



Hawkinge Primary School

Online safety policy

Online Safety Policy

Scope of the Policy

Online safety encompasses internet technologies and electronic communications such as mobile phones. This policy 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 will operate in conjunction with other school policies including those for Computing, behaviour, bullying and child protection.

Paul O'Brien is the school's Online Safety Coordinator.

1 Teaching and Learning

1.1. The aims and purpose of internet use

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

The Internet is an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

1.2 Internet use to enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what is acceptable and what is not acceptable 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.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval.

2. Responsible use and management of the Internet

2.1 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 (filters in place on all links, staff apply strict filter to all Google image searches, internet access forbidden unless in the presence of a teacher).

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 KCC can accept liability for the material accessed, or any consequences of Internet access. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks are reviewed regularly.

2.2 How will pupils learn to evaluate Internet content?

- Pupils are taught, over time, to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- If staff or pupils discover unsuitable sites, the URL (address) and content will be reported to the Internet Service Provider via the Online Safety Coordinator.
- The school will ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

2.3 How will e-mail be managed?

Pupils are taught how to use e mail as part of the Computing curriculum.

- 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 details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail communication.
- Access in school to external personal e-mail accounts may be blocked.
- 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 prohibited.

2.4 Management of the School Website

- The point of contact on the Website is the school address, school e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher/Deputy Headteacher will take overall editorial responsibility and ensure that the content is accurate and appropriate.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school Website.
- Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be identified, unless parental consent is given.
- Pupils' full names will not be used on the Website, particularly associated with photographs.
- The Website will comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

2.5 Social Networking and Personal Publishing

- Pupils will not be allowed access to public or unregulated chat rooms.
- Children should use only regulated educational chat environments within our own school. This use will always be supervised and the importance of chat room safety emphasised.
- Newsgroups will not be made available unless an educational requirement for their use has been demonstrated.
- Pupils are advised never to give out personal details of any kind which may identify them or their location.

2.6 Managing Filtering and Information Security Systems

- School ICT systems capacity and security are reviewed regularly.
- Virus protection is updated regularly.
- The school will work with the LA and Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Coordinator. In the event that this is a child, the child's parent will be informed.
- The ICT technician will make regular checks to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Filtering strategies will be selected by the school in discussion with the filtering provider where appropriate. Where possible, the filtering strategy will be selected to suit the age and curriculum requirements of the pupil.

2.7 Managing Video Conferencing

- Videoconferencing is appropriately supervised for the pupils' age. Children will not be able to make or receive a video conference call unless they are supervised. Videoconferencing uses the educational broadband network.

2.8 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.

2.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1988.

3. Policy Decisions

3.1 Authorising Internet Access

- All staff must read and sign the 'Acceptable Use Policy' before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted internet access.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved online materials.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form.
- Pupils will also sign a 'code of conduct' form. This reinforces online safety rules which are displayed in classrooms. These rules are reinforced to the children whenever the internet is accessed. Pupils are informed that internet access is monitored and appropriately followed up. Inappropriate internet use sanctions are in place to address inappropriate behaviour. These are as follows:
 - 1) Withdrawal of internet access for the remainder of the lesson.
 - 2) Withdrawal of internet access for the remainder of the day.
 - 3) Withdrawal of internet access for one week.
 - 4) Denied internet access for a term and parents informed.Other sanctions within the school behaviour policy (may be combined with sanctions 1-4).
- Online safety training will be embedded within the Computing/P.S.H.E. curriculum.

3.2 Assessing Risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. See 2.1
- All staff including teachers, supply staff, classroom assistants and support staff, will be made aware of this 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.
- Staff development in the safe and responsible Internet use and on school Internet policy will be provided as required.
- Staff are also expected to use the internet appropriately in school. Expectations of staff are outlined in the staff code of conduct document guidance.
- The school will audit ICT provision to establish if the Online Safety policy is adequate and that its implementation is effective.

3.3 Handling Online Safety Complaints and Working with Parents

- Complaints of internet misuse will be dealt with by the Online Safety Coordinator.
- Any complaint about staff misuse will be referred to the Headteacher.
- If a child misuses the internet then sanctions are in place to address the inappropriate behaviour. These are outlined in the summary guidance for parents.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Procedures to deal with a concern about internet misuse are attached as an appendix. Any complaints concerning the misuse of the internet in school will be in accordance with our school complaints policy.
- Parents' attention will be drawn to the Online Safety Policy in newsletters, the school brochure and on the school Web site.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
- A stock of relevant leaflets/websites will be available for parents/carers.

3.4 Community Use of the Internet

- This policy will be made known to any members of the community who may access the internet in school.

12 Monitoring and review

12.1 The Computing co-ordinator is responsible for monitoring the standards of work and quality of teaching in use of the internet. The Computing co-ordinator is also responsible for supporting colleagues in the teaching of ICT, for being informed about current developments in the subject, and for providing a strategic lead and direction for the subject in the school.

12.2 This policy is reviewed every year.

Policy reviewed September 2018

Review date: September 2019