Brookhurst Primary School

Online Safety Policy

Autumn Term 2023

Author : Miss S Beamish

Approved : Miss A Stanton

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.

This policy should be read in conjunction with other policies including those for Pupil Behaviour, Bullying, Curricular Data Protection and Security and Child Protection.

Writing and reviewing the online safety policy

The Online Safety Policy is part of the School Development Plan and relates to other policies including those for Computing, Child protection and GDPR.

- The school will appoint an online safety Coordinator. At the time of writing, this is the Computing Subject Leader.
- Our online safety Policy has been written by the school, building on the Warwickshire ICT Development Service online safety Policy and government guidance. It has been agreed by the senior management and approved by governors.
- The Online Safety Policy will be reviewed every 2 years.

Teaching and learning

Why internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. Brookhurst recognises that it has a duty to provide children and young people with quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool in teaching and learning for staff and pupils.

Internet use will enhance learning

- The schools internet access is available to enhance the teaching and learning in school. It is designed expressly for pupil use and includes excellent filtering 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.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity. Staff will also educate them in the effective use of the internet for research, including the skills of knowledge location, retrieval and evaluation. **It is important that pupils learn not to copy information from the internet (plagarise) but use it to inform their writing.**

Pupils will be taught how to evaluate internet content

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to: ICT Services, and (where appropriate) the school e-safety officer.
- The school will ensure that the use of internet derived materials by staff and by pupils complies with copyright law.
- 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

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses the Warwickshire Broadband with its firewall and filters.
- The school provides an addition level of protection through its deployment of Policy Central in partnership with ICT Services.

E-mail

- Pupils may only use approved e-mail accounts on the school system. Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Use of words included in the Policy Central 'banned' list will be detected and logged.
- 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.
- The forwarding of chain letters is not permitted.1.3.3 Published content and the school web site
- The contact details on the school website or the learning portal will be the school address, e-mail 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 staff and pupil's images and work

- Photographs that include pupils will be selected carefully and parent's permissions asked before using for educational purposes.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/newspaper.
- Pupil's work can only be published with the permission of the pupil and parents. Images of staff will not be published without consent.
-

Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Pupils will be taught 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, name of school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.

<u>In accordance with the new KCSIE 23 Key Changes</u>

<u>Cyber security</u>

- Using an outside agency, SaVVit, we check Guidance on e-security, as seen on the National Education Network and trying to meet the Cyber security standards for schools and colleges.GOV.UK.
- All staff have been given training on cyber security (Sept 2023)

<u>Online safety and filtering and monitoring</u>

- All Governing bodies and proprietors and staff have undergone safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring). All staff have been spoken to about filtering and monitoring and the expectations of what this means.

- Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors are doing all that they reasonably can to limit children's exposure to risks from the school's or college's IT system. As part of this process, governing bodies and proprietors are ensuring their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. We are using outside agencies to help use assess our filtering and monitoring.

Managing filtering and monitoring

- The school will work in partnership with the ICT Services and Becta to ensure filtering systems are as effective as possible. The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty.

- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to ICT Services and (where appropriate) the school E-Safety coordinator.
- The DSL and online safety coordinator, with support from senior staff will ensure that regular checks are made to ensurethat the filtering methods selected are appropriate, effective and reasonable. (***Note: There is a danger in 'testing' the system to try to access inappropriate materials as when it is picked up by policy central it will be***

traced back and the perpetrator will then have to prove their innocence! It is advisable that ITservices at Warwickshire County Council are notified before these checks are due to commence.

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.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with pupils is required.

Protecting personal data

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

Policy Decisions

Authorising Internet access

- All internet use in school by pupils will be supervised.
    - All visitors from other schools can use a separate internet connection called BYOND
- Internet access is only given by; Office, Headteacher, Deputy and Computing coordinator
- The school will maintain a current record of all staff and pupils who are granted internet access. All users must read and abide by the age appropriate acceptable users policy on an annual basis.
  At EYFS and Key Stage 1, access to the internet will be by adult demonstration (where necessary) with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form to show they have read, discussed and accepted the Acceptable Users Policy on behalf of their child/ren.

Assessing risks

- 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. Neither the school nor WCC can accept liability for the material accessed, or any consequences of internet access.
- The head teacher will ensure that the Online Safety Policy is implemented and compliance with the policy monitored.

Handling online safety complaints

- Complaints of Internet misuse by pupils will be dealt with by a senior member of staff. In the first instance this will be the Computing Subject Leader. The head teacher will be informed about all incidents. A log of such incidents will be maintained.
- Any complaint about staff misuse must be referred to the head teacher who should use the agreed WCC procedures.
- Complaints of a child protection nature will be dealt with in accordance with agreed child protection procedures.
- Pupils and parents will be informed of the complaints procedure. Sanctions
- within the school discipline policy include:
    - informing parents or carers;
    - removal of internet or computer access for a certain time period.

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to online safety as and when the need arises.
- The school will be sensitive to internet related issues experienced by pupils out of school, e.g. social

networking sites, and offer appropriate advice.

Communications Policy Introducing the

online safety policy to pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Online Safety will be taught by all teaching staff to support the understanding of online safety to all pupils.
- An online safety training programme will be provided to raise the awareness and importance of safe and responsible internet use by all staff in school.

Staff and the Online Safety policy

- All staff will be given the School Online Safety Policy 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.

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school website.
- Sources of further guidance for parents to help them to provide guidance for their children in the safe use of computing technologies are signposted on the school website and via the learning portal.

Safeguarding pupils in online learning and communication between staff and pupils

Where school staff are delivering lessons online or virtually (e.g. to children unable to attend school due to COVID-19 or ill health), all such lessons will be delivered in accordance with the school's safeguarding and child protection, staff behaviour (code of conduct) and acceptable use of ICT policies. This will ensure that the school's filtering and monitoring software is enabled.

The school will take account of guidance from DfE in relation to the planning and delivery of online learning when it is issued; as well as nationally recognised guidance including *guidance from the UK Safer Internet Centre on safe remote learning and London Grid for Learning on the use of videos and livestreaming.*

Staff will always use school/service owned devices and accounts for the delivery of online/virtual lessons/tutorials. School leaders have the right to randomly join live lessons in order to safeguard pupils/students and staff and to ensure that policies are being followed.

When delivering online/virtual lessons on a one-to-one basis or communicating with vulnerable children who are not attending school via video chat, staff will have emailed a timetable to parents so that they know when the child should be online for lessons and gained prior permission to have these one-to-one sessions.

The school will request and obtain written consent from parents/carers before staff communicate with children online.

It is important that all staff who interact with children online continue to look out for signs that a child may be at risk, distressed for some reason or vulnerable in some other way; and report and record any concerns to the DSL in the normal way. The DSL will respond to any such concern as they would any other safeguarding concern.

The school will ensure that online learning tools and systems are used in line with privacy and data protection/GDPR requirements.

Online/virtual lessons should be timetabled and the headteacher or DSL will be able to drop into any virtual lesson at any time – the online version of entering a classroom for pupil/student welfare and safeguarding purposes. Staff delivering online/virtual teaching will be expected to display the same standards of dress and conduct that they would when working face to face in school, modelling appropriate behaviour and presentation to pupils/students and parents.

Below are other issues that staff need to take into account when delivering online/virtual lessons or communicating with children online, particularly where webcams are used:

- Staff and children must be fully dressed and wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example not in bedrooms; and the background should be blurred. If it is not possible to blur the background, staff must consider what children can see in the background and whether it would be appropriate in a classroom. This includes photographs, artwork, identifying features, mirrors etc.
- Staff will ensure that resources and videos used are age appropriate – the child may not have support immediately to hand at home if they feel distressed or anxious about content.
- Live classes will be kept to a reasonable length of time so that children do not have too much screen time and in order to minimise disruption for the family.
- Language must be professional and appropriate, including that used by any family members in the background.
- Staff must only use platforms specified by senior managers and approved by the school's ICT manager/co-ordinator for communication with pupils/students – Starleaf, Teams, Seesaw, Purple Mash.
- Staff should record the date and children's attendance to these sessions so that lack of attendance and any concerns can be passed over to the DSL.

Staff members delivering lessons or communicating with children online/virtually will raise any issues in respect of inappropriate dress, setting, behaviour etc with the child and/or parent immediately and will end the online interaction if necessary. Any such incident will be recorded and reported to the DSL.

If a staff member believes that a child or parent is recording a lesson or conversation without prior consent, the lesson will be brought to an end or the child will be logged out immediately.

In rare and exceptional circumstances where staff urgently need to contact a pupil or parent by telephone and do not have access to a school-owned device, they will discuss this with a senior member of staff. If it is agreed there is no alternative to using a personally owned device, staff members will always use 'caller withheld' to ensure the pupil and/or parent is not able to identify the staff member's personal contact details

Appendix 1: Internet use - Possible teaching and learning activities (revised 2021)

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Purple mash Mathletics BBC bitesize (KS1 & 2) Wikipedia for schools: http://schools-wikipedia.org/

Using search engines to access information from a range of websites.	Parental consent should be sought. 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. Google Yahooligans CBBC Search Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use school e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.	Welearn account AR reader mathletics E-mail a children's author E-mail Museums and Galleries ThinkUKnow
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.	Seesaw Teams Purple mash blog
	Parental consent for publication of photographs should be sought. File names (save name) should not refer to the pupil by name.	Seesaw Teams Purple mash blog Digital Storytelling BBC – Primary Art

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.	ThinkUKnow
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.	Starleaf / Teams National Archives National History Museum Imperial War Museum