Policy
Bradfield CE Primary School

E-Safety

Policy Statement

"In the context of inspection, e-safety may be described as the school's ability to protect and educate pupils and staff in their use of technology and to have the mechanisms in place to intervene and support any incident where appropriate."

Ofsted Inspection Briefing Document, 2013

Safeguarding is a serious matter; at Bradfield Primary School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety, is an area that is constantly evolving and as such this policy will be reviewed on an **annual basis or in response to an e-safety incident**, whichever is sooner.

The primary purpose of this policy is twofold:

- *To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met*.

- *To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the pupil or liability to the school.*

This policy is available for anybody to read on the Bradfield Primary School website. All members of staff will sign as read and understood this e-safety policy, the more specific Staff Social Media Policy (Separate Policy) and the Staff Acceptable Use Policy. All three will form part of the Staff Induction Pack, given to new members of staff on appointment.

Policy Governance (Roles & Responsibilities)

Governing Body
The governing body is accountable for ensuring that Bradfield Primary School has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

- Appoint one governor to have overall responsibility for the governance of e-safety at the school who will:

- Keep up to date with emerging risks and threats through technology use.
- Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.
- Chair an e-Safety sub-Committee

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff, the e-Safety Officer (or more than one), as indicated below.

The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. pupils, all staff, senior leadership team and governing body, parents.
- All e-safety incidents are dealt with promptly and appropriately.

E-Safety Officer

The designated responsibilities of the e-Safety Officer is devolved to*:* Hannah Dennis

The e-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher and governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose.
- Make him/herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

ICT Support

Are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Software updates are regularly monitored and devices updated as appropriate.
    - Any e-safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Headteacher.
    - Passwords are applied correctly to all users. Passwords for staff will be a minimum of 8 characters with uppercase and numbers.
    - The IT System Administrator password is changed on a regular basis.

Classroom Teachers and Associate Staff

Are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any e-safety incident is reported to the e-Safety Officer (and an e-Safety Incident report is made), or in his/her absence to the Headteacher. If you are unsure the matter is to be raised with the e-Safety Officer or the Headteacher to make a decision.
- The reporting flowchart contained within the E-safety Incident Log (Appendix 1) is fully understood.

All Pupils

- Any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.
- E-Safety is embedded into the curriculum - pupils will be given the appropriate advice and guidance by staff across the curriculum.
- All pupils will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have access to resources to acquire the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents evenings, school newsletters and the availability of free online training courses the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that pupils are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded

E-Safety Committee

This committee is chaired by the Governor designated responsible for E-Safety.

The committee includes; parents' representative, e-Safety Officer, and others as required. The E-Safety Committee will meet on a termly basis and is responsible

- For advising on changes to the e-safety policy.
- For establishing the effectiveness (or not) of e-safety training and awareness in the school.
- For recommending further initiatives for e-safety training and awareness at the school.

Network and Device Management

Bradfield Primary School uses a range of devices including PC's, laptops and tablets. In order to safeguard the pupil and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering

We use a web filter that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The e-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering
We use technology that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message. The system is also used to filter certain words and can be used for monitoring.

Passwords
All staff and pupils will be unable to access the network without a unique username and password. Staff and pupil passwords should be changed if there is a suspicion that it has been compromised. The e-safety officer will be responsible for ensuring that passwords are changed as and when required.

Anti-Virus
All capable devices will have anti-virus software. This software will be updated at least **weekly** for new virus definitions.

Safe Use

School Network & the Internet
Use of the school network, with access to the Internet, in school is a privilege, not a right.

Use will be granted to new staff upon signing of this E-safety Policy, staff Social Media Policy ***These policies apply to all staff and pupils whether access to the school network or internet is by cable or wireless (or personal mobile account whilst on school premises, including school trips either in the UK or abroad) and on any device, laptop or PC, either school owned or personal.***

Email
All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is expected to be used for professional work-based emails only. The use of personal email addresses for the purposes of contacting pupils is not permitted.

Photos and videos
All parents sign a photo release slip on entry to the school, as part of the Induction Pack they receive; non-return of the permission slip will not be assumed as acceptance.

Social Networking
Bradfield Primary School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. Any subject specific social media services, permitted for use within Bradfield Primary School, must have been appropriately risk assessed, managed and moderated in accordance with the Social Media Policies.

In addition, with reference to images that may be uploaded to such sites, the following is to be strictly adhered to:

- Permission slips (either as hard copy filed in the pupil record folder or as flagged on the pupil record on SIMS) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of pupils using first name and surname; first name only is to be used, if at all.

- All images, videos and other visual resources that are not originated by the school are not allowed unless the owner's permission has been granted. Permission to use copyrighted resources must be sought and received before they are used.

Notice and take down policy
Should it come to the schools attention that there is a resource which has been inadvertently uploaded, either to the school website or school authorized social networking sites, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Reporting E-safety Incidents
Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer, or in his/her absence the Headteacher. the e-Safety Officer will assist in taking the appropriate action to deal with the incident and to fill out an incident log (*see Appendix 1*). All staff should make themselves aware of the procedures and the responsible staff involved in this process.

Training and Curriculum
It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. This includes the regular distribution of e-safety information to staff, pupils and parents.

In addition, Bradfield Primary School will have an annual programme of online e-safety training for teaching/associate staff, to be incorporated within the CPD programme, with the Board of Governors included. This online e-safety training provides staff with a certificate which must be renewed by further training on an annual basis. This continuous rolling training programme means that staff will always be up to date with the latest issues on e-safety from new and evolving technologies.

The school should ensure that aspects of e-Safety for pupils is firmly embedded into the curriculum. Whenever ICT is used in the school, staff will ensure that pupils are made aware about the safe use of technology and risks as part of the pupil's learning. If asked, class teachers should be able to demonstrate where and how the awareness of risk is imparted to pupils in lessons.

As well as the programme of training, the school will establish further training or lessons as necessary in response to any incidents.

The e-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

IEB. Feb 2015
Reviewed Feb 2016

Appendix 1

E-Safety Log

Log Number:	**Reported By:**		**ACTION ROUTE**
	Signed:	**Date:**	***E-Safety Officer*** **Date:** **Initialed**
Incident Description: (Describe what happened, involving which children and/or staff, and what immediate action was taken)			***Action Taken***
Result of Review:		**Date:**	***Classteacher*** **Date:** **Initialed**
			Action Taken
Signature (Headteacher)		**Date:**	***NOTES:***
Signature (Governor)		**Date:**	***Return to E-Safety Officer to file…..***

Appendix 2

Staff Agreement for the Use of the ICT at Bradfield School

Staff Agreement Conditions

1. Bradfield School provides ICT facilities to all staff who have been registered with the e-safety officer by signing and returning their ICT Agreement. As a registered user you may use any these facilities in order to carry out your work, to store files in your own user area on the network, to send and receive emails and to access appropriate information on the Internet.
2. You cannot use any ICT facilities until you are registered and have signed the conditions for use agreement. These conditions are necessary for one or more of the following reasons:
    a. To ensure that all equipment, peripherals, curriculum or administration networks and internet access function properly and are thus available for the benefit of registered users at all times
    b. To ensure that information stored by staff and pupils is kept safe and available at all times
    c. To comply with the appropriate laws governing the use or misuse of ICT and internet facilities
    d. To ensure that the school and its staff can carry on with their day to day business effectively

3. You should be aware that by signing this agreement you give consent to the e-safety officer in the normal pursuit of their work, having access to your user area, your files, to your e-mails. If you break the conditions of the agreement you may be liable to sanctions, up to and including dismissal.

When using Bradfield Primary School ICT facilities you MAY:

4. Use the facilities for your schoolwork or for other appropriate work.
5. Send personal e-mails outside of lessons using only the email system provided with your login account. The sending of emails during lessons, other than class work related messages, is not allowed.
6. Access the Internet providing this does not prevent anyone else from carrying out their work and that such activity falls within the conditions for the use of the facilities.
7. Store only such files as are needed for your work

When using Bradfield Primary School ICT facilities you MAY NOT:

8. Send e-mails which could bring yourself or the school into disrepute or which could render yourself or the school liable to prosecution
9. Knowingly access, view or download any material capable of giving offence
10. Keep, or pass on, e-mails received which contain material capable of giving offence
11. Knowingly import programmes, download files or open attachments that cause viruses to be spread
12. Add to the programmes already available to you, either on the network or a stand-alone machine. This includes accessing or downloading games and other programs either from the internet or from other external storage devices (including flash drives or similar)
13. Leave yourself logged in. When away from your station, you must logout
14. Give your password to any other person or allow them to use your account.
15. Attempt to gain the password of or access the work area of another user
16. Take part in any other computer related activity which could give offence or bring yourself or the school into disrepute or render yourself or the school liable for

prosecution

17. Attempt to change the operation of any ICT facility by amending its configuration settings, except with the express permission of the e-safety officer or under instruction of those acting on his/her behalf
18. Attempt to circumvent any security systems in place or to be knowingly party to such attempts, either before or after the event.