Bilton Church of England Junior School

`

Policy for: E-safety

Formed by: Mrs Satsangi

Date of original formation: September 2015

Ratified by the Governing Body on:

Our Christian ethos is at the heart of Bilton C/E Junior School and its community, where we inspire each and all, to grow and flourish within a creative and supportive environment, embracing change and relishing new challenges.

We rejoice in our children as individuals and ensure each and every child is empowered to achieve their full potential through inspirational learning experiences and high aspirations for ourselves and others.

Table of review and modifications

Date reviewed	Page number of changes	Summary of changes made

Bilton Church of England Junior School

E-safety

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning.

We at Bilton C of E Junior School are committed to ensuring that our whole school community is able to operate with safety and confidence whenever and wherever they use the Internet or mobile technologies. We understand the need to educate users about the benefits and risks of using technology and provide safeguards to enable them to control their online experience.

Who has developed this policy for e-safety at Bilton C of C Junior School?

Committee for e-safety within Bilton C of E Junior School are:

- Computing subject leader (Mrs Satsangi)
- Safeguarding Designated person, SMT & E-safety officer (Mrs A Norton)
- Safeguard Designated person and Home School support (Mrs S Hodgson)
- ICT support (Mrs J Thomas)
- Governor for safeguarding (Kenny Nessling)

Other stakeholders involved in the development of this policy are:

- Parents (PPF)
- Pupils (JLT)

Roles and Responsibilities

Governors / Board of Directors:

- Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors /Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor (it is suggested that the role may be combined with that of the Child Protection / Safeguarding Governor). The role of the E-Safety Governor will include:
  - regular meetings with the E-Safety Officer
  - regular monitoring of e-safety incident logs
  - regular monitoring of filtering / change control logs
  - reporting to relevant Governors / Board / committee / meeting

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 will be delegated to the E-Safety Officer.
- The Headteacher, Chair of Governors and another member of the Senior Senior Management Team should be aware of the procedures to be followed in the event of an e-safety allegation being made against a member of staff.

- The Headteacher /Senior Leaders are responsible for ensuring that the E-Safety Officer and other relevant 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.
- The Senior Management Team will receive regular monitoring reports from the E-Safety Officer.

E-Safety Officer:

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and 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
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

The E-safety committee and support from Technical Staff / Co-ordinator for ICT / Computing are responsible for ensuring:

- **that the school's technical infrastructure is secure and is not open to misuse or malicious attack**
- **that the school meets required e-safety technical requirements and any local authority E-Safety Policy / Guidance that may apply.**
- **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 and that its implementation is not the sole responsibility of any single person
- 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 / website/ remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / E-Safety Coordinator / Safeguarding DPs for investigation / action / sanction
- that monitoring software / systems are implemented and updated regularly

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school 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 / E-Safety Officer/ ICT support / ICT subject leader for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems (as per Staff Use of Social Networking Policy, Child Protection Policy and Staff Handbook)
- 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 and know how to report any concerns
- 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 students / 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.

Child Protection / Safeguarding Designated Person

- should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:
  - sharing of personal data
  - access to illegal / inappropriate materials
  - inappropriate on-line contact with adults / strangers
  - potential or actual incidents of grooming
  - cyber-bullying

E-Safety Committee (parents/carers and pupils included through consultation)

Members of the E-safety Committee will assist the E-Safety Officer with:

- the production / review / monitoring of the school e-safety policy / documents.
- the production / review / monitoring of the school filtering policy and requests for filtering changes.
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the pupils about the e-safety provision
- monitoring improvement actions identified through use of the 360 degree safe self review tool

Pupils:

- are responsible for using the school digital technology systems in accordance with the Student / 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 school'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 school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school 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
- their children's personal devices in the school and at home

Community Users

Community Users who access school systems / website as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

Acceptable Use Agreement

Our school expects both pupils and adults in school to agree to be responsible users.

Our Acceptable Use Agreements are intended to ensure:

- that pupils, staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

Acceptable Use Agreements are issued to every pupil and member of staff / volunteer at the start of each academic year. They are issued to new starters as necessary. Pupil and parent AUAs are kept by class teachers. Adult AUAs to kept by Home School Support.

How are members of the school community prepared for e-safety?

Staff receive regular e-safety training and volunteers / those who are not able to receive internal training.

Pupils receive special e-safety assemblies and termly e-safety sessions which are reinforced during learning sessions where ICT is in use.

How are E-safety incidents monitored?

All e-safety incidents must be reported to ICT support / subject leader / safeguarding DPs which are then logged on the incident log which is stored in Teacher's drive. Where appropriate, a green safeguarding form is raised and given to a DP.

Sanctions (constructed in consultation with JLT and PPF)

If a user is found to have used ICT devices at school inappropriately, it is at the class teacher's discretion what sanctions to put in place / a member of Headteacher / Chair of Governors' discretion if involving an adult within school. As a guide:

Unacceptable language

- If a user has genuinely mis-typed a word, the matter is recorded as such and left at that.
- If a user is believed to have deliberately typed unacceptable language the matter is recorded, parents are informed and the user has a discussion with the class teacher about using pleasant language as in the school's covenant.
- In the case of an adult, the Headteacher / Chair of Governors will deal with the user.
- If the user continues to use inappropriate language, the matter is dealt with by SMT, Home School support and parents.

Inappropriate searches / images

- If a user has genuinely accidently come across an image / searched using an inappropriate word, the matter is recorded as such and left at that, after discussing the matter sensitively with the child. Depending on the image, parents may be informed for their information.
- If a user is believed to have deliberately searched for / views inappropriate images, the matter is recorded and the user has a discussion with the class teacher about e-safety and parents are informed. Further sanctions are then decided.
- If the user continues to make deliberate inappropriate searches the matter is dealt with by SMT, Home School support and parents.
- In the case of an adult, the Head teacher / Chair of Governors will deal with the user.

Unpleasant emails

- If a user communicates in a manner which they would not do in real life (ie sending inappropriate images, making unpleasant comments about others, spamming etc) class teacher is informed and they have discussion about appropriate use with the user.
- If the user continues to use email inappropriately, the account is blocked and parents are informed. Further action is agreed between class teacher and parents.
- If cyberbullying is identified, the SMT and Home School support will deal with the matter, in accordance with the Bullying and Behaviour Policies.
- In the case of an adult, the Head teacher will deal with the user.

<u>Teaching and learning</u>

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. Our school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- Inclusion in the National Education Network which connects all UK schools;
- Educational and cultural exchanges between pupils locally, nationally and internationally;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with the LA and DfES;
- Access to learning wherever and whenever convenient.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and be given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to a member of the e-safety committee.
- Our school will ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

Our pupils will be taught at a time appropriate to them to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

Managing Internet Access

Information system security

- The security of the school information systems will be reviewed regularly.
- Sophos Anti-Virus protection is installed and updated regularly.
- The school uses Virgin Broadband with BT as back up Broadband
- Firewall and filtering is provided by Smoothwall
- The school provides an additional level of protection and monitoring through its deployment of policy central. Reports are monitored daily.
- Portable media may not be used without specific permission and a virus check.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked by policy central and monitored by ICT subject leader/ network manager (ICT Support).
- The ICT/ Computing Subject Leader and ICT support will review system capacity regularly through ICT Technical visits provided by Launch System and will be advised appropriately from Launch.

E-mail

- Pupils will be issued with name@biltonjuniorschool.co.uk email accounts for their using during their time at Bilton Junior School. Pupils will receive these when parental consent is obtained and accounts will be deleted on leaving the school.
- Pupils may only use approved e-mail accounts on the school system (name@biltonjuniorschool.co.uk).
- Pupils can only send emails to other @biltonjuniorschool.co.uk email address from their @biltonjuniorschool.co.uk email address. Pupils will only send e-mails to people they know and trust.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Use of words included in the Policy Central 'banned' list will be monitored, reviewed, detected and logged..
- The forwarding of chain letters is not permitted.
- Staff - E-mails sent to an external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper (in accordance with the Staff Email Policy).

Published content and the school web site

- The contact details on the Web site is the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The website managers will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Email addresses should be published carefully, to avoid spam harvesting.
- The Website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully.
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site or learning platform. (see Use of Images policy)
- Images of staff should not be published without consent.

Social networking and personal publishing

- Social networking sites and newsgroups will be blocked (unless with express, written prior agreement of Headteacher as per Staff Use of Social Networking Sites in School policy).
- Pupils will be supported in never giving out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils through, for example, e-safety Parent workshops.
- Pupils will be encouraged to think carefully before posting picture or video online.
- Staff should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Staff should be encouraged to invite known friends only and deny access to others. Staff and parent friendships on social networking sites are actively discouraged. (See Staff Handbook and Staff Use of Social Networking Policy)
- Staff should ensure that any forms of e-communications do not bring themselves, their school or their profession into disrepute. This is outlined on the staff acceptable use form which all staff should sign.
- Schools should be aware that bullying can take place through social networking especially when a space has been set up without a password and others are invited to see the bully's comments. Any forms of bullying should be reported to the Headteacher and will be dealt with in accordance with the Bullying Policy.

Managing filtering

- The school will work in partnership with Smoothwall, Launch systems and Network manager (ICT Support)to ensure filtering systems are as effective as possible. Regular checking of the filtering system will take place by Home School Support and ICT Support in the form of regular 'dips'.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school e-Officer and ICT Support.
- Home School Support and ICT Support will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported to appropriate agencies such as CEOP and the police / local safeguarding board.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time by staff or pupils. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Portable storage devices will be encrypted.

Policy Decisions

Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the acceptable ICT use agreement, 'E-Safety Staff / Volunteer Acceptable Use Agreement ', before using any school ICT resource.
- Within our school, pupil access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Only approved search engines will be used on the curriculum network.
- Children may be asked to type in website addresses. Where appropriate, links will be made by staff and placed in a shared folder for children to access, having checked them for educational purpose and appropriateness first.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to read and acknowledge the school's 'Acceptable Use Agreement' issued to pupils.

Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The ICT subject leader, in conjunction with the Headteacher, will ensure that the E-Safety Policy is implemented and compliance with the policy monitored.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher / Chair of Governors who will deal with the situation in accordance with the Whistleblowing Policy.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. Notify a designated person: Head teacher Deputy or Home School Support.
- Pupils and parents will have access to the Complaint's Policy via the school's website.
- Parents and pupils will need to work in partnership with staff to resolve issues.

Community use of the Internet

- The school liaises with local organisations to establish a common approach to e-safety.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

Communications

Introducing the e-safety policy to pupils

- 'Top 10 Tips to stay safe online' and 'Rules for Responsible ICT device and Internet Use' poster are displayed in all classrooms.
- E-safety assembly.
- E-safety page on the school website Be SMART stay SAFE on line
- Pupils are taught that Internet use is only with adult supervision.
- An e-Safety curriculum is used to raise the awareness and importance of safe and responsible internet use.
- This is done through an on-going computing / E-safety curriculum, covering both school and home use.
- Instruction in responsible and safe use precedes Internet access.

Staff / Volunteers and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff should not use personal email or mobile technology to contact pupils or parents/carers. If contact is necessary, a school telephone / email account should be used.
- All staff will read and sign the 'E-Safety Staff / Volunteer Acceptable Use Agreement'.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

- Staff development in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

Enlisting parents' support

- Parents' attention will be drawn to the School E-Safety Policy in the bulletin, with the school prospectus and via the school's website.
- Parents will sign the 'E-Safety Parents Acceptable Use Agreement' and are expected to support the schools policy on e-safety.
- Internet issues will be handled sensitively to inform parents without alarm.
- A partnership approach with parents will be encouraged which includes parents' evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

Bring Your Own Device (BYOD)

Pupils are permitted to bring Kindles to school for reading purposes only, on an individual basis with prior written agreement between parents and class teacher.

If children are found to be using their Kindle for other purposes, parents will be contacted and permission will be reviewed.

Class teachers are responsible for recording and monitoring this and will pass this on information on to the child's next class teacher.

USB portable storage drives: To avoid transferring a virus on personal pen-drives, pupils are expected to email work to themselves at school. Staff may use portable storage devices if they have been check for viruses and are encrypted.

Passwords (See Password policy)

All staff set their own personal password from the default password.

Pupils set their own password after being taught about how to authenticate their password in accordance with BECTA guidelines.

Staff and pupils are informed of the importance of keeping their password secure and are encouraged to change it every term or if they consider their account is at risk.