

E-Safeguarding Policy



St. Bede's Catholic Voluntary Academy

We commit ourselves to love, respect and
serve one another as disciples of Jesus Christ

November 2015

St. Bede's Catholic Voluntary Academy

- Supervises children and young people's use at all times and is vigilant in the areas where young people have more flexible access;
- We use an appropriate and approved filtering system which blocks harmful and inappropriate sites;
- We have added additional user-level filtering, and can be appropriately adapted. Websites to be used with children and young people should be previewed by staff.
- If raw image searches are used staff vigilance is crucial
- Computer use is monitored and logged on all school equipment both inside and outside of school.
- Informs children, young people and staff that they must report any failure of the filtering systems directly to the classroom teacher. Our systems administrators report to and work with YHGfL where necessary;
- Manages access to Chat rooms and social networking sites and recommends those that are part of an educational network or approved Learning Platform;
- Has blocked children and young people's access to music download or shopping sites – except those approved for educational purposes.
- Requires students to individually sign an e-safety / acceptable use agreement form which is fully explained.
- Requires all staff, on induction, to sign an e-safety / acceptable use agreement form and keeps a copy on file;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse. Keeps a record, of any bullying or inappropriate behaviour for evidence in line with the school behaviour policy;
- Ensures the named child protection officer has appropriate training in E safety;
- Ensures parents provide consent for their child to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement.
- Makes information on reporting offensive materials, abuse / bullying etc available for children, young people parents and carers and staff;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

In this school:

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- Uploading of information to the school website is restricted to the E-learning Coordinator, website technician and the data manager. All teachers can upload information to the VLE.
- The school web site complies with the school's guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- Digital images /video of pupils are stored in the teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication;
- We do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website;
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- Pupils are only able to publish to their own 'safe' web-portal
- Pupils are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are taught about how images can be abused in their eSafety education program;

Student data and personal information

The school is responsible for the safeguarding of student data and information. When data is exported to external organisations for processing it is always done so in an encrypted manner.

If teachers require student information off-site they are encouraged to use the online encrypted data tool – Go4Schools.

If teachers require further information not held in Go4schools off-site they should follow the following procedure:

- A school IT technician should install a piece of encryption software onto their device.
- The IT technicians will show the teacher how to encrypt any student data.
- The encryption should be activated using a strong password.
- This password should be placed in a sealed envelope and placed in the school safe.

Social networking and personal publishing

Parents and teachers need to be aware that the Internet has online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control.

For use by responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published.

Examples include: facebook, blogs, wikis, Instagram, tumblr, MySpace, Bebo, Piczo, Windows Live Spaces, forums, bulletin boards, multi-player online gaming, chatrooms, instant messenger and many others.

- The schools will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.
- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for student use on a personal basis.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Students should be advised not to publish specific and detailed private thoughts.
- Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

Radicalisation

- Protecting children from the risk of radicalisation (PREVENT) is seen as part of schools' wider safeguarding duties, and is similar in nature to protecting children from other harms (eg drugs, gangs, neglect, sexual exploitation), whether these come from within their family or are the product of outside influences. The school is aware of the increased risk of online radicalisation, as terrorist organisation such as ISIL seek to radicalise young people through the use of social media and the internet. This is managed as part of this e-safety policy, linked with the safeguarding policy.

Acceptable Use Policy

Dear Parent/Guardian,

ST BEDE'S CATHOLIC VOLUNTARY ACADEMY COMPUTER AND INTERNET POLICY

The School's computer network is well established and plays a big part in the education of pupils and others at St. Bede's

In school, access to the Internet is provided for the purposes of educational research and learning. We have developed the following ICT policy for staff and students to provide rules and safeguards for appropriate use of the Internet.

If you wish your child to gain access to the Internet when appropriate, would students and parents/guardians please carefully read, sign and return the following agreement to your form tutor at school. The school will then keep the signed agreement on record.

Please detach the form at the bottom of this document and return to your form tutor

STUDENT AGREEMENT

- I am aware that computer use is monitored and logged on all school equipment both inside and outside of school.
- I understand that access to the Internet from St. Bede's School must be in support of educational research or learning, and I agree to the following:
- I will refrain from accessing any Newsgroups, links, list servers, web pages or other areas of cyberspace that would be considered offensive in the judgement of the school's Headteacher (or delegate) because of pornographic, racist, violent, illegal, illicit or other content.
- I will not use chat rooms unless as part of a teacher-led educational project.
- Accordingly, I am responsible for monitoring and appropriately rejecting materials, links, dialogues and information accessed/received by me.
- I will not use valuable Internet time playing non-educational games.
- The school has effective web and email content filtering, but not all offensive material will be automatically detected. I will not try to "cheat" the filtering system under any circumstances, and will not search for information of an offensive nature. If I feel that a website is unnecessarily filtered, instead of trying to "cheat" the filtering system, I will seek help and guidance from the network manager or member of ICT staff.
- I will be courteous and use appropriate language. I will refrain from using obscene, harassing or abusive language and will report any cases of such usage against me to my teacher, learning tutor or head of house.
- I accept responsibility to keep copyrighted material from entering the school. Therefore I will not download software, games, music, graphics, videos or text materials that are copyrighted. I will not violate any copyright laws by posting or distributing copyrighted materials.
- Plagiarism is unacceptable. Therefore I will use any downloaded material in an appropriate manner in assignments, listing its source in a bibliography and clearly specifying any directly quoted material.
- I will not reveal personal information, including names, addresses, credit card details and telephone numbers of others or myself.

- I will not damage computers, computer systems or networks.
- I understand that all school equipment will be subject to monitoring.
- I will not attempt to change any computer, monitor or software settings on any school computers without permission to meet a personal need.
- I will abide by the current sign-on procedures for access to the computer network, respect other student's work and not attempt to access other people's work on the network by using either aliases or passwords that are not mine.
- The entire network is protected by anti-virus software. Pupils and staff are advised to use anti-virus software on home computers and laptops. If a virus is reported on screen, a member of ICT staff should be informed immediately.
- The Network Manager carries out daily network backups. I will, however, attempt to save my own work correctly, and use sensible file management techniques at all times.
- Each student has a school e-mail address made available through the school's network. When using this web-based e-mail account, I will conform to the expectations set out in the points above.
- I will not take digital photographs, or edit digital images of staff or pupils without their consent.
- I will not attempt to use personal devices such as a mobile phone in the school unless the school/teacher gives permission and it is for educational use.
- I will not use my USB memory sticks on the school network. I will bring files into school using the school email address and eportal only.
- If I violate any of the terms of this agreement, I will be denied access to the Internet and/or computers for a time to be determined by the Headteacher and may face further disciplinary action as determined by the Headteacher. I am aware that each case will be considered on its merits.

IMPORTANT PARENTAL NOTE

Your son/daughter may have been involved with school events.

(Examples: Drama Performances, Talent Show, School Trips, Sponsored Bounce, Sports Teams.)

We often take photographs at such events.

The photographs may be displayed as a photo album within the website. Names of pupils WILL NOT be attached to the pictures.

IMPORTANT

If you DO NOT want photographs of your son/daughter participating in school events to be published on the school website either **now or in the future**, please contact me via letter or telephone as soon as possible.

Thank you for your continued support.

Yours sincerely,

Mrs M Travers
Headteacher

STUDENT AGREEMENT

Name *(Please Print Name)*Form

SignedDate

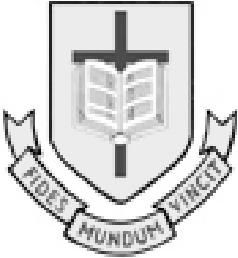
PARENTAL AGREEMENT

As the parent/guardian of(please complete), I hereby acknowledge that I have read the agreement on student use of computers and the Internet at St. Bede’s School and discussed it with my child. I understand that access is designed for educational purposes. I recognise that, while efforts will be made to monitor student use of computers and Internet, it is impossible for St. Bede’s School to continually monitor and restrict access to all controversial materials. I further acknowledge that, while questionable material exists on the Internet, the user must actively seek it and therefore is ultimately responsible for bringing such material into the school. I therefore do not hold the staff or Headteacher of St. Bede’s School responsible for any such materials acquired from the Internet.

Name (Please Print Name)

Parent or Guardian of Form

Signed Date

	Name of School	St. Bede's Catholic Voluntary Academy
	AUP review Date	November 2014
	Date of next Review	June 2015
	Who reviewed this AUP?	Mr N Brown Safeguarding group

Acceptable Use Policy (AUP): Staff

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, mobile technologies, equipment and systems.

- I am aware that computer use is monitored and logged on all school equipment both inside and outside of school.
- I understand that all school equipment is subject to electronic monitoring both inside and outside of the school buildings.
- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will only use the school approved, secure email system for any school business
- I will not browse, download or send material that could be considered offensive to colleagues and any other individuals.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or to be used by any individual than myself.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will ensure my personnel email accounts, mobile/home telephone numbers are not shared with children, young people or families.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that it is very important that the School Behaviour Policy is followed. All contact with parents should go through the House Leader and copies of any letters sent by Subject Leaders must be forwarded to the relevant House Leader and Learning Mentor. **It is school policy that any communication with parents must first be checked by the Headteacher.**
- I understand that if I wish to communicate with another member of staff about a student the behaviour Policy must be followed and any communication about a student at any stage of

the policy should be cc'd to student records. The address is:
studentrecords@stbedesscunthorpe.org.uk

- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that has not been approved by the School and meets its minimum security specification (i.e up to date approved Anti virus etc.)
- I will not use personal digital cameras or camera phones for transferring images of pupils or staff without permission.
- I will use the school's Learning Platform in accordance with school and providers policies and guidance.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any software or device relating to personal use to ensure it does not breach the schools policies.
- I will ensure any confidential data that I wish to transport from one location to another is adequately protected.
- I understand that The Data Protection Act requires that any information seen by me with regard to staff or pupil information, held within any schools system (e.g. MIS, Learning Platforms etc), will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will ensure I am aware of digital safe-guarding issues so they are appropriately embedded in my classroom practice.
- I understand that all computer equipment will be subject to electronic monitoring both inside and outside of the school.
- I will only use LA systems in accordance with any Corporate policies.
- I understand that failure to comply with the Acceptable Use Policy could lead to disciplinary action.

Laptop Agreement

- It is expected that teachers who are issued with laptops agree to the School's Acceptable Use Policy (AUP), in particular that inappropriate content is not be placed on the laptop.
- The laptop is for work use. Teachers are encouraged to use the laptop computer outside work hours; however, if other family members use the laptop they must be made aware of this agreement and abide by its rules. The teacher will be held responsible for any infringements of this agreement by other family members.
- The laptop remains the property of the school at all times.
- Teachers are both permitted and encouraged to take their laptop computers home and to work from home. The laptop is always to be available at school for work.

- The laptop is to be returned to the school at the end of each academic year, or earlier if employment is terminated. With approval from the headteacher the laptop may be borrowed for Summer holiday use for professional opportunities.
- Teachers are held responsible for any loss or damage to the laptop computer and may be asked to pay a monetary charge if deemed necessary by the headteacher.
- Teachers must take adequate care and security precautions when using their computer, for example, teachers will not leave their laptop computer in an unlocked room, unsecured overnight at school nor in any car while the car is unoccupied.
- Teachers will immediately report any damage or loss of the laptop to the School.
- In the first instance teachers will refer any problems in using the laptop computer to a member of the IT Department.
- To facilitate learning and teaching, teachers will be given administrative rights on the devices. However teachers are not permitted to install any unlicensed software.