Blythe Bridge High School & Sixth Form's online learning communities will be denied access to Frog. The following constitutes unacceptable use of Frog:

37. **Unauthorised use of another person's login details to gain access to the Frog system.**
38. **Unauthorised reading, copying, modification, or corruption of another users files, communications, or data.**
39. **Attempts to undermine the security or integrity of Frog and related systems/software.**
40. **Posting or using material that infringes copyright and intellectual property rights. If you are unsure whether Blythe Bridge High School & Sixth Form owns a particular licence to reproduce materials, you should contact the Senior ICT Technician or Business Manager for confirmation.**
41. **Creation or transmission of any materials that are considered offensive, obscene, or indecent.**
42. **Creation and transmission of materials/communications that include profanity, vulgarity, hate speech, disruptive or hostile comments, interpersonal disputes, or threats of violence.**
43. **Discussing or re-posting materials/communications that have been deemed inappropriate and removed by the school.**
44. **Creation and transmission of materials, or taking actions, that interfere with Frog operations.**
45. **Including another user's contact details or personal information in materials/communications without express permission from the individual concerned.**
46. **Refusing to adhere to the schools IT and conduct policies, procedures and agreements.**
47. **Using Frog for commercial purposes or financial gain without express approval from Blythe Bridge High School & Sixth Form.**
48. **Violating the privacy and confidentiality of other users.**

Additional Notes

- **All users are responsible for their activities on the Frog system and for the content of their uploaded materials and communications (via chat rooms, email or discussion forums).**
- **The school aims to remove any inappropriate materials as soon as possible after they are discovered or reported and will deal with inappropriate use or behaviour of Frog swiftly and rigorously within the guidelines of the school's disciplinary procedures.**

I have read and understand the information above:

Name:	***Signature***	***Date***

School Image Consent Form

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make any recordings of your child.

Conditions of use:

1. This form is valid for the period of time your child attends this school. Images of your child will not be used after this time. Please write to the school if you wish to withdraw consent at any time.

2. The images we take will be of activities that show the school and children in a positive light.

3. Embarrassing or distressing images will not be used. The images will not be associated with negative or sensitive issues.

4. We may use group or class photographs or footage with very general labels e.g. 'science lesson'.

5. We will only use images of pupils who are suitably dressed.

6. We will make every effort to ensure that we do not allow images to be taken of any children for whom we do not have permission or who are 'at risk' or disallowed from having their photographs taken for legal or social reasons.
7. We will take all reasonable measures to ensure the images are used solely for the purposes for which they are intended. However we cannot guarantee this and take no responsibility for the way images are used by other websites or publishers or for any consequences arising from publication.

I give permission for my child's image to be taken and used in publicity material for the school, including printed and electronic publications, video and webcam recordings and on websites.	☐
I give permission for images of my child to be used by the news media in printed and/or electronic form and stored in their archives. This might include images sent to the news media by the school and images / footage the media may take themselves if invited to the school to cover an event.	☐
I do not want my child's image used in any publicity.	☐

PARENT/CARER
I have read and understood the information above:

Name of child	Date
Parent Name	*Parent/Carer Signature*

BLYTHE BRIDGE HIGH SCHOOL & SIXTH FORM
A FOUNDATION TRUST SCHOOL

Consent Form for 6th Form

E-Safety Policy

Please complete, sign and return to the IT Support Office

Name:	***Form:***

6th Form Declaration

You must read, understand and sign this form if you use our ICT facilities and services. We will keep the completed form in our signed declarations file.

Declaration

I confirm that, as an authorised user of the School's ICT facilities, I have read, understood and accepted all of the conditions in the E-Safety Policy.

Signed:	***Date:***