E-Safety Policy

Ownership	**Headteacher**
Created	**April 2015**
Approved by Governors	**25/06/15 and 28/11/18**
Updated (if apt)	**28/11/18**
To be reviewed	**November 2020**

1. Writing and Reviewing the E-Safety Policy

The E-Safety Policy is part of the School Development Plan (Safeguarding Action Plan) and relates to other policies including those for ICT, Behaviour, and Anti-bullying, Social Networking and Child Protection.

The school's DSL will also act as E-Safety Coordinator/Champion.

Our e-Safety Policy has been written by the school, building on the SWGFL E-Safety Policy (January 2013) and most recent government guidance. It has been agreed by all staff and approved by governors.

The E-Safety Policy and its implementation will be reviewed annually (next review November 2019).

2. 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 children 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 is designed expressly for pupil use 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 in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

The school will ensure that the 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. Please see appendix 1 – Internet Acceptable Use.

3. Managing Internet Access

Information system security

School ICT systems capacity and security will be reviewed regularly. Virus protection is updated regularly. Advice on security strategies will be monitored and clarification sought as necessary. Our wireless network is fully secured and filtered.

4. E-mail

Pupils may only use approved e-mail accounts on the school system and email usage will be supervised and monitored by a staff member. 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. The forwarding of chain letters is not permitted.
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 head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

5. Publishing pupils' images and work

Photographs 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 Web site, particularly in association with photographs.
Permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
Pupils' work can only be published with the permission of the pupil and parents.

6. Photographs/Videos

Photos and video of pupils should be taken on school equipment only. These images should be transferred from the internal memory (cards) regularly and stored on the school's secure network. Under no circumstances should staff take photos or videos of children on personal equipment.

7. Social networking and personal publishing (Also see Social Networking Policy)

The school will block/filter access to social networking sites.
Newsgroups will be blocked unless a specific use is approved. Pupils will be advised never to give out personal details of any kind that may identify them or their location.
Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

8. Managing filtering

The school will work with the LA, SWGFL and the 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 E-Safety Champion (Headteacher).
Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

9. 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.

10. Protecting personal data

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

11. Policy Decisions

11.1 Authorising Internet access

All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource. The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance, a member of staff may leave or a pupil's access be withdrawn.

For Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials. Parents will be asked to sign and return a consent form.

11.2 Assessing risks

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. The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective. The school is registered with the 360degree E-safety tool.

11.3 Handling e-safety complaints

Complaints of Internet misuse will be dealt with by the head. 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. Pupils and parents will be informed of the complaints procedure. Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

12. Communication

12.1 Introducing the e-safety policy to pupils

E-safety rules will be posted in all rooms and discussed with the pupils at the start of each year.

Pupils will be informed that network and Internet use will be monitored.

12.2 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.

12.3 Enlisting parents' support

Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

13

Training

E-Safety Training

Training by the Dorset Safe Schools Team DSST will be provided to ensure that staff, children, parents and governors are kept up to date with E-Safety issues

Appendix 1 – Internet Acceptable Use Policy

Appendix 1 – E-Safety Policy

Stower Provost Community School - **INTERNET ACCEPTABLE USE POLICY**

The Internet is an invaluable and exciting learning resource, which is constantly being added to and changing. Stower Provost Community School encourages the use by pupils and staff of the rich information resources available on the Internet together with the development of appropriate skills to analyse and evaluate such resources. These skills will be fundamental in the society our pupils will be entering. On-line services significantly alter the information landscape for schools by opening classrooms to a broader array of resources. Teaching and library materials are carefully chosen to be consistent with national policies, to support and enrich the curriculum while taking into account the varied teaching needs, learning styles, abilities and developmental levels of the pupils. Internet access, because it may lead to any publicly available site in the world, will open classrooms to electronic information resources which have not been selected by teachers as appropriate for use by pupils.

It is our aim that pupils should be able to explore the Internet including the use of electronic mail in a safe and well-managed environment. To ensure this, the following procedures will be followed.

1. Children not to be given access to the Internet without adequate adult supervision and appropriate filtering of content. The school uses the filtered access provided by DCC through its contractual arrangement with the Internet Service Provider. Staff can bypass this filtering but will only do so with great caution.

2. Siting computers used by children capable of accessing the Internet so that the screens are open to ‘public’ view.

3. Staff should evaluate new materials/web sites to use and give prior guidance and instruction to pupils in the appropriate use of such resources.

4. Electronic mail. Occasionally children may use e-mail to send and receive messages. Key Stage 2 children would do this under supervision of the teacher through using a class e-mail Address.

5. All members of staff are responsible for involving pupils in discussion and agreement of rules for the responsible use of the Internet including e-mail, chatrooms, and ensuring they are adhered to. These would include: not entering chatrooms, not giving out their addresses or telephone numbers, not sending or displaying messages that are offensive, respect for computer equipment, passwords and other children’s work.

6. Class teachers will be responsible for making this policy available to all members of staff and volunteer helpers who work in their class and ensuring they are aware of possible misuses of on-line access and their responsibilities towards pupils.

7. Parents will be informed about their children's use of the Internet and the procedures taken to ensure responsible use in school and are invited to contribute comments and express any concerns. They will be encouraged to work in partnership with the school in setting and conveying the standards that their children should follow, when using media and information sources.

8. All staff need to ensure that children cannot be publicly identified when putting their own information into Internet sites e.g. school website – avoid the use of the first and surnames of individuals in a photograph. This reduces the risk of inappropriate unsolicited attention from people outside the school.

An easy rule to remember is:

If the pupil is named, avoid using their photograph.

If the photograph is used, avoid naming the pupil.

Only use images of pupils in suitable dress to reduce risk of inappropriate use of images of pupils.

Ask for parental permission to use an image of a pupil.