St Bede's Catholic High School

IT Policy for Staff and Pupils

Rationale

The use of ICT in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

Purpose

To ensure ALL staff are aware of the risks and enforce, this IT Policy. The school will ensure that members of staff use computer equipment and its applications in such a way as to:-

- minimise the risk of damage to property (including data, software and hardware) and
- ensure that all legal responsibilities of individuals and the school are met.

All members of staff are therefore asked to read, comply and agree to abide by the ICT policy. This policy should be read in conjunction with Lancashire County Council information and communication technology ICT security framework and St. Bede's E Safety policy. They should make sure that they are aware of any unacceptable practices together with consideration of the Data Protection Act as outlined in the staff handbook.

St. Bede's have official Twitter and Facebook accounts. To ensure access to the official site, links will be provided from the school official website. These sites are locked down in order that the public may not be able to comment or add friendship groups. Access to update these sites is limited to ICT support and any information placed on the official sites have been scrutinised by a member of the Senior Leadership Team.

Implementation

At St. Bede's High School, there are a number of ways in which we protect the data and software which is stored on our computer systems.

- Access to hardware, software, and data is restricted to those who have right of access.
- School ICT systems will be reviewed regularly with regard to security and the school will ensure a filtering system is in place to protect students and staff.
- Virus protection will be installed and updated regularly
- Unapproved system utilities and executable files will not be allowed in student/staff work areas or attached to e-mail.
- Care should be taken to avoid unauthorised access: for example, computers should not be left unsupervised. Users should lock their computer when not in use.
- Access restrictions on a user by user basis can be provided upon request. By default all

users may use all workstations.

- Physical security of network servers is essential and such servers should reside in air conditioned rooms specifically put aside for this purpose
- Access to cabling infrastructure, in particular switches and routers should be limited to technical staff, or their representative, in the form of a contractor.
- The IT Support staff are responsible for setting access rights within the system. Any additional access must be requested through IT Support.
- As staff have access to confidential information on the network, passwords are recommended to be changed at least once per term, must be at least eight characters and include at least two character types (letter, number, non-alphanumeric character e.g. *&#$). Passwords must not be disclosed to any third party.
- Confidential data should not be stored on the hard drive of individual workstations or external devices. Such information should be saved to the network location as recommended by the Network Manager.
- Software should be installed only by the ICT support team.. The use of unauthorised software is forbidden. Software purchases should be authorised by the Network Manager prior to purchase to ensure compatibility.
- E-mail sent to an external organisation should be written carefully in the same way as a letter written on school headed paper. Further guidance can be obtained on the Schools Portal via LCC.
- The forwarding of chain letters is not permitted.
- The school will block/filter unauthorised access to social networking sites.
- Care should be taken when capturing photographs or video to ensure that all students are appropriately dressed. Photographs and video clips should be stored on the appropriate secure drive in school.
- It is not appropriate to use photographic or video devices in changing rooms or toilets. CCTV in the pupil toilets is covered under the CCTV policy.
- The unauthorised downloading of audio or video files is not permitted without prior permission and should be done so with reference to the CCTV policy.
- If staff or students discover an unsuitable site, it must be reported to IT Support.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Staff and students should comply with current legislation and internal policies by using the internet in an acceptable manner that complies with this policy.
- Staff and students should not create any unnecessary risk to the school by their misuse of the IT network, internet and ICT systems.

Off-site Security

- School equipment and laptops are not to be taken off-site without authorisation. Where necessary and appropriate, equipment is logged out and back by the Network Manager. Equipment and media taken off the premises is not to be left unattended in public places. Portable computers are to be carried as hand luggage and disguised if possible when travelling. Remote access to the network is available to all staff users. Remote access is preferable to taking portable equipment off the premises.

Unacceptable Practices

In particular, the following is deemed unacceptable use or behaviour by staff and students.

- Visiting Internet sites that contain obscene, hateful, pornographic, racial, offensive or otherwise illegal material.
- Using the computer to perpetrate any form of fraud, including software, film and/or music piracy.
- Using the Internet to send offensive or harassing material to other users.
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence.
- Hacking into unauthorised areas or ICT systems.
- Publishing defamatory and/or knowingly false material about St. Bede's High School or its staff.
- Users should not use social networking sites, blogs, online chat rooms, journals, or any online publishing format unless it is controlled and monitored from within school. Users should not pair smart devices, phones and watches to the school network without prior permission from the Network Manager. Users should refer to the LCC policy on Social Media and Mobile Phones.
- Users should not attempt to bypass any school or council filtering system.
- Connecting any unauthorised computers or laptops to the network.
- Installing software onto workstations or laptops including computer games
- Making personal copies of any software installed on the Network
- Plagiarism of other peoples work.
- Attempting to repair any equipment that appears faulty
- Sharing usernames and passwords or using someone else's login details
- Removing or moving any equipment or materials without permission from IT Support
- Drinking or eating hot food near computer equipment
- Using computers for purposes that are not related to your job and in such a way as to involve disclosure of personal or financial data (e.g. credit card details) as the school will bear no responsibility for the security of this information.
- Personal email or messaging between staff and students should not take place.
- Staff personal use of the Internet and E-mail system during working hours.

Monitoring and Evaluation

- The school maintains the right to monitor the volume of Internet and network traffic, together with the internet sites visited using third party monitoring software. Staff and students sign an acceptable user policy in advance of being given access to the Internet.
- Staff and students should be aware that internet traffic will be monitored and traced to the individual user. Discretion and professional conduct is essential. Where it is believed that a member of staff or student has failed to comply with this policy, they will face the schools disciplinary proceedings.
- The Network Manager will monitor the filtering methods regularly to ensure they are effective and reasonable.
- Any documents produced, processed or collected in the course of employment or student use remains the property of St. Bede's High School. This includes such information stored on third-party websites such as webmail service providers.
- The school will audit ICT provision to establish that online safety is adequate and that its implementation is effective.
- Complaints of internet misuse by staff or students will be referred to a member of the senior leadership team to investigate.
- Any concerns relating to child protection will be dealt with in accordance with the

school child protection procedures and will be referred to a member of the child protection team.

Usernames and passwords

All users of the networks are required to use a unique username and password in order to use the computers supplied by the school.

All passwords are kept private to the individual. Network users are advised to use complex passwords and to change them frequently.

Students only have access to the curriculum network. The Students security group has limited functionality on the network compared to a member of staff who might be in the Staff Security Group.

Backup

In order to prevent permanent data loss through accident or perhaps fire, the data held on the school servers is backed up each week day. Staff and pupils should not store any data or files on the local 'C' drive as this is not backed up and information can be lost.

Appendix 1

Dear Parent

Responsible Internet Use

As part of your child's curriculum and the development of ICT skills, St.Bede's Catholic High School is providing supervised access to the Internet. We believe that the use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached 'E-mail and Internet Use Good Practice - 'Rules for ICT Use' document, and sign and return the consent form so that your child may use Internet at school.

Although there have been concerns about pupils having access to undesirable materials, we are taking positive steps to deal with this risk in school. Our school Internet provider operates a filtering system that restricts access to inappropriate materials. This may not be the case at home and we can provide references to information on safe Internet access if you wish. We also have leaflets from national bodies that explain the issues further.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the Internet. The school will not be liable for any damages arising from your child's use of the Internet facilities.

Should you wish to discuss any aspect of Internet use please do not hesitate to contact me.

Yours sincerely

C Horrocks
Headteacher

St.Bede's Catholic High School

E-mail and Internet Use Good Practice - Students

Rules for ICT Use

The school computer system provides Internet access to students for learning. This E-mail and Internet Use Good Practice statement will help protect students and the school by clearly stating what is acceptable and what is not.

- School computer and Internet use must be appropriate to the student's education.
- Access must only be made via the user's authorised account and password, which must not be given to any other person.
- USB sticks, CDs and DVDs must not be brought into school unless permission has been given and have been checked for viruses before use.
- Copyright and intellectual property rights must be respected.
- Users must respect the work of others, which might be stored in common areas on the system. Conversely, users should always try and store their files and data in their own secure area or on removable media. Files and data stored in common areas of the system must be transferred at the earliest opportunity to the users own area. Such files will be regularly removed from the system.
- Users are responsible for e-mail they send and for contacts made. E-mail should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property. Anonymous messages and chain letters must not be sent.
- Users should report any unpleasant material or messages received. The report will be confidential and will help protect others.
- The use of public chat rooms is not allowed.
- The school ICT systems may not be used for private business purposes, unless the Headteacher has given permission for that use. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- The security of ICT systems must not be compromised, whether owned by the school or by other organisations or individuals.
- Irresponsible use may result in the loss of ICT access.
- The system is monitored and inappropriate use will be detected.

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

St.Bede's Catholic High School

Responsible E-mail and Internet Use Consent Form

Students

St.Bede's Catholic High School **Responsible E-mail and Internet Use** **Please complete, sign and return to school**	
Pupil:	**Form:**
Pupil's Agreement I have read and understand the school 'E-mail and Internet Use Good Practice - Rules for ICT Users' document. I will use the computer system and Internet in a responsible way and obey these rules at all times.	
Signed:	**Date:**
Parent / Carer's Consent for Internet Access I have read and understood the school 'E-mail and Internet Use Good Practice - Rules for ICT Users' document and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.	
Signed:	**Date:**
Please print name:	
Parent / Carer's Consent for Web Publication of Work and Photographs I agree that, if selected, my son/daughter's work may be published on the school Web site and in-house TVs. I also agree that photographs that include my son/daughter may be published subject to the school rules that photographs will not clearly identify individuals and that full names will not be used.	
Signed:	**Date:**

St.Bede's Catholic High School

Student Acceptable Internet Use Statement

The computer system is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties - the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.
Staff and students requesting Internet access should sign a copy of this Acceptable Internet Use Statement and return it to the IT Manager for approval.

- All Internet activity should be appropriate to staff professional activity or the student's education;
- Access should only be made via your authorised network account and password, which should not be made available to any other person;
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden;
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Copyright of materials must be respected;
- Posting anonymous messages and forwarding chain letters is forbidden;
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.

Full name	**Form**
Signed	**Date**
Access granted	**Date**

Appendix 2

St.Bede's Catholic High School

E-mail & Internet Use Good Practice

Rules and Agreements for Staff

The following guidelines (some of which also apply to other forms of correspondence) tell you what is and what is not good practice when you use internal or Internet E-mail services.

You should:

- check your E-mail inbox for new messages regularly;
- treat E-mail as you would a letter, remember they can be forwarded / copied to others;
- check the message and think how the person may react to it before you send it;
- make sure you use correct and up to date E-mail addresses;
- file mail when you have dealt with it and delete any items that you do not need to keep;

You should not:

- use E-mail to manage staff where face-to-face discussion is more appropriate;
- create wide-distribution E-mails (for example, to addressees throughout the world) unless this form of communication is vital;
- print out messages you receive unless you need a hard copy;
- send large file attachments to E-mails to many addressees;
- send an E-mail that the person who receives it may think is a waste of resources;
- use jargon, abbreviations or symbols if the person who receives the E-mail may not understand them.

St.Bede's Catholic High School

Staff Acceptable Internet Use Statement

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school is keen to see staff make full use of the system, in order that they might broaden their skills and enhance their professional development.

The school's Internet Access Policy has been drawn up to protect all parties. With the agreement of the Headteacher, the system and internet access can be made available for occasional personal use, during the employee's own time i.e after school and during the lunch break. Staff are reminded that inappropriate use of the internet could result in action being taken under the terms of the School's disciplinary procedure. The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Therefore, it is important that all staff familiarize themselves with the principles set out below

- All Internet activity should be appropriate to staff professional activity, including research for professional purposes. Where the system is made available for personal use, the same principles apply.
- USB sticks, CDs and DVDs must not be brought into school unless permission has been given and have been checked for viruses before use.
- Under the terms of the Authority's Trade Union Facilities Agreement, reasonable use of computer facilities for authorised trade union representatives is permitted.
- Access should only be made via your authorised network account and password, which should not be made available to any other person;
- Activity that threatens the integrity of the school ICT systems and laptops, or activity that attacks or corrupts other systems, is forbidden;
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Copyright of materials must be respected;
- Posting anonymous messages and forwarding chain letters is forbidden;
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- The system will be monitored for inappropriate use.
- Staff are advised against registering for social networking sites such as Facebook

St.Bede's Catholic High School

Employee Agreement to E-mail and Internet Use

I have received a copy of the E-Mail and Internet Use Good Practice and the Acceptable Internet Use Statement and agree to comply with the standards set in the document, for the duration of my employment.

I am aware that e-mail or internet related documents that I initiate, manipulate or respond to may be examined at any time without notifying me.

I am aware that if I violate the guidelines on e-mail and internet acceptable use I may face disciplinary action, up to and including dismissal from employment. I understand that I may be personally liable for any criminal offence that I commit in relation to this policy.

Employees Full Name (printed)	
Employees Signature	
Date	
Manager's Signature	
Date	

Appendix 3

St.Bede's Catholic High School

E-mail and Internet Use Good Practice

Rules for ICT Use - Third Party Use

The school computer system provides Internet access to third parties, that is other than staff and students. This E-mail and Internet Use Good Practice statement will help protect third parties, students and the school by clearly stating what is acceptable and what is not.

- Access must only be made via your user's authorised network account and password, which must not be given to any other person.
- USB sticks, CDs and DVDs must not be brought into school unless permission has been given and have been checked for viruses before use.
- Copyright and intellectual property rights must be respected.
- Users must respect the work of others, which might be stored in common areas on the system. Conversely, users should always try and store their files and data in their own secure area or on removable media. Files and data stored in common areas of the system must be transferred at the earliest opportunity to the users own area. Such files will be regularly removed from the system.
- Users are responsible for e-mail they send and for contacts made. E-mail should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property. Anonymous messages and chain letters must not be sent.
- Users should report any unpleasant material or messages received. The report will be confidential and will help protect others.
- The use of public chat rooms is not allowed.
- The school ICT systems may not be used for private business purposes, unless the Headteacher has given permission for that use. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- The security of ICT systems must not be compromised, whether owned by the school or by other organisations or individuals.
- Irresponsible use may result in the loss of Internet access.
- The system is monitored and inappropriate use will be detected.
- Learners must only use school software which is accessible on the desktop
- Users must not run software from portable devices such as USB's, external hard drives, DVD's or CD's

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful**.**

St.Bede's Catholic High School

Third Party Use Consent Form

St.Bede's Catholic High School **Responsible E-mail and Internet Use**	
Name:	**Address:**
Agreement **I have read and understand the school 'E-mail and Internet Use Good Practice - Rules for ICT Users' document. I will use the computer system and Internet in a responsible way and obey these rules at all times.**	
Signed:	**Date:**

Please complete, sign and return to the Network Manager at St.Bede's Catholic High School