Plympton St Maurice Primary School

Online Safety Policy

Reviewed September 2018

Online Safety Policy

Online Safety (or E-Safety) encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's e-safety policy will operate in conjunction with other policies including those for Safeguarding, Pupil Behaviour, Bullying, Curriculum, Data Protection, Internet policy and Security.

Good Habits

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the South West Grid for Learning including the effective management of content filtering.

The school has appointed Online Safety coordinators.

Our Online Safety Policy has been written by the school, building on the South West Grid for Learning guidance. It has been agreed by the senior management team and approved by governors.

The Online Safety Policy will be reviewed annually.

Why is Internet Use Important?

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 administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access

Pupils will use the internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Benefit Education?

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;
- 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 Local Authority and Department of Education;
- access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school internet access will be 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.
- Internet access is planned to enrich and extend learning activities.
- Staff guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff/pupils and parents must read and sign the Acceptable ICT Use Agreement' before using any school ICT resource. We have an acceptable use policy for children 8 years and under. These are circulated to parents annually.
- Parents will be informed that pupils will be provided with supervised internet access.
- Parents will be asked to sign and return a consent form for pupil access.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to their teacher, in the first instance, who then alerts the school business manager, who will be able to add the site to the school filter list.
- School will ensure that the use of internet derived materials by pupils and staff complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- 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 personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses are used in school. Individual e mails are used with restrictions placed on pupils to send e mails from pupil to pupil unless authorised to send to other schools for the purpose of curriculum learning.
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations is 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.

Social Networking

- We will block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location
- Pupils are advised not to place personal photos on any social network space.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

Filtering

The school will work in partnership with the Local Authority and the South West Grid for Learning to ensure filtering systems are as effective as possible.

Video Conferencing

- 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.

- Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden. (See mobile phone policy.)

- Staff will be issued with a school phone where contact with pupils/ parents is required.

Published Content and the School Web Site

- The contact details on the Website will be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The Head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

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 website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil and parents.

Information System Security

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

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate. This will include monitoring three times per academic year and incidents reported on an incident log to the head teacher who will report to the governors.

Handling Online 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.
- 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.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.

Staff

- All staff will be given the School Online Safety Policy and the importance of the policy explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

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

All pupils/staff and parents will be required to sign an acceptable use policy agreement.

(See also Behaviour policy, Data policy, Internet policy, Filtering policy, and Mobile Phone policy.)

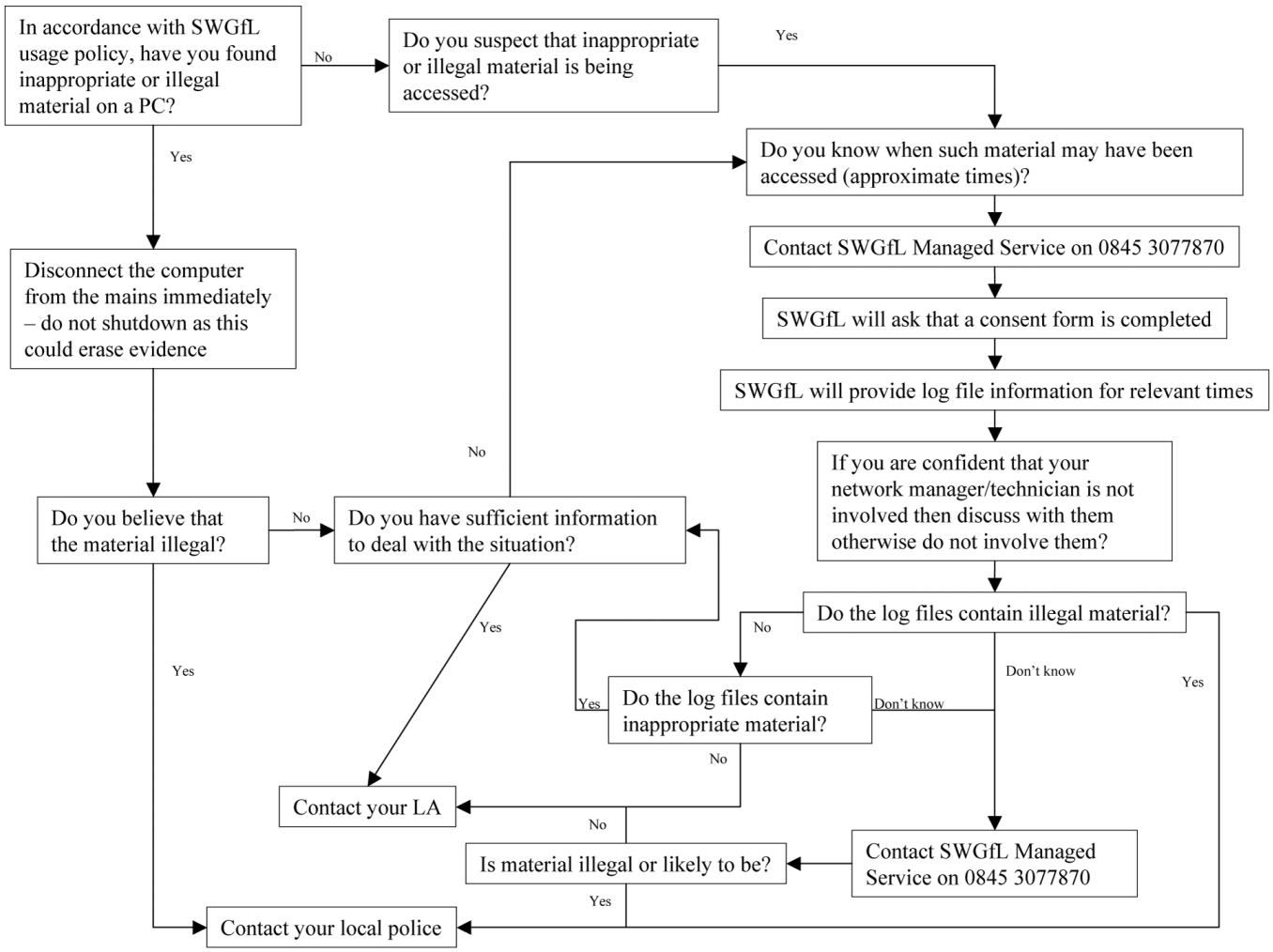
This document has been completed, ensuring that all concerned with its production have taken into account current legislation relating to race, gender, age, ability and disability.

This will ensure that, where possible and within the limits of reasonable adjustment, we meet the needs of every child and adult linked to the life of the school.

The school Online Safety policy is available on request or from the school website: www.plympton-st-maurice-primary.org.uk

Appendix A

Flowchart for responding to e-safety incidents in school



Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

Staff Online Safety Rules

These Online Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.