Beaufort Primary School

E-Safety Policy

Date of original Policy	June 2015
Author	C Dewberry / H Hutchison
Approved by	Curriculum Committee
Last Review Date	15th March 2018
Next review Date	Spring 2019

Policy reviewed	Signed:	Date:
Policy reviewed	Signed:	Date:
Policy reviewed	Signed:	Date:
Policy reviewed	Signed:	Date:

Contents:

Statement of intent

At Beaufort Primary School, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

1 Legal framework

1.2 This policy also has regard to the following statutory guidance:
- DfE (2016) 'Keeping children safe in education'

1.3 This policy will be used in conjunction with the following school policies and procedures:
- Acceptable Usage and Laptop Protocol
- Anti-Bullying Policy
- Behaviour Policy
- Data Protection and Information Security Policy
- Mobile Devices Policy
- Safeguarding Policy
- Social Networking in Safety
- Computing Policy
- PSHE Policy
- Code of Conduct for Safe Practice

2 Use of the internet

2.1 The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

2.2 Internet use is embedded in the statutory curriculum and is therefore an entitlement for all pupils, though there are a number of controls the school is required to implement to minimise harmful risks.

2.3 When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:
- Access to illegal, harmful or inappropriate images

- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

2.4 **Different technologies**:

New internet and online technologies are enhancing communication and the sharing of information. Current and emerging internet and online technologies used in school and, in many cases more importantly, used outside of school by children include:

- The internet – World Wide Web
- E-mail
- Instant messaging, e.g. Instant Messenger
- Web-based voice and video calling, e.g. Skype
- Online chat rooms
- Online discussion forums
- Social networking sites, e.g. Facebook
- Blogs and micro-blogs, e.g. Twitter
- Podcasting, e.g. audio downloaded to MP3/4 player or other device
- Video broadcasting, e.g. YouTube
- Music and video downloading, e.g. iTunes, YouTube
- Mobile phones with camera and video functionality
- Smart phones with e-mail, messaging and internet access

3 Roles and responsibilities

3.1 It is the responsibility of all staff to be alert to possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside of the school, and to deal with incidents in line with school policy.

3.2 The governing body is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils. The ICT Technician is employed to check systems are effective.

3.3 The E-Safety officer is the Headteacher, Carla Dewberry, and is responsible for ensuring the day-to-day E-Safety in the school, and managing any issues that may arise.

3.4 The Headteacher / E-Safety officer is responsible for ensuring that staff receive CPD in line with SIP.

3.5 The Headteacher / E-Safety officer will provide all relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach pupils about online safety.

3.6 The Headteacher and School Business Manager will ensure there is a system in place which monitors E-Safety in the school, keeping in mind data protection requirements.

3.7 The computing co-ordinators will regularly monitor the provision of E-Safety in the school and will provide feedback to the Headteacher.

3.8 The computing co-ordinators will ensure that all members of staff are aware of the procedure when reporting E-Safety incidents, and will keep a log of all incidents recorded. This will be passed to the Headteacher/SBM and ICT Technician.

3.9 Cyber bullying incidents will be reported in accordance with the school's Anti-Bullying Policy.

3.10 The governing body will evaluate and review this E-Safety Policy on an annual basis, taking into account the latest developments in ICT and the feedback from staff/pupils.

3.11 The Headteacher will review and amend this policy with the computing co-ordinators, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.

3.12 Teachers are responsible for ensuring that E-Safety issues are embedded in the curriculum and safe internet access is promoted at all times.

3.13 All staff are responsible for ensuring they are up-to-date with current E-Safety issues, and this E-Safety Policy.

3.14 All staff will ensure they understand and adhere to our Acceptable Usage and Laptop Protocol, which they must sign and return to the SBM.

3.15 The Headteacher is responsible for communicating with parents/carers regularly and updating them on E-Safety issues through the website or in newsletters.

3.16 All pupils are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour.

4 E-Safety education

4. 1 **Educating pupils:**
- An E-Safety programme is established and taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of new technology both inside and outside of the school.

- Pupils will be taught about the importance of E-Safety and are encouraged to be critically aware of the content they access online, including extremist material and the validity of website content.
- Clear guidance on the rules of internet use will be presented in classrooms.
- Pupils are instructed to report any suspicious use of the internet and digital devices.
- PSHE lessons will be used to educate pupils about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.
- The school will hold E-Safety events, such as Safer Internet Day and Anti Bullying Week, to promote online safety.

4.2 **Educating staff**:
- The annual School Improvement Plan identifies priorities for a programme of E-Safety training opportunities.
- All staff participate in E-Safety training to ensure they are aware of current E-Safety issues and any changes to the provision of E-Safety, as well as current developments in social media and the internet as a whole.
- All staff employ methods of good practice and act as role models for pupils when using the internet and other digital devices.
- All staff are educated on which sites are deemed appropriate and inappropriate.
- All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.
- New staff induction packs include the E-Safety policy.
- The Headteacher will act as the first point of contact for staff requiring E-Safety advice.

4.3 **Educating parents/carers**:
- E-Safety information will be directly delivered to parents/carers through a variety of formats, including newsletters, the school website and social media.

5   E-Safety control measures

5.1 **Internet access**:
- Internet access will be authorised once parents/carers and pupils have returned the signed consent form in line with our Responsibe Internet and Email Use Agreement.
- Management systems will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.
- Effective filtering systems will be established to eradicate any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.
- Filtering systems will be used which are relevant to pupils' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.

- The governing body will ensure that use of appropriate filters and monitoring systems does not lead to 'over blocking', such that there are unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the Headteacher and referred to the ICT technician.
- All school systems will be protected by up-to-date virus software.
- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.
- Master users' passwords will be available to the Headteacher for regular monitoring of activity.
- Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times in line with school policies.
- Personal use will only be monitored by the Headteacher for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy.

5.2 **Email**:
- Staff will be given approved email accounts and are only able to use these accounts.
- No sensitive personal data shall be sent to any other pupils, staff or third parties via email.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

5.3 **Social networking**:
- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the Headteacher.
- Pupils are regularly educated on the implications of posting personal data online outside of the school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.
- Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.
- Staff are not permitted to publish comments about the school which may affect its reputability.
- Staff are not permitted to access social media sites during teaching hours unless it is justified to be beneficial to the material being taught. This will be discussed with the Headteacher prior to accessing the social media site.

5.4 **Published content on the school website and images**:
- The Headteacher and SBM will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- Contact details on the school website will include the phone number, email and address of the school – no personal details of staff or pupils will be published.

- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents/carers has been received.
- Pupils are not permitted to take or publish photos of others without permission from the individual.
- Staff are able to take pictures, though they must do so in accordance with school policies in terms of the sharing and distribution of such. Staff will not take pictures using their personal equipment.
- Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

5.5 **Mobile devices and hand-held computers**:
- The Headteacher may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use.
- Pupils are not permitted to access the school's Wi-Fi system at any times using their mobile devices and hand-held computers.
- Mobile devices are not permitted to be used during school hours by pupils or members of staff.
- Staff are permitted to use hand-held computers which have been provided by the school, though internet access will be monitored for any inappropriate use by the E-Safety officer when using these on the school premises.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- The school will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.

5.6 **Network security**:
- Network profiles for pupils and staff members will be used when accessing the ICT systems within the school.
- Passwords should be stored using non-reversible encryption.

5.7 **Virus management**:
- Technical security features, such as virus software, are kept up-to-date and managed by the ICT Technician.
- The ICT Technician will ensure that the filtering of websites and downloads is up-to-date and monitored.

6 Cyber bullying

6.1 For the purpose of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images online.

6.2 The school recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.

6.3 The school will regularly educate staff, pupils and parents/carers on the importance of staying safe online, as well as being considerate to what they post online.

6.4 The school has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-Bullying Policy.

6.5 The Headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a pupil.

7 Reporting misuse

7.1 Beaufort Primary School will clearly define what is classed as inappropriate behaviour in the Responsible Internet and Email Use Agreement, ensuring all pupils and staff members are aware of what behaviour is expected of them.

7.2 Inappropriate activities are discussed and the reasoning behind prohibiting activities due to E-Safety are explained to pupils as part of the curriculum in order to promote responsible internet use.

7.3 **Misuse by pupils**:
- Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the Headteacher
- Any pupil who does not adhere to the rules outlined in our Responsible Internet and Email Use Agreement and is found to be wilfully misusing the internet, will have a letter sent to their parents explaining the reason for suspending their internet use.
- Complaints of a safeguarding nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with our Safeguarding Policy.

7.4 **Misuse by staff**:
- Any misuse of the internet by a member of staff should be immediately reported to the Headteacher.
- The Headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff in line with LA policies.

7.5 **Use of illegal material**:
- In the event that illegal material is found on the school's network, or evidence suggest that illegal material has been accessed, the police will be contacted.
- If a safeguarding incident is suspected, the school's safeguarding procedure will be followed.

8 Monitoring and review

8.1 The E-Safety officer and computing co-ordinators will evaluate and review this E-Safety Policy on an annual basis, taking into account the school's E-Safety calendar, the latest developments in ICT and the feedback from staff/pupils.

8.2 This policy will also be reviewed on an annual basis by the governing body; any changes made to this policy will be communicated to all members of staff.

8.3 Members of staff are required to familiarise themselves with this policy as part of their induction programmes.

APPENDIX 1

Responsible Internet and Email Use
Pupil agreement

- I will ask permission before entering any web site, unless my teacher has already approved that site.

- On a network, I will use only my own login and password, which I will keep secret. I will always logout when I have finished using the computer.

- I will not look at or delete other people's files.

- I will not bring disks or memory sticks into school without permission.

- I will only e-mail people I know, or my teacher has approved.

- The messages I send will be polite and sensible.

- When sending e-mail, I will not give my home address or phone number, or arrange to meet someone.

- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.

- I will not use Internet chat.

- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.

- I know that the school may check my computer files and may monitor the Internet sites I visit.

- I understand that if I deliberately break these rules, I could be stopped from using email or internet.

I agree to follow these rules for internet and email use.

Signed: _____

Name: _____

Date: _____

Responsible Internet and Email Use
Parent/Carer Agreement

- I have read and understood the internet and email use agreement signed by my child and will enforce these rules at home when my child uses his/her email account outside of school.

- I will not give my child's logon details or password to anyone else. I will ensure that my child logs out at the end of the session.

- I will not use my child's email account to send emails personally or on behalf of my child.

I have read and understood the above. I agree to abide by the above agreement.

Name: _____ (parent/guardian)

Signed: _____ Date: _____

Parent/carer consent for web publication of work and photographs.

I agree that, if selected, my children's work may be published on the:

School website yes/no (delete as appropriate)

I also agree that photographs that include my child may be published subject to the school rules that photographs will not clearly identify individuals and that full names will not be used.

School website yes/no (delete as appropriate)

Names of children:

Child 1 _____

Child 2 _____

Child 3 _____

Name: _____ (parent/guardian)

Signed: _____ Date: _____

Dear Parents

Responsible Internet Use

As part of your child's curriculum and the development of ICT skills, our school is providing supervised access to the Internet. We believe that the use of the Web and email is worthwhile and an essential tool for children as they grow up in the modern world. Please read the rules and agreements for responsible Internet and email use. Then sign and return the agreement. Also please read and if you agree sign the web publication consent for photographs and work.

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 access provider operates a filtering system that restricts access to inappropriate materials. This may not be the case at home and we enclose references to information on safe Internet access that may be of use.

Whilst every effort 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 under any circumstances for any damages arising from your child's use of the Internet facilities.

I enclose a copy of the rules for Responsible Internet Use that we operate at our school. We also have a number of leaflets from national bodies that explain issues further.

Should you wish to discuss any aspect of Internet use please telephone the office to arrange an appointment.

Yours sincerely

C Dewberry
Headteacher