



Beaufort Primary School

Online Safety Policy



The school's Online Safety coordinator is Natasha Haycraft.

This policy should be read in conjunction with the following policies:

- Computing and ICT Policy
- Acceptable Use Agreement
- Staff Code of Conduct Policy
- Social Media Policy
- Anti-bullying Policy
- Safeguarding Policy
- Mobile Phone Policy
- Data Protection Policy
- School Photographic and Film Consent Form
- Home/School Agreement
- Blended Learning Policy (within the Contingency Plan 2021)

Introduction

At Beaufort Primary School we recognise that Internet and digital communications are important and that internet use can enhance learning for our children. The Internet is an essential element in 21st century life for education, business and social interaction. We have a duty to provide students with quality Internet access as part of their learning experience. In addition, Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Providing Internet Education

- Pupils will be educated 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 and to be critically aware of the materials they read.
- Pupils will be shown how to validate information before accepting its accuracy.
- Pupils will be shown how to publish and present information appropriately to a wider audience.

Keeping Staff and Pupils Safe

- The school internet access is provided by EXA contract and includes Surf Protect filtering (cloud based) appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be taught how to report inappropriate Internet content.

Responsible Use

- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Texting and email system to parents is protected by secure log in and has restricted staff use.

Managing Internet Access

- School ICT systems security will be reviewed regularly, using both the Bitdefender administration console and SECURUS, which monitors all activity on the school network.
- Virus protection, Malware and Phishing protection are all set to automatically update as updates are released.
- Filtering is customised for both staff and pupils.
- The school email system (Outlook Web App, OWA) is encrypted and scans each email on receipt.
- Securus monitors and reports potential inappropriate use on the network.
- Incoming email should be treated as suspicious and attachments not opened unless the author is known.

Published content and the school website

- The contact details on the website should be the school address, school email and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. Where practical, the school will look to use group photographs rather than photos of individual children.
- Pupils' full names will be avoided on the website, as appropriate, including in year group blogs, forums, pupils' work and videos particularly in association with photographs.
- Permission is sought on an annual basis from parents or carers for photographs of pupils to be published on the school website, school blog or any other publication.
- Pupils must not reveal personal details of themselves or others in any online communication, or arrange to meet anyone without specific permission.

Personal publishing on the school learning platform

- The school will educate pupils, through the online safety curriculum, on the safe use of social network sites, password safety and digital footprints.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised against pupil use of social network spaces outside school as they bring a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Staff may only use approved email accounts on the school system.
- There is a page on the website that advises parents on keeping children safe online.

Managing filtering

- The school will work in partnership with EXA and the Swan Trust schools to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable online materials, the site must be reported to the Online Safety Coordinator.
- Senior staff will regularly check that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- A group policy is set so only the Admin User can install new software.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and in accordance with General Data Protection Regulations 2018.

Policy Decisions

Authorising Internet access

- All network users must read and sign the 'Staff Code of Conduct' and sign an Acceptable Use Agreement before using any school ICT resource.
- The school will maintain a current record of all users who are granted access to school ICT systems.
- Parents will be asked to sign and return an Acceptable Use Agreement.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials and any searches will be made using Swiggle, a child-friendly search engine.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked 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.
- The school will audit ICT using '360°Safe' to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective.

Handling online safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school Online Safety Policy.

Policy Communications

Introducing the Online Safety Policy to pupils

- Pupils selected as digital leaders are members of the online safety committee.
- Appropriate elements of the Online Safety Policy will be shared with pupils.
- Online safety rules will be posted in all networked rooms.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of online safety issues and how best to deal with them will be provided for pupils through Internet Safety lessons.

Staff and the Online Safety Policy

- All staff will be given the School Online Safety Policy during their induction and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

- Parents and carers will be given online safety information when their child receives log-in details for Online Learning links (Mathletics, PurpleMash and Seesaw).
- Parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school web site.
- An icon linking to an anonymous reporting system (SWGfL *Whisper* report) can be accessed from the school website Home page, to report any online safety concerns.
- Parents and carers will regularly be provided with additional information on online safety.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

Date written: February 2014

Reviewed and agreed by LGC in Autumn 2023

Date for next Review: Autumn 2024