



Brickhouse Primary School Online Safety Policy

Writing, Reviewing & Implementing the Policy

The Online Safety Policy has been written by the school to give guidance about all aspects of online safety. The policy has been written in consultation with staff, parents and governors and will be reviewed in line with our policy cycle. Any issues relating to online safety should be discussed with a member of the Leadership Team.

Teaching and Learning

Use of the Internet

The school recognises that 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.

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;

- exchange of curriculum and administration data with the LA and DfE;
- access to learning wherever and whenever convenient.

Using the Internet to Enhance Learning

- The school internet access will be designed expressly for educational use and the purposes of running the school and will include 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 guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Evaluating Internet Content

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and 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.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials is a part of every subject.

Internet Access

- The School will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- Internet access will be supervised and children will be encouraged to use previously vetted websites used through favourites.


- Children will be taught how to use safely a variety of search engines and be taught specific skills in locating information effectively using search engines.
- Pupils will sign annually the acceptable use policy and these will be sent home to parents with an accompanying letter to support parents in keeping their children safe when using the Internet at home.

Acceptable Use of Internet Statement

- The computer system is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and engagement.
- The school's 'Acceptable Use Policy' has been drawn up to protect all parties - the pupils, the staff and the school. The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any internet sites visited.
- Staff and pupils using internet access should sign a copy of this Acceptable Use Policy and return it to the school office.

Managing Communication

E-Mail

- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Mention of GDPR signature at the end of an email. Teacher and parent communication via email.
- The forwarding of chain letters is not permitted.
- Staff should be aware that school email may be monitored.
- All staff will have access to work email addresses which will form an integral part of communication within the school.
- Access in school to external personal email accounts are blocked. (e.g. Hotmail accounts)
- All email (both incoming and outgoing) is checked for banned words and for viruses.
- Any breach of content is reported and dealt with.
- Staff should not link their school email to their  phone.

Mobile Phones

- It is inappropriate for children or parents to contact members of staff on their mobile phone.
- Mobile phones will not be used during lessons or formal school time unless discussed with the Headship Team.
- Mobile phones should not be used in the corridors or in learning areas during the school day unless discussed with the Senior Leadership Team.
- The sending of abusive or inappropriate text messages is unacceptable.
- Children will not use mobile phones in school. If they bring a phone to school, because they need it when walking home, they must give it to a member of the Headship Team and collect it at the end of the day.
- This is the same on school trips. Children should hand any mobile phones to teachers before going on the trip as they are not needed on school trips.
- Staff and parents should not use cameras and videos on mobile phones to record images or videos whilst on school trips or visits.

Published Content

School Website

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.
- E-mail addresses should be published carefully, to avoid spam harvesting.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Pupils' Images or Work

- Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Parents or carers are asked to return a signed form if they do not wish images of their children to be used electronically.

Managing Social Networking and Personal Publishing in School

- The school will block/filter access to social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, instant messaging and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school.
- Staff are advised not to run social network spaces for student use on a personal basis.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils are encouraged to invite known friends only and deny access to others.
- Pupils are advised not to publish specific and detailed private thoughts.
- The school is aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.
- Pupils will be shown how to publish and present information to a wider audience.
- Our online safety curriculum, Natterhub teaches relevant content in relation to social media for pupils and parents.

Social Networking – Staff

- Staff are advised to be cautious of information shared on social network sites and be mindful of who has access to this information and the importance of good privacy settings. (Facebook “Friends only” / Do you want all your tweets public for the school community to read?)
- Check what can be accessed on your profile – it could be your contact details and photos people have posted.
- Think about the content of what you write and of the photographs published. Ask yourself, if you would feel comfortable about a current or prospective employer, colleague, pupil or parent, viewing your content.

- Social networking sites create a written record of what you write which can be used in disciplinary action if it is used unprofessionally or inappropriately.
- Staff should not be friends or share information with pupils. Keep a professional distance from parents at the school.
- If staff have any concerns about the use of social networking sites in relation to school, please speak to a member of the Headship Team.
- Advice from unions include:
 - Be sensible and mind your language! Don't make negative or inappropriate comments about your colleagues, pupils or school.
 - Don't be friends with pupils on Facebook.
 - Keep a professional distance at all times.
 - Don't appear in inappropriate photos.
 - Increase the privacy settings for your own profile.

Managing Filtering

- The school will work with the LA and our Internet Service Provider to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL must be reported to Leadership Team.
- LA ICT will manage the configuration of the school's filtering.
- Any material that the school believes is illegal must be reported to the Leadership Team who will report it to appropriate agencies such as IWF or CEOP.
- School internet access is controlled through the LA ICT's web filtering service and Smoothwall keyword and key stroke monitoring on all computers and iPads. This is regularly checked by the school IT Support and school will receive direct contact from Smoothwall for serious breaches as the system is monitored 24/7 by a human moderator.

Managing Information Systems

Security & Protecting Personal Data

- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.

- Portable media may not be used without specific permission followed by a virus check.
- Portable media provided by school is encrypted
- Staff should only use portable media encrypted device to store personal data and sensitive information
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.
- Sensitive documents should be password protected.

Risk Assessment

- The school will take all reasonable precautions to ensure that users access only appropriate 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. Neither the school nor the LA can accept liability for the material accessed, or any consequences resulting from Internet use. Websites to be used during a lesson or recommended for Home Learning should be checked prior to use for inappropriate content, e.g. advertisements, although it is acknowledged that these can change between this check and the site being used by pupils.
- The school audits IT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Handling Online Safety Complaints

- Complaints of Internet misuse will be dealt with by a member of the Leadership Team.
- Any complaint about staff misuse must be referred to a member of the Leadership Team.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Discussions will be held with the local PCSO's to establish procedures for handling potentially illegal issues.

Implementing this Policy

With Children

- Online Safety rules in line with our online safety curriculum are posted in rooms accessible to pupils with internet access.
- Pupils are informed that network and Internet use will be monitored.
- The school incorporates online safety learning into Computing learning to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use of the Internet is an integral part of Computing learning in school.

With Staff

- All staff have access to the Online Safety Policy and its application and importance explained.
- Staff are aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use and on the school Online Safety Policy will be provided as required.

With Parents / Carers

- Parents' attention will be drawn to the school's Online Safety Policy in newsletters and on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents is encouraged. This includes parent workshops with demonstrations and suggestions for safe home Internet use.

Date: September 2023

Review: September 2024