

THE FEDERATION OF BURLEY AND SOPLEY PRIMARY SCHOOLS



Online Safety Policy

Date of issue	Sept '22	Date to be revised	Sept '23
----------------------	----------	---------------------------	----------

Names of relevant post holders

Post	Holder	Post	Holder
Headteacher	Nanette Allies	Chair of Governors	Ian Satchwell
SENDCo/Inclusion Lead	Claire Bleakley		

Revision Log (last 5 changes)

Date	Version No	Brief details of change
01/05/2021	1.0	Policy created.
01/05/2022	2.0	No changes.
01/09/2022	3.0	<ul style="list-style-type: none"> Added current personnel names, bullet points now numbered and a few minor grammatical changes. P2. End-to-end online safety: added points 4,5 and 6 about training for staff and governors re: online safety. P4. Managing: point 6 a caution about 'overblocking'.

Introduction

Online safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's online safety policy should operate in conjunction with other policies including those for pupil behaviour, anti-bullying, curriculum, data protection and security.

End-to-end online safety

Online safety depends on effective practice at a number of levels:

1. Responsible IT use by all staff and pupils; encouraged by education and made explicit through published policies.
2. Sound implementation of online safety policy in both administration and curriculum, including secure school network design and use.
3. Safe and secure broadband including the effective management of filtering systems
4. Staff should understand that pupils could be at risk of harm online. All staff should be aware that children are at risk of abuse and other risks online and that children can abuse other children online. All staff will receive training and regular updates about online safeguarding.
5. Governors should get appropriate training about safeguarding and child protection, including online safeguarding.
6. The federation headteacher should ensure that children are taught how to keep safe while online.

Writing and reviewing the online safety policy

The online safety policy is part of the school safeguarding practices.

1. The IT Coordinator works in close co-operation with the federation headteacher, who is the Designated Safeguarding Lead (DSL), and Deputy DSLs.
2. Our online safety policy has been written by the school. It has been agreed by the staff and governors.
3. The online safety policy will be reviewed annually

Teaching and Learning

Why internet use is important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

1. The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
2. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
3. Internet access will be planned to enrich and extend learning activities.
4. Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate internet content

1. If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the school IT Coordinator.
2. Staff should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
3. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

1. The security of the school information systems will be reviewed regularly.
2. Virus protection will be installed and updated regularly.
3. The school uses broadband with its firewall and filters.

E-mail

1. Pupils may only use approved email accounts on the school system. Children are not allowed access to personal email accounts or chat rooms whilst in school.
2. Pupils must immediately tell a teacher if they receive an offensive email.
3. Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
4. E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
5. The forwarding of chain letters is not permitted.

Published content and the school website

1. The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
2. The federation headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

1. Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
2. Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
3. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
4. Pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

1. Social networking sites and newsgroups will be blocked unless a specific use is approved.
2. Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs, etc.
3. Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.

Managing Filtering

1. The school will work in partnership with the service provider to ensure filtering systems are as effective as possible.
2. If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school Online safety coordinator.
3. Senior staff will ensure that checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
4. The IT coordinator will be careful to ensure that "over blocking" does not lead to unreasonable restrictions on what children can be taught with regard to online teaching and safeguarding (KCSiE 2022).

Managing video-conferencing

1. IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
2. External IP addresses should not be made available to other sites.
3. Pupils should ask permission from the supervising teacher before making or answering a video-conference call.
4. Video-conferencing should be supervised appropriately for the pupils' age.

Managing emerging technologies

1. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
2. Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
3. Staff have access to a school phone where contact with pupils is required.

Protecting personal data

1. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998

Assessing risks

1. In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school **cannot** accept liability for the material accessed, or any consequences of Internet access.
2. The federation headteacher will ensure that the online safety policy is implemented and compliance with the policy is monitored.

Policy Decisions

Authorising Internet access

1. All staff, including teaching assistants and supply teachers must adhere to the school's IT acceptable use policy (AUP) before using any school IT resource.
2. Children's access to the Internet will be by adult demonstration or through supervised access to specific, approved on-line materials.

Handling online safety complaints

1. Complaints of Internet misuse will be dealt with by a senior member of staff.
2. Any complaint about staff misuse must be referred to the federation headteacher.
3. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
4. Pupils and parents will be informed of the complaints procedure.
5. Sanctions within the school discipline policy include: interview/counselling by class teacher / headteacher; informing parents or carers; and removal of Internet or computer access for a period.

Community use of the Internet

1. The school will be sensitive to Internet related issues experienced by pupils out of school, e.g., social networking sites, and offer appropriate advice.
2. Parents using school IT equipment must adhere to the school's IT AUP.

Communications Policy

Introducing the online safety policy to pupils

1. Pupils will be informed that Internet use will be monitored.
2. Advice on online safety will be introduced at an age-appropriate level to raise the awareness and importance of safe and responsible internet use.

Staff and the online safety policy

1. All staff will be given the school online safety policy and its importance explained.
2. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.

Enlisting parents' / carers' support

1. A copy of this policy will be made available on the school website or in hard copy via the school office upon request.

Appendix 1: Internet Use

Possible Teaching and Learning Activities	Key Online safety issues	Relevant Websites
Using search engines to access information from a range of websites.	Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Ask Jeeves for kids Yahooligans CBBC Search Kidsclick Picsearch safesearch NOT Google images
Exchanging information with other pupils and asking questions of experts via email.	Pupils should only use approved email accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.	GridClub School Net Global Kids Safe Mail E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	School website Learn Premium Espresso
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	School website
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	GridClub
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	City Learning Centres
Creating web directories to provide easy access to suitable websites: <ul style="list-style-type: none"> - Pupils should be supervised. - Pupils should be directed to specific, approved on-line materials. 		

Internet Rules and Permission: Please see related document – ‘**The Federation of Burley and Sopley Primary Schools online safety and acceptable use of IT by pupils**’ (to be signed by parents and pupils)