The Venerable Bede CE Academy

ICT & Acceptable Use Policy

Reviewed February 2014

Scope of the Policy

This policy applies to all members of the Venerable Bede Academy (including staff, governors, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school / academy ICT systems, both in and out of the academy.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the academy, but are linked to membership of the academy.

The academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

The academy uses a 'filtered Internet Service' that stops as much of the unsuitable material as possible from entering the school system or being displayed on a computer being used by students. It is virtually impossible to guarantee the removal of all such materials.

Pupils in school are unlikely to see inappropriate content in books due to selection by publisher and teacher. The Internet is a communications medium and is freely available to any person wishing to send e-mail or publish a Website. Staff will need to ensure that access is appropriate to the user. Some secondary pupils, as part of a supervised project, might need to access adult materials, for instance a set novel that includes references to sexuality. Teachers might need to research areas, for example drugs, medical conditions, bullying or harassment. Systems are available that enable different levels of filtering to be applied by time, location or user, but use of these facilities may incur charges from our Internet Service Provider.

In common with other media such as magazines, books and video, some materials available via the Internet are unsuitable for pupils. The academy will supervise pupils and take all reasonable precautions to ensure that users access only appropriate material. This will include adult supervision during open access periods. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on a terminal. The academy cannot accept liability for the material accessed, or any consequences thereof.

- Methods to quantify and minimise the risk will be reviewed;
- Pupils, staff, parents and governors all have a contribution to make to ensure that unsuitable material does not appear on the school system;
- Staff will check that the sites selected for student use are appropriate to the age and maturity of students;
- From time to time, checks may be carried out by senior staff to monitor the effectiveness of Internet access strategies;
- Access levels will be reviewed as pupils' Internet use expands and their ability to retrieve information develops (as filtering systems develop);
- Senior staff will ensure that occasional checks are made on files to monitor compliance with the school's Internet Access Policy.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the academy:

Governors:

Governors are responsible for the approval of the ICT & Acceptable Use Policy and for reviewing the effectiveness of the policy.

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety may be delegated to other members of staff.
- The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headteacher / Senior Leaders are responsible for ensuring that staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

Designated Person (s) for Safeguarding:

- has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff

ICT/Data / Technical staff:

The ICT/Data Manager / Technical Staff / Co-ordinator for ICT / Computing is responsible for ensuring:

- that the academy's technical infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy , is applied and updated on a regular basis.
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leader; / ICT/Data Manager for investigation / action / sanction
- Securus monitoring software is updated as agreed in school / academy policies.

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current academy e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher / Senior Leader ; / ICT Data Manager for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems.
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Pupils:

- are responsible for using the academy digital technology systems in accordance with the Pupil Acceptable Use Policy.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the academy's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the academy in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / VLE and on-line student / pupil records
- their children's personal devices in the school / academy (where this is allowed)

When will Access to the Internet be Allowed?

The School will allocate access to the Internet on the basis of educational need. This will usually include all staff and all students and will include an e-mail address.

- Internet access is a necessary part of planned lessons. It is an entitlement for students based on responsible use;
- Parents will be informed that students will be provided with supervised Internet access where it is important to their education. They will be asked to signify if they are unhappy about their child's work appearing on the Internet;
- Pupils undertaking personal study will be required to be responsible for appropriate use of the Internet. Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The academy will take every opportunity to help parents understand

Staff Internet Use

Staff use of the internet is restricted to professional use only unless permission has been given by the Headteacher. The internet on academy computers should not be used for any political purpose, personal gain or social use e.g. personal emails, booking holidays, private financial matters or social networking. Restrictions may also apply to any laptops that are booked out for use at home.

- Random checks on internet history may be undertaken and logs maintained.
- Inappropriate use of the internet may lead to disciplinary action.
- All staff and pupils will be expected to accept the terms and conditions of the 'Acceptable Use' policy on the desktop each time they sign into their individual accounts.

School System and User's Files

- Virus protection will be installed and updated regularly;
- The ICT/Data Manager will ensure that the system has the capacity to take increased traffic caused by Internet use;
- The security of the whole system will be periodically reviewed with regard to threats to security from Internet access;
- Use of e-mail to send attachments will be limited to files created by students that have been virus checked and approved by a member of staff;
- All Internet traffic will be virus scanned automatically on receipt from the ISP.
- Files may be uploaded and downloaded via the VLE.

Use of the Internet in the Classroom

- Internet access will be planned to enrich and extend learning activities as an integrated aspect of the curriculum;
- Internet Access is intended for work and educational use only;
- Pupils will be given clear objectives for Internet use;
- Pupils will be provided with lists of relevant and suitable Websites;
- No websites with pornographic, racist or sexist or otherwise offensive content are to be viewed at any time; Accidental access to such websites must be immediately reported to Teacher / ICT/Data Manager.
- At no time should pupils or staff participate in Chat-Room, Bulletin Board activity.
- Pupils will be educated in taking responsibility for Internet access;
- Pupils will be informed that checks can be made on files held on the system;
- Pupils using the Internet will be supervised appropriately;
- Pupils will not send personal data over the Internet.

Information on the Internet

ICT teaching will be widened to incorporate Internet content issues, for instance the value and credibility of Web materials in relation to other media.

- Students will be taught to validate information before accepting it as true, an important aspect of higher levels of subject teaching;
- When copying materials from the Web, students will observe copyright;
- Students will be made aware that the writer of an e-mail or the author of a Web page may not be the person claimed;
- Students will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV;
- Students will be encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

Electronic Mail

All email sent to and from the academy is scanned for virus's and all emails are logged. Pupils need to be aware that the school reserves the right to check and monitor files on their work areas of the server and mail as it is sent and received if there is evidence to make this necessary. ICT teaching will be widened to incorporate Internet content issues, for instance the value and credibility of Web materials in relation to other media.

- Pupils are expected to use e-mail and will be given individual e-mail accounts;
- E-mail is intended for Educational & Work Related Use only;
- The forwarding of chain letters is banned;
- The completion of order forms or questionnaires on behalf of others on the Internet shall not be allowed;
- E-mail messages on school business (e.g. arranging a work placement) must be approved before sending;
- E-mail will only be sent or received as part of the lessons unless specifically authorised;
- The content of all email (incoming & outgoing) are subject to monitoring at any time;
- No email with pornographic, racist, sexist or otherwise offensive content is to be sent or received; (staff and students)
- All email to be scanned for viruses upon receipt;
- If an email is received from an unfamiliar sender it should be deleted immediately unless instructed otherwise by a member of the IT Team;
- In-coming e-mail will be regarded as public. There may be occasions when a pupil or ex pupil emails a member of staff ie re homework deadlines. Where a response is to be made, the member of staff will cc another member of staff into the email for security purposes. Only school email addresses should be used when contacting either pupils or parents/carers.

Child Pornography

The Internet has now become a significant tool for the distribution of child pornography. Some adults also use the Internet to try to establish contact with children with a view to "grooming" them for inappropriate or abusive relationships. The use of social media is of particular concern in this context.

This is one of the main reasons why social media sites are not permitted at the Venerable Bede Academy.

Concerns about the hazards that the Internet may present for children have long been recognised and information is currently available to address those concerns. For example Northumbria Police have produced a leaflet "Safety tips for parents and children using the Internet" to be found at www.northumbria .police.uk.

Communications with Users and Parents

- All staff and students agree with the school Internet Access Policy. Staff should be given opportunities to discuss the issues and develop good teaching strategies. All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the Internet Access Policy, and its importance explained;
- Parents' attention will be drawn to the Policy through appropriate channels in newsletters, the school brochure and on the school Website;
- Rules for Internet access will be posted near computer system.
- The academy may communicate by SMS and email to parents.

Computer Use

- Computers in the Venerable Bede Academy are intended for educational and approved work related use only
- No software programs or files are to be installed, deleted, moved or altered on all pc's including laptops without prior consultation with the IT Team
- The approved applications are to be installed by the IT Team
- All computers and contents therefore are subject to periodic search (with or without notification of the IT Team)
- All PC's should be logged off and shut down nightly
- When PC's are not in use students and staff are responsible for locking pc's or using screensaver passwords.
- Networked Access and activity may be audited and monitored by the IT Team
- Each students/staff's password is unique and must not be supplied or divulged to any individual for any reason other than the IT Team
- If a password has been forgotten, compromised or otherwise rendered unusable, contact the IT Team immediately
- All passwords will expire within 60 days of their creation
- All new passwords are to be at least 6 (six) characters in length and unique