Bathampton Primary School
Together on a learning adventure

E-Safety Policy

Updated May 2015

1. Introduction

Bathampton Primary School has been described as having a 'welcoming and delightfully happy environment in which pupils thrive and want to do their best.' We want all children to enjoy school, to be challenged to achieve their very best, and to consider their time at the school as their own 'learning adventure'. We are committed to giving all of our children every opportunity to achieve the highest of standards. We do this by taking account of pupils' varied life experiences and needs. We offer a broad and balanced curriculum and have high expectations for all children. The achievements, attitudes and well-being of all our children matter.

2. Aims and objectives

e-Safety is an essential part of our lives today and today's Computing curriculum. This policy sets out the ways in which the school will:

- educate all members of the school community on their rights and responsibilities with the use of technology
- build both an infrastructure and culture of e-Safety
- work to empower the school community to use the Internet as an essential tool for life-long learning

Thus, through teaching relevant aspects of e-Safety, pupils will be equipped with the necessary skills about how to use the Internet safely and will have increased knowledge about how to deal with potential online risks.

This policy is to be used alongside other School policies.

3. Schedule for Development, Monitoring and Review

The implementation of the e-Safety policy will be monitored by an e-Safety working group[1] and e-Safety Leader, who will report annually to the Governors.

The impact of the policy will be monitored by the e-Safety working group by looking at:

- Log of reported incidents
- Internet monitoring log
- Surveys or questionnaires of learners, staff, parents and carers
- Other documents and resources
- Future developments

The e-Safety policy will be reviewed at least every two years or more regularly in the light of significant new developments in the use of technologies, new threats to e-Safety or incidents that have taken place.

The E-safety Policy was discussed by Staff on: Wednesday 7th May 2014

The E-Safety policy approved by the Governors on: Thursday 22nd May

The next review date is May 2016

Signed:

4. Teaching and Learning

4.1 The Internet is an essential part of our lives today in education, business and social interaction. Bathampton Primary has a duty to provide students with quality Internet access as part of their learning experience.

4.2 A progressive planned e-Safety education programme takes place through discrete lessons and across the curriculum, for all children in all years and is regularly revisited.

- Key e-Safety messages are reinforced through assemblies, Safer Internet Week (February) and throughout all lessons
- Pupils are taught to keep themselves safe online and to be responsible in their use of different technologies
- The Internet is an essential part of the curriculum. Pupils are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material. Processes are in place for dealing with any unsuitable material that is found in internet searches[2]
- Pupils are taught to be critically aware of the content they access on-line and are guided to validate the accuracy and reliability of information
- If video-conferencing is used, children will be supervised by a member of staff
- Pupils are taught to respect copyright when using material found online and to acknowledge the source of information
- Pupils will agree and sign an age appropriate Acceptable Use Policy for their class [*also to be agreed in class rules*] at the beginning of each school year, which will be shared with parents and carers

5. Cyberbullying

Bathampton Primary does not tolerate any form of bullying, including cyberbullying. (Please also refer to the School's Anti-bullying policy.)
In the unfortunate case of a cyberbullying incident, the School will follow procedures in place to support the individual(s) concerned and identify main causes of the problems as well as others concerned.
All incidents of cyberbullying reported to the school will be recorded. Pupils, staff and parents and carers will be advised to keep a record of the bullying as evidence.

6. Managing Internet Access

6.1 Information system security

- School computer systems (including audits of the safety and security of the systems) will be regularly reviewed with the ICT Technician
- Virus protection will be updated regularly

- Security strategies will be discussed with the Local Authority and the ICT Technician

6.2 E-mail

Class e-mail

- Pupils may only use approved class e-mail accounts. The password for the class email will be kept by the class teacher
- Class emails will only be used in conjunction with class projects and will be overseen by the class teacher(s)/TA
- Pupils will be taught not to reveal personal details of themselves or others in e-mail communication
- Incoming e-mail to class email addresses will only be opened if the author is known
- Any offensive emails must be reported to a teacher/TA
- The School will not allow forwarding of chain letters

Staff e-mail

- Personal email addresses (e.g. yahoo, Hotmail, gmail) will not be given to any parents or children
- Any communication over email between staff and parents will be via the school email system i.e. using a bathnes.gov.uk email address (or via School office)
- Any offensive emails must be reported to the Headteacher/SMT

7 Data Protection

7.1 The SWGfL Data Protection Policy[3] provides full details of the requirements that need to be met in relation to the Data Protection Act 1998. The school will:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- use personal data only on secure password protected computers and other devices
- ensure that users are properly “logged-off” at the end of any session in which they are accessing personal data
- store or transfer data using encryption and secure password protected devices *(data via email without password encryption is not always deemed as secure)*
- make sure data is deleted from the device once it has been transferred or its use is complete

7.2 Published Content and the School Website

The contact details on the website will be the school address, e-mail and telephone number. Staff and pupils’ personal information will not be published on the website.

Class teachers will have overall responsibility for content published on their class pages.

7.3 Publishing Photographs, Images and Work

- Parents should be clearly informed of the school policy on image taking and publishing
- A general written permission note from parents or carers will be obtained so the school can use images in newsletters and online
- Staff are encouraged to take images to support educational aims. However, they must ensure they follow guidance in the acceptable use policy[4] concerning the sharing, distribution and publication of those images
- Photographs and video taken within school are used to support learning experiences across the curriculum, as well as to provide information about the school on the website
- When using digital images, pupils should be educated about the risks associated with the taking, use, sharing, publication and distribution of images (including on social networking sites)
- Images or videos that include pupils will be selected carefully and will not provide material that could be reused
- Photographs or video are not to be taken in school for any purpose by members of the public without permission from the Headteacher/Senior Management Team

8. Social networking

- Staff will carry out risk assessments of sites before use and check the site is age appropriate
- Class blogs will be password protected and will run from the school website with approval from the Senior Management Team. Class blogs will be overseen by the class teacher
- Pupils, parents and staff will be advised on the safe use of social network spaces
- The School will control the use of social media and social networking sites. Currently, the School does not allow use of social media and social networking sites in school unless educational and discourages their use out of school
- Pupils will be taught to not give out personal and location details on social media and social networking sites. They will be encouraged to use nick-names and avatars

9. Personal Publishing

- Pupils will be taught via age appropriate sites suitable for educational purposes
- All members of the School community will be advised not publish detailed private thoughts or opinions on social networking sites
- Parents and carers will be contacted by the School if there are any concerns regarding pupils' use (in and out of school) of social media, social networking and personal publishing sites, particularly concerning situations where pupils are using sites which are not age appropriate
- The personal use of email, social networking, social media and personal publishing sites will be discussed with staff as part of staff induction and relevant matters will be raised in Staff Meetings/ongoing staff training. Safe and professional behaviour is expected of all staff

10. Mobile phones

- Staff are advised to only use mobile phones during break, lunchtimes or during non-contact time
- Staff are advised not to use their personal mobile phones to contact pupils, parents and carers except in exceptional circumstance when the number should be preceded by 141 to protect privacy
- Pupils are asked to not bring mobile phones in to School but if parents request this for a specific purpose the phone would be kept in a locked drawer in the school office during the day

11 Assessing risks and reporting incidents

11.1 Risk assessments will be reviewed regularly to ensure that technological advances are incorporated into the School's e-Safety Policy. Risk assessments will include:

- looking at the educational benefit of the technology
- considering whether the technology has access to inappropriate 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. The School cannot accept liability for the material accessed, or any consequences resulting from internet use

11.2 Managing filtering

Content accessed through the School's internet system is managed and filtered by SWGfL. Any inappropriate content must be reported to the nominated e-Safety Leader or Headteacher. Procedures will be followed to report inappropriate content to SWGfL and reviews will be carried out on the security of the system.

11.3 Reporting Incidents

The School will ensure all incidents are reported and responded to as necessary, following guidlelines from SWGfL/Somerset Learning Platform[5].
Any complaints about Internet misuse will be dealt with by the Headteacher and e-Safety Leader.
Reported issues about safeguarding will be referred to the Headteacher, who will follow guidelines in accordance with the Child Protection Policy.

All members of the School community will be notified of the complaints procedure[6].

12 Authorising Internet Access

All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

Parents and children will be asked to sign and return a consent form for children to be allowed to use the Internet. Pupils must agree to comply with the Responsible Internet Use statement before being granted Internet access.

Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' form before being allowed to access the Internet on the school site.

13. Communicating the e-Safety Policy

13.1 Pupils

- All pupils will have relevant e-Safety aspects explained to them
- E-Safety guidelines will be clearly displayed by computers and children will be made aware of these
- E-Safety will be part of the curriculum to increase pupils' awareness of issues and how to deal with them
- Pupils will understand that internet use will be regularly monitored and reviewed

13.2 Staff

- All staff will be required to read (and sign) the e-Safety policy and its importance will be explained during Induction/Staff Meetings
- Staff will understand that Internet traffic can be monitored and traced back to the individual user. Professional conduct is essential

13.3. Parents

- Parents and carers will be made aware of e-Safety procedures and relevant changes and/or updates in parent induction meetings, newsletters and on the School website
- New parents, carers and pupils will be asked to sign the Safe Internet Use agreement (Children to sign from Y1)
- Parents will be invited to attend a meeting on e-Safety held in School or with other cluster schools

References (& Resources/Links)

Somerset Learning Platform
http://bit.ly/elimsomersetpolicies

South West Grid for Learning
http://www.swgfl.org.uk/Staying-Safe

Childnet
http://www.childnet.com/

Kidsmart
http://www.kidsmart.org.uk/