LSCB
Bath & North East Somerset
Local Safeguarding Children Board

Batheaston Primary School

Online Safety Policy

Part of the Safeguarding Strategy

(See also policies on Child Protection, Behaviour Policy, Anti-Bullying, Internet Policy, Acceptable Use, Mobile Devices, Data Protection /Security Policy, Computing and Complaints)

1. Aims and objectives

New technologies have become integral to all our lives in today's society – and not least to children and young people. Children will need to develop high-level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment.

The internet and associated technologies are powerful tools for learning. They have the potential to access information at high speed and to empower children to take an increased level of ownership over their learning. The use of the internet and associated technologies in school are tools that provide our children with exciting opportunities to pursue 'personalised learning'. The purpose of this policy is to ensure Online Safety risks are minimised, not only for children and young people, but for their parents and the other members of the school community through 3 key areas: Policies and practice; Education and training; and infrastructure & technology. This will allow all members of the school community to make the most of the internet's potential (and its associated technologies) for learning and everyday living.

Aims

- To build both an infrastructure and culture of Online Safety.
- To ensure safe access to on-line material for all users.
- To provide guidelines for internet use that is planned, task-orientated and educational within a regulated and managed environment – that accords with our school's ethos. (This includes use by adults and children.)
- To establish Acceptable Use Agreements for all members of the School Community, covering the conditions of responsible internet and technology use for all users.
- To create guidelines that will lead to a safer online for children and will include filtering appropriate to the age of the children.

- To ensure that children will be taught what is acceptable and what is not acceptable and given clear objectives for responsible Internet use - including: an ability to evaluate the quality, accuracy and relevance of information on the internet; Plagiarism and copyright infringement; illegal downloading of music or video files.
- To ensure that children and teachers are aware of 'cyber-bullying', how to prevent it happening how to stop it if it occurs, and including how to report.
- To ensure that staff are aware of the need for them to understand how the internet is being used by pupils at the school (or by young people in general)
- To provide information to parents to enable them to both support and proactively contribute to the school's Online Safety framework (including the potential for excessive use which may impact on the social and emotional development and learning of their children)

2. Schedule for Development, Monitoring and Review

- The implementation of the Online Safety policy will be monitored by the Online Safety Leader.
- The impact of the policy will be monitored by the Online Safety leader by looking at:
  Log of reported incidents
  Internet monitoring with support from Eye-Tech (tech support)
  Surveys or questionnaires of learners, staff, parents and carers
  Scheme of work – IT Switched On
  Future developments i.e. staff Sharepoint
- The Online policy will be reviewed annually or more regularly in the light of significant new developments in the use of technologies, new threats to Online Safety or incidents that have taken place. As children's use of mobile devices grows rapidly there needs to be some recognition that the monitoring of the school network is only part of the solution as many children and young people will be using mobile devices on 3 and 4G and so will not need to use the school network.

3. Teaching and learning

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

3.2 A progressive planned Online Safety education programme takes place through discrete lessons, the PSHE scheme and other curriculum subjects (where appropriate), for all children and young people in all years and is regularly revisited.

- Key Online Safety messages are reinforced through assemblies, Safer Internet Week (February) and throughout all lessons where appropriate
- Pupils are taught to keep themselves safe online and to be responsible in their use of different technologies.

- Teachers should be aware of the term 'Sexting' and its impact.
  'Sexting' is when someone shares sexual, naked or semi-naked images or videos of themselves or others, or sends sexually explicit messages. They can be sent using mobiles, tablets, smartphones, laptops - any device that allows you to share media and messages.
- Teachers and pupils are made aware of the term 'Cyber-bullying' and its impact.
  'The use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature.'
- The Internet is an essential part of the curriculum. Where appropriate, and particularly with younger children, 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
- 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.
- The positive use of technology, rather than the negative, should be emphasised in order to promote self-esteem, assertiveness and encourage a learning environment
- Children will be taught the importance of not sharing personal information and photographs over the internet. As children get older it is particularly important that children are made aware of what is safe to share and how as older children cannot do certain things online without sharing some personal 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 agreement for using the internet responsibly [*also to be agreed in class rules*] at the beginning of each school year, which will be shared with parents and carers

4. Online Bullying (Cyberbullying)

Batheaston Primary School does not tolerate any form of bullying, including online bullying. (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 documented, recorded and investigated. Pupils, staff and parents and carers will be advised to keep a record of the bullying as evidence.
Staff should adhere to the following guidelines for helping the online bullying victim. (Please also refer to anti – bullying policy and the recent national guidance www.childnet.com/cyberbullying-guidance)

1. Reassure that they have done the right thing.
2. Acknowledge that it is difficult to tell but do not promise confidentiality.
3. Reiterate that no one has the right to do that to others
4. Ensure school has a culture which does not tolerate bullying.

5. Advise the victim not to retaliate or return the message but keep evidence (e.g. time and date, content of message preferably on the device itself) and take it to designated child protection staff and /or head teacher.
6. Write down everything that has been disclosed as soon as possible.
7. Report the incident to the Online Safety Teacher who will then record it in the Online Safety incident log
8. This policy applies to both children and adults in the school community.

5. Managing Internet Access

5.1 Information system security

School computer systems (including audits of the safety and security of the systems) will be regularly reviewed with the ICT Technician (Eye-Tech)
Virus protection will be updated regularly
Security strategies will be discussed with the Local Authority and the ICT Technician.
See Guide for Appropriate Filtering and Monitoring (Sept 2016)

5.2 The safe use of the computer network

- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Online Safety leader.
- Older children (generally accepted by Ofsted as KS2) should have individual passwords for platforms such as Doodle Maths.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- Pupils will be taught how to log on and off correctly.
- The school ICT systems will be reviewed regularly with regard to security.
- The school will use SOPHOS Anti-Virus Protection. Updates will be administered by the school ICT technician. (Eye-Tech)
- Files held on the school's network will be regularly checked by the ICT Subject Leader and by class teachers. Where inappropriate material, or an excess of material, is found to be stored in an individual user file the necessary action will be taken to rectify the problem. This might lead to school disciplinary action

5.3 The safe use of websites and the internet

- The school uses a web based filtering system provided by RM SafetyNet through the South West Grid for Learning (SWGfL). This system provides three tiers of filtering safety.

RM SafetyNet provide a filter service for all schools as part of the SWGfL. This is updated constantly using information from Local Education Authorities, web-based watch dogs and from research carried out by RM themselves

This service is refined by the Local Authority (LA), who receive information from schools regarding inappropriate sites that have slipped through the filter

- Schools have a local facility to block specific sites or keywords from searches. This ensures maximum and immediate high level filter protection.
- This provision is in addition to standard filtering software installed on each PC as standard which will also be set at maximum.
- Children do not have unauthorised access to the internet. Younger children will be supervised by a member of staff when accessing on-line material.
- All users of the internet will follow the agreed guidelines for safe and acceptable use (see Acceptable Use Agreement (pupils) – Appendix 1 and Acceptable Use Agreement (staff and adults in school) – Appendix 2. Any user found to be in violation of these guidelines will be subject to school discipline procedures. Repeated violations would cause that user to be banned from using the internet in school and in the case of adults, banned from working with children.
- Parents and children will be asked to sign and return a consent form before their child is permitted to use the internet or e-mail in school. Please see the Acceptable Use Agreement
- Staff and Adults in school will be asked to sign and return the Acceptable Use / ICT Agreement form. The school will keep a record of all staff and children who are granted Internet access. The record will be kept up-to-date, for instance a member of staff leaving or the withdrawal of a pupil's access
- Children will be guided to suitable web sites – pre-checked as suitable for their use. Often blocks are put in place by the school on sites deemed not suitable
- If staff or children discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Subject Leader.
- Should inappropriate material be found, staff and children should take the following action:
  1. Click on 'Hector the Protector'. DO NOT switch off the computer.
  2. Children should notify an adult immediately. This would usually be the child's class teacher.
  3. The adult should report the incident to the ICT Subject Leader immediately who will record the URL (address) of the web-site and any keywords that might have been used in the search. Both will be added to the school banned list. If s/he is unavailable the adult should refer the matter to the Headteacher AND record all details in the ICT Log Book
  4. In the rare event that an incident should occur, the child's parent(s)/Guardian(s) will be informed.
  5. The incident will be recorded in the Online Safety incident log kept by the Online Safety teacher.

- Rules for responsible Internet access will be posted near all computer systems and children helped to understand them. [Appendix 3]
- Children will be informed that Internet use will be monitored.
- Instruction in responsible and safe use will precede Internet access. Resources could include Hector and friends/Thinkuknow (from Childnet) for younger children. A planned Online Safety programme will be provided as

part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. In addition key Online Safety messages will be reinforced as part of a planned programme of assemblies

- Children will be taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information. They will also be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

6. E-mail

a) Class e-mail

Pupils may only use approved class e-mail accounts (Office 365). 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

b) Staff e-mails

- 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 (Parentpay/Office 365 or via School office)
- All communication between adults and children will take place within clear and explicit professional boundaries – and, where age appropriate, with the prior consent of parents/carers. Adults will not share any personal information with a child and they should not request or respond to any personal information form the child other than that which might be appropriate as part of their professional role. Adults MUST ensure that all communications are transparent and open to scrutiny.
- Any offensive emails must be reported to the Headteacher/SMT
- Staff should not contact pupils via personal email
- Staff must use children's initials in emails and use encrypted memory sticks when transferring data

N.B. Any user found to be using e-mail for sending inappropriate messages will be subject to school discipline procedures. Repeated violation of these guidelines by any one user will cause them to be banned from using e-mail in school

7. Data Protection

7.1

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive

- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The South West Grid for Learning (SWGfL) Data Protection Policy 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)*
- laptops and USBs should be encrypted if photos or personal data for pupils is being taken off-site
- 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 using school devices and not their personal ones. However, they must ensure they follow guidance in the Internet policy 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.
- Schools could encourage parents/carers to consider the following ideas before they share photos or videos online *[from the Information Commissioners Office]:*
    - Some children and adults are at risk and MUST NOT have their image put online. Not all members of the school community will know who they are – so ALWAYS ask permission before sharing photos or videos online
    - Once posted and shared online any image or video can be copied and will stay online forever
    - Some people do not want their images online for personal or religious reasons
    - Some children, families and staff may have a complex family background which means that sharing their image online can have unforeseen consequences
    - In order to keep all members of the school community safe we must all 'Think Before We Post' photos and videos online

8. Social networking

- Where possible/age appropriate, staff will check the content of websites before using the internet to support learning
- 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
- Staff are advised to use strong privacy settings if using social media
- 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
- Pupils will be taught about the positive impact social media can have but remind children of age appropriateness i.e. age 13 for Facebook and Instagram.

9. Personal Publishing

- Pupils will be taught via age appropriate sites suitable for educational purposes
- 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 and volunteers are expected model 'acceptable use' to the children and to only use mobile phones during break, lunchtimes or during non-contact time and not use them while they are with children / discharging their professional duties.
- Staff should 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 encouraged to not bring mobile phones in to School but if parents request this for a specific purpose the phone must be handed in to the School Office/ children will not use one during the school day or on any part of the school site. Any phones should be kept in bags and turned off.

11. Assessing risks and reporting incidents

11.1 Staff will ensure that technology is being used appropriately to support learning and where possible will consider 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.
Any user found to be in violation of these guidelines will be subject to school discipline procedures. Repeated violations would cause that user to be banned from using the internet in school and in the case of adults, banned from working with children.

11.2 Managing filtering

- Content accessed through the School's internet system is managed and filtered by SWGfL. Guidance is available from Childnet: http://www.childnet.com/blog/appropriate-filtering-and-monitoring-required-in-schools-from-5th-september
- Any inappropriate content must be reported to the nominated Online 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 guidelines from SWGfL/Somerset Learning Platform.
- Any complaints about Internet misuse will be dealt with by the Headteacher and Online 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.

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.

13. Communicating the Online Safety Policy Pupils:

- Pupils will be taught Online Safety through PSHE and in other subjects where appropriate including the ICT curriculum and staff will reinforce Online Safety messages in the use of ICT across the curriculum to increase pupils' awareness of issues and how to deal with them.
- Online Safety guidelines will be clearly displayed by computers and children and young people will be made aware of these
- Pupils will understand that internet use will be regularly monitored and reviewed
- Children will be expected to sign the Acceptable Use Policy.

Parents:

- Parents will be invited to attend a meeting on Online Safety held in School or with other cluster schools. These will reinforce the key Online Safety messages from this policy and provide parents with information to support all children (and the wider school community) in staying safe as they use the internet and associated technologies. Materials provided will include reference to the SWGfL's "Golden Rules" for parents.
- Parents will be asked to discuss and sign Acceptable Use Policy on entry into school and then again annually.
- As part of the Online Safety curriculum, children will also receive any relevant information available to share with their family.
- Where specific advice is received from time to time through external sources such as 'Thinkuknow', it will be passed on to parents through school induction events/newsletters / emails/ website.

Staff:

- It is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Staff will understand that Internet traffic can be monitored and traced back to the individual user. Professional conduct is essential. KCSIE makes clear that staff training on online safety needs to be integrated and planned into the overall safeguarding approach. Initial signing and review of the Staff Acceptable Use Policy during Induction Safeguarding Interview
- Regular reviews of the Internet Safety Policy
- Discussion with ICT Leader on delivering the Online Safety curriculum
- Staff Development Interviews and the annual ICT skills audit

- The Online Safety Officer will stay updated with latest information through CP Forum and Thinkuknow / SWGfL contacts
- The Online Safety Officer will provide additional advice / guidance / training as required

Governors:

- Governors will be given the opportunity to take part in Online Safety training / awareness sessions – particular the Governors with responsibility for ICT and Child Protection – through:
- Attendance at training provided by the Local Authority / National Governors Association / SWGfL or other relevant organisation
- Participation in school training / information sessions for staff or parents
- Regular reviews of the Internet Safety Policy
- Signing their Acceptable Use Agreement (See UKCCIS guidance Appendix 2)

This policy was agreed by staff on:

This policy was adopted by the Governing Body at its meeting held on:

Signature of Chairperson of Governing Body:

Next Review Date: Annually (or earlier due to change in statutory guidance/internal review)

Appendix 1: Staff Self-Check List:

Internet
I have checked against the internet permission returns and know who is and who is not allowed to use the internet.

My children know that should they find a web page that upsets them they are to turn off the monitor and see me immediately.

I know the procedure for reporting bad internet sites.

I have checked that no one can use the internet without supervision, particularly at wet plays or lunch times.

I will only use the Internet, ICT equipment or other technologies according to school policy and within clear and explicit professional boundaries. The consequences of any breach of trust could lead to me being banned from working with children and possible legal proceedings

E-mail
I check children's school e-mail accounts as appropriate to ensure that they are used in a safe, purposeful and appropriate manner.

I am aware of the user restrictions that will be applied to the user accounts held by the children in my class.

I will only communicate with children following prior consent of their parents / carers, in accordance with school policy and within clear and explicit professional boundaries

I will only use school email accounts for school communications

Other Technologies
I have saved digital photographs into a class picture folder.
I have not identified individuals when uploading school web site.
I will only record images with due regard to the law and the need to safeguard the privacy, dignity, safety and wellbeing of children. I have obtained prior informed written consent from parents or carers and agreement where possible from the child
I will avoid images in one to one situations or which show a single child with no surrounding context

I know it is NOT appropriate for any adult to take photographs of children for their personal use. I will report any concerns I have about inappropriate or intrusive photographs I find
I will not use mobile phones or personal devices to take images of children
I will model the acceptable use of mobile phones and other technologies
I will not take images in 'secret' or in any situation which may be construed as 'secretive'
I have read and understood the Internet and ICT Safety Policy
I have signed, returned and taken note of the Acceptable Use (Internet / Associated Technologies) Agreement (Staff & Adults)

References (& Resources/Links)

LSCB E Safety Strategy
http://www.bathnes.gov.uk/sites/default/files/sitedocuments/Children-and-Young-People/ChildProtection/e-safety strategy_june_2016.pdf

UK Council for Child Internet Safety (UKCCIS)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/562876/Guidance_for_School_Governors_-_Question_list.pdf

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

South West Grid for Learning
http://www.swgfl.org.uk/Staying-Safe
SWGFL Policy template
http://swgfl.org.uk/products-services/esafety/resources/online-safety-policy-templates

Online Safety FAQs
http://swgfl.org.uk/FAQs/Online-Safety-FAQs

360 Degree Safe
https://360safe.org.uk/

360 Degree Safe self-review tool (free)
https://360safe.org.uk/About-the-Tool

Childnet; including Cyberbullying and Filtering guidance
http://www.childnet.com/

www.childnet.com/cyberbullying-guidance

http://www.childnet.com/blog/appropriate-filtering-and-monitoring-required-in-schools-from-5th-september

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

Digital Parenting Magazine
http://www.theparentzone.co.uk/vodafone_digital_parenting_magazine/2248_0

Internet Matters (for parents)
www.internetmatters.org

NSPCC – Net Aware
http://www.net-aware.org.uk

www.thinkuknow.co.uk

www.saferinternet.org.uk/about/helpline

Appendix 3: Useful Documents:

UKCCIS Guidance for Schools

Guidance_for_School
Governors-_Questi

Key Documents For Schools from Karl Hopwood http://www.esafetyltd.co.uk/
(Accurate as of December 2016)

Key documents for
schools.pdf