E-SAFETY POLICY

Bembridge CE Primary School

Introduction
E-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.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through this published policy.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of filtering.

Writing and reviewing the e-safety policy
The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT and for child protection.

- The school's e-Safety Officer is also the ICT Subject Leader, who works in close co-operation with the headteacher who is the Designated Child Protection Officer.
- Our e-Safety Policy has been written by the school. It has been agreed by the staff and governors.
- The e-Safety Policy will be reviewed on a three yearly cycle.

TEACHING AND LEARNING
Why Internet use is 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 statutory curriculum and a necessary tool for staff and pupils.

Internet use will 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 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 will guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

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 the school e-safety officer and the Headteacher.

- Staff should ensure that the use of Internet derived materials by themselves and by their pupils complies with copyright law.

Information system security

- The security of the school information systems will be reviewed regularly by our Network Manager
- Virus protection will be installed by our ICT Technician and updated regularly by the technician and staff who use computers.
- The school uses the RM safety Broadband with its firewall and filters.

E-mail

- Pupils may only use approved e-mail accounts on the school system. Children are not allowed access to individual e-mail accounts or chatrooms whilst in school.
- Whole-class or group e-mail addresses are used in primary schools.
- 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.
- 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.

Published content and the school web site

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
The Headteacher, who is also the Designated Child Protection Officer 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. Photographs must only be taken on a camera provided by the school.
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission is sought from parents re photographs of their child being published on the school website.

Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Pupils are advised about the use of social networking sites out of school. 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, 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.

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.
- Pupils are not permitted to have mobile phones in school.
- Staff adhere to the schools Mobile Phone Policy.

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

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the acceptable ICT use agreement, 'E-Safety Agreement Form for School Staff', before using any school ICT resource.
- At Key Stage 1 and Early Years, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

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 can accept liability for the material accessed, or any consequences of Internet access.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a member of the SLT.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Community use of the Internet

The school does not allow community use of the internet

COMMUNICATIONS POLICY

Introducing the e-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.
- Advice on e-Safety will be introduced at an age-appropriate level to raise the awareness and importance of safe and responsible internet use and taught as an on going area of the ICT Curriculum.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff are aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential at all times.

Enlisting parents' / carers' support

- The School e-Safety Policy will be published on the school website
- Parents sign a letter giving permission for their child to use the internet and email in school