Jesus said *'I have come so that you might have life - life in all its fullness'* St John's gospel Chapter 10, verse 10

Brill Church of England School

E-Safety Policy

Policy Reviewed	**Sept '18**	**Sept 2019**			
Policy Owner	**J.Clayton**	**J.Clayton**			
Signed Headteacher					
Review date	**Sept '19**	**Sept 2020**			

Aim of this policy

To provide our pupils with the knowledge, skill and understanding from which they can make informed and safe choices and decisions regarding their use of the internet and emerging technologies.

Teaching and learning

Why is Internet use important?

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 functions. Internet use is part of the statutory curriculum and a necessary tool for learning.

Managing Information Systems

How will information systems security be maintained?

- Users must act reasonably – e.g. the downloading of large files during the working day will affect the service that others receive. Brill Church of England Primary School's internet service provider (Updata) has in place firewalls and switches to prevent unauthorised access.
- The security of the school information systems will be reviewed regularly.
- •Workstations are secured with passwords and staff/student accounts.
- •The school's server is located securely and physical access is restricted.
- •Users agree to acceptable usage that may be monitored by the school. This includes the use of wireless devices.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Bucks CC advisers and the school's technical support team (provided by BITES). This includes strategies for keeping our operating system safe.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- •Data protection issues to be considered in line with our data protection policy
- 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.
- The ICT co-ordinator/network manager will review system capacity regularly.

How will e-mail be managed?

- Staff and pupils may only use approved Bucks GfL e-mail accounts.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and may be restricted.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Checks for unsuitable content and viruses in email are done through TIO (our ICT provider).

- •Access to Bucks GFL e-mail accounts is permitted. Access to external webbased email is not permitted. This is blocked through filtering from our internet service provider.

How will published content be managed?

- The contact details on the website should be the school address, e-mail and telephone number.
- Staff or pupils' personal information must not be published.
- E-mail addresses should be published carefully, to avoid unsolicited spam mail. The office email is available on website.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- •The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Can pupil's images or work be published?

- Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Parental consent regarding use of a pupil's image is indicated on the home/school agreement and will be checked before an image is electronically published. If consent is not given the image is not to be used.

How will social networking and personal publishing be managed?

- 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 e.g. Housenumber, street name or school.
- Teachers' official blogs or wikis should be password protected and run from the school website or VLE.
- 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.
- Pupils will be taught these skills through both stand-alone lessons (CEOP planning) as well as alongside day-to-day teaching where relevant.

How will filtering be managed?

- The school will work with Turn it on to ensure that systems to protect pupils are regularly reviewed.
- •Turn it On which are our support for Computing effectively filter available internet content.
- If staff or pupils discover unsuitable sites, the URL must be reported to the e-Safety Coordinator (Jenny Clayton)
- The co-ordinator 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 IWF or CEOP (addresses later).
- The school's filtering strategy will be designed by educators to suit the age and curriculum requirements of the pupils, advised by Bucks GfL.

How can emerging technologies be managed?

- 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. The sending of abusive or inappropriate text messages is forbidden.
- The school should investigate wireless, infra-red and Bluetooth communication technologies.
- Staff will be issued with a school phone where contact with pupils is required. How should personal data be protected?
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Policy Decisions

How will Internet access be authorised?

- The school, through BITES and Updata, will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff must read and sign the 'e-safety Code of Conduct' before using any school ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- At Key Stage 2, pupils may be researching and looking more freely across internet content. The content available is filtered by our internet service provider. Pupils use will be monitored by teachers.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form for pupil access.

How will risks be assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Bucks CC can accept liability for the material accessed, or any consequences resulting from Internet use.

- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- 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.

How will e-safety complaints be handled?

- 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.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Discussions will be held with the local Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.
- Sanctions will be within the school discipline policy.

Communicating the Policy

How will the policy be introduced to pupils?

- E-Safety rules will be posted in rooms with Internet access.
- Pupils will be informed that network and Internet use will be monitored.
- An e-safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use. An Internet safety workshop for parents will be run annually.
- Instruction in responsible and safe use should precede Internet access.
- An e-safety module will be included in the ICT programmes covering both school and home use. This planning comes from the National Curriculum and through visits from our local PSCO for both parents and pupils.
- E-safety will also be taught whenever it is relevant in other lessons/subjects.

How will the policy be discussed with staff?

- All staff will be given the School e-Safety Policy and its application and 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 that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

How will parents' support be enlisted?

- Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.

• A partnership approach with parents will be encouraged. This will include an annual parent workshop with demonstrations and suggestions for safe home Internet use run by McAfee.
• Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
• Interested parents will be referred to organisations listed in section e-Safety Contacts and References.

E-Safety Contacts and References Bucks ICT Support Team Website

http://www.bucksict.org.uk
Bucks GfL Website http://www.bucksgfl.org.uk
BBC Chat Guide http://www.bbc.co.uk/chatguide/
Becta http://www.becta.org.uk/schools/esafety
Childline http://www.childline.org.uk/
Child Exploitation & Online Protection Centre http://www.ceop.gov.uk
Grid Club and the Cyber Cafe http://www.gridclub.com
Internet Watch Foundation http://www.iwf.org.uk/
Internet Safety Zone http://www.internetsafetyzone.com/
Kidsmart http://www.kidsmart.org.uk/
NCH – The Children's Charity http://www.nch.org.uk/information/index.php?i=209
NSPCC http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm
Stop Text Bully www.stoptextbully.com
Think U Know website http://www.thinkuknow.co.uk/
Virtual Global Taskforce – Report Abuse http://www.virtualglobaltaskforce.com