Haytor View Community Primary School & Nursery
E Safety Policy 2023-24

Learning together - enjoying success - aiming high - celebrating difference – enriching community

Teaching and learning

Why Internet and digital communications are important:

- 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.
- Internet use is a part of the curriculum and a necessary tool for staff and pupils.
- The school Internet access is provided by South West Grid for Learning (SWGFL) and includes 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.
- Pupils will be educated in the effective use of the internet.
- Pupils will be shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate Internet content:

- The school will seek to 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.
- Pupils will be taught how to report unpleasant internet content to teaching staff.

Managing Internet Access

Information system security

- School ICT systems security will be reviewed regularly
- Virus protection will be updated regularly
- Security strategies will be discussed with the Local Authority

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive unacceptable e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- Staff to pupil email communication must only take place via a school email address and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.
- Staff should not share personal email addresses numbers with pupils and parents (a school admin address is provided for staff where contact with parents is required).

Published content and the school web site

- 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.

Publishing photographs, images and work

- Pupils' full names will be avoided on the website, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs or images of pupils are published.

- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories
- Staff will not keep images of children on personal devices e.g. memory sticks, or use them for any use other than in school.

Social networking and personal publishing on the school learning platform

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- All users will be advised never to give out personal details of any kind which may identify them, anybody else or their location.
- Pupils, parents and staff will be advised on the safe use of social network spaces
- Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing filtering

- The school will work in partnership with SWGFL 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 Head Teacher.
- The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- If used, pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- If used, videoconferencing will be appropriately supervised for the pupils' age.

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.

Other devices

- Mobile phones and associated cameras will not be used during lessons or formal school time. Taking photographs at any time without the subject's consent is prohibited.
- The sending of abusive, offensive or inappropriate material is forbidden.
- Staff should not share personal telephone numbers with pupils and parents (a school phone is provided for staff where contact with parents is required).

Protecting personal data

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

<u>Policy Decisions</u>

Authorising Internet access

- All staff will be informed of their appropriate use of ICT systems, this will form part of the induction process.
- The school will maintain a current record of all staff, governors and pupils who are granted access to school ICT systems.
- Parents will be provided with necessary information via the school newsletter.
- Pupils must agree to comply with the Responsible Internet Use rules, which are discussed through a whole school assembly and as part of class ICT lessons.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Devon Children's Services can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if this E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate and effective

Handling E-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 Head Teacher and will be dealt with through the Governing body complaints procedure if required.
- Complaints of a child protection nature must be referred to the Senior Designated Professional (SDP) for Safeguarding and 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 E-Safety policy.

Communicating E-Safety

Introducing the E-Safety policy to pupils

- Appropriate elements of the E-Safety policy will be shared with pupils
- Pupils will be informed that network and Internet use will be monitored
- Curriculum opportunities to gain awareness of E-Safety issues and how best to deal with them will be provided for pupils

Staff and the E-Safety policy

- All staff will be given the School E-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.
- Staff who 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 carer's attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school web site.
- Parents and carers will from time to time be provided with additional information on E-Safety.
- Parents and carers will be reminded that they must not publish any images or comments of performances and other community events on social network sites before and after each event.

This policy should be read in conjunction with the Schools Safeguarding Policy.

Monitoring, evaluation and review
The school will review this policy annually and assess its implementation and effectiveness. The policy will be promoted and implemented throughout the school.

This policy is monitored on a day-to-day basis by the Head Teacher who reports to governors about the effectiveness of the policy as part of the Head Teacher report.

This E-Safety policy is the governors' responsibility and they review its effectiveness annually. They do this by reviewing incidents in discussion with the Head Teacher.