E- Safety Policy

This policy has been written with the underlying principles of our Church of England VC school status.

January 2013

E SAFETY POLICY

INTRODUCTION AND AIMS

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 Student Behaviour, Bullying, Curriculum, Data Protection and Security.

This policy statement has been formally adopted by the governing body, in consultation with the Headteacher. It is consistent with the overall aims of the school as expressed in the School Prospectus and the Christian Foundation of the school as expressed in the Trust Deed.

SCHOOL AIMS

1. CHRISTIANITY
To encourage the experience of Christian life and participation in worship.

2. CURRICULUM
To enable each child to achieve the highest standard of work and learning of which s/he is capable, which will help each one of them have a good start in life, so that they are able to achieve social and economic well being.

3. HEALTH AND WELL BEING
To help our children enjoy good health and a healthy life style and to ensure they know how to stay safe.

4. ETHOS
To promote qualities of tolerance, respect and awareness in a community where everyone feels appreciated, protected and safe and is able to develop as an individual.

5. PARTNERSHIP
To work together with parents.
To contribute to the life of the neighbourhood, the parish and beyond.

6. ENVIRONMENT
To create a stimulating environment in and around the school, which will help develop lively and enquiring minds, positive and responsible attitudes and will promote aesthetic and spiritual awareness.

Good Habits

E-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 Edit including the effective management of content filtering.

- National Education Network standards and specifications.

Contents

School e-Safety Policy

The school will appoint an e-Safety group. This will be the Designated Child Protection Teacher (Head Teacher), the ICT co-ordinator and Deputy Head Teacher.
Our e-Safety Policy has been written by the school. It has been agreed by the senior management team and will be approved by governors.

The e-Safety Policy will be reviewed annually. This policy will next be reviewed in January 2014.

Why is Internet use important?

The purpose of Internet use in school is to raise educational standards, to promote student 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 learning wherever and whenever convenient
- 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 DCSF

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 will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support 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, 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 must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource
- 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 student access
- Pupils must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement (KS1 and KS2)

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported.
- We will ensure that the use of Internet derived materials by pupils and staff complies with copyright law
- Pupils should 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 (Easy Mail)
- 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
- Access in school to external personal e-mail accounts may be blocked
- E-mail sent to external organisations 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

Social Networking

- The School has blocking/filtering access to social networking sites and newsgroups unless a specific use is approved
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space
- Pupils should be 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, MSP and Becta to ensure filtering systems are as effective as possible.

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 are not permitted in school. The sending of abusive or inappropriate text messages out of school is discouraged.
- The school is working towards SMS services in line with LA guidance

Published Content and the School Web Site

- The contact details on the Web site will be the school address, e-mail and telephone number. Staff or pupils personal information will not be published
- The Head teacher or ICT co-ordinator 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 be appropriate for the context
- Pupils' full names will not be used anywhere on the Web site or Blog, 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

Protecting Personal Data

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

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 Dorset County Council 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.

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 Headteacher.
- 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 shared in specific lessons and reminders throughout their time at Preston Primary
- Pupils will be informed that Internet use will be monitored

Staff
- 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 that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues

Parents
- Parents' attention will be drawn to the School e-Safety Policy in newsletters, and on the school Web site. They will have a Parents E-Safety meeting within the year.
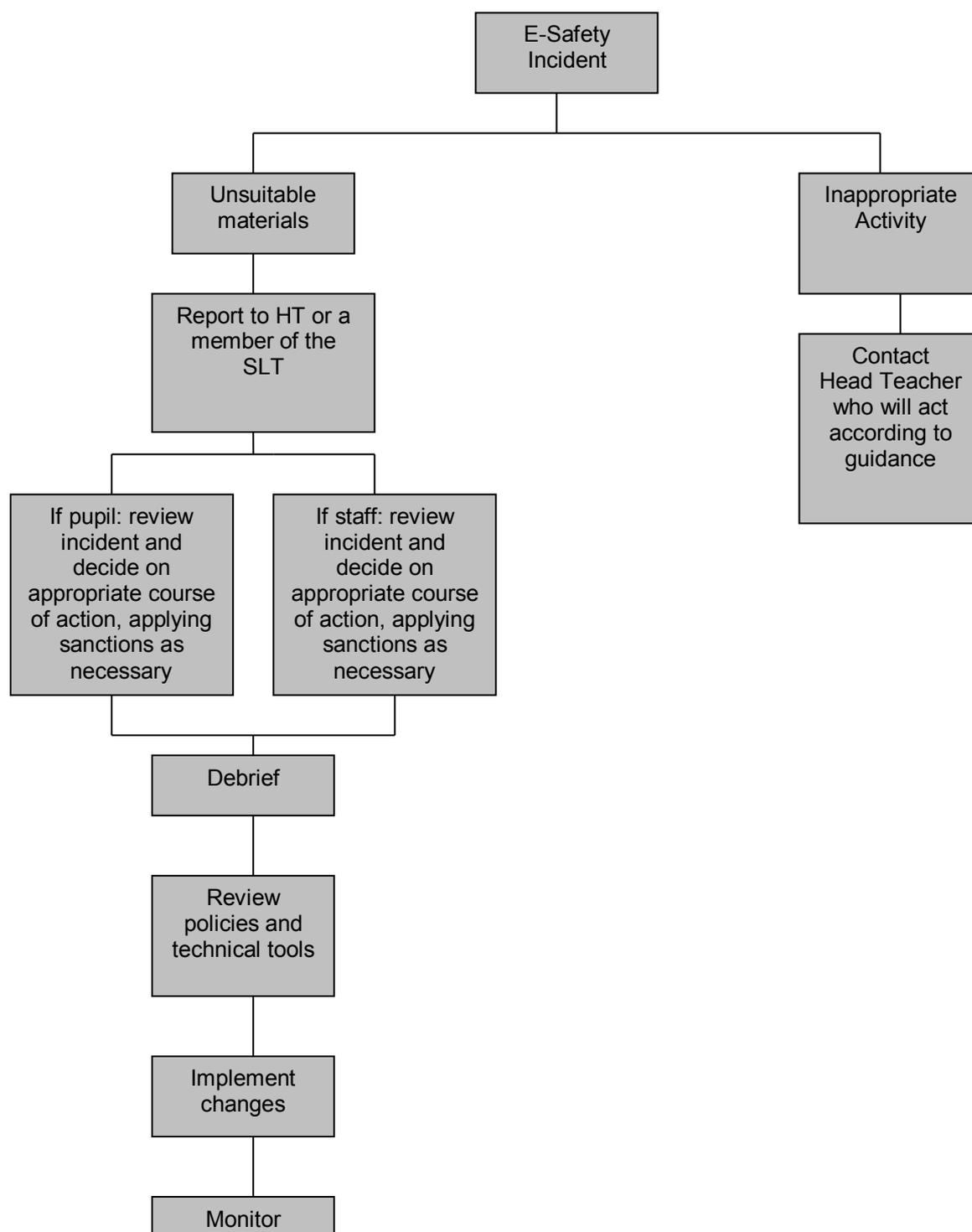
Referral Process – Appendix A

E-Safety Rules KS1– Appendix B

E-Safety Rules KS2 – Appendix B

Appendix A

Flowchart for responding to e-safety incidents in school

```
                        ┌─────────────────┐
                        │   E-Safety      │
                        │   Incident      │
                        └────────┬────────┘
                 ┌───────────────┴───────────────┐
        ┌────────────────┐              ┌──────────────────┐
        │   Unsuitable   │              │   Inappropriate  │
        │   materials    │              │     Activity     │
        └───────┬────────┘              └────────┬─────────┘
        ┌────────────────┐              ┌──────────────────┐
        │ Report to HT or│              │     Contact      │
        │  a member of   │              │   Head Teacher   │
        │    the SLT     │              │   who will act   │
        └───────┬────────┘              │  according to    │
                │                       │    guidance      │
    ┌───────────┴───────────┐          └──────────────────┘
┌──────────────┐  ┌──────────────┐
│If pupil: review│ │If staff: review│
│incident and   │ │incident and   │
│decide on      │ │decide on      │
│appropriate    │ │appropriate    │
│course of      │ │course of      │
│action,        │ │action,        │
│applying       │ │applying       │
│sanctions as   │ │sanctions as   │
│necessary      │ │necessary      │
└───────┬──────┘  └───────┬──────┘
        └─────────┬───────┘
           ┌──────────────┐
           │   Debrief    │
           └──────┬───────┘
           ┌──────────────┐
           │   Review     │
           │ policies and │
           │technical tools│
           └──────┬───────┘
           ┌──────────────┐
           │  Implement   │
           │   changes    │
           └──────┬───────┘
           ┌──────────────┐
           │   Monitor    │
           └──────────────┘
```

Adapted from Becta – E-safety

Think before you click

S I will only use the Internet and email with an adult.

A I will only click on icons and links when I know they are safe.

F I will only send friendly and polite messages.

E If I see something I don't like on a screen, I will always tell an adult.

My Name:

My Signature:

KS1 E-Safety Rules

Think before you click

- We never share our Virtual Classroom password with anyone but our parents or guardians.

- 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 or unhappy with.

- We immediately close any webpage we're not sure about.

- We only e-mail people an adult has approved.

- We send e-mails and messages that are carefully written, polite and friendly.

- We never give out personal information.

- 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 (without an adult present).

- We think carefully about pictures and messages we share with others (we know they could be passed on to anyone).

Stay SMART!

(www.kidsmart.co.uk)

KS2 E-Safety rules