Merryhills Primary School

Merryhills

TRUTH ABOVE ALL

E Safety Policy

December 2017

Responsibility: Michelle Motley

Review Date: December 2018

E-Safety Policy Overview

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

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 London Grid for Learning including the effective management of content filtering.

□ The school will work with Enfield LEA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

□ Any material that the school believes is illegal must be reported to appropriate agencies such as IWF (Internet Watch Foundation) or CEOP (Child Exploitation & Online Protection Centre).

Contents

Merryhills Primary School acknowledges the assistance of Kent County Council in providing content in this document.

School e-Safety Policy

Merryhills Primary School's Safeguarding Designated Officer will also act as the E-Safety Coordinator as the roles overlap.

Our e-Safety Policy has been written by the school. It has been agreed by the senior management team and approved by governors in December 2017.

The e-Safety Policy will be reviewed annually by the ICT Coordinator or other senior member of staff.

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;

□ inclusion in the National Education Network which connects all UK schools (The NEN is the UK collaborative network for education, providing schools with a safe, secure and reliable learning environment and direct access to a growing range of online services and content);

□ 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 DfE; 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 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

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the e-safety coordinator or other senior member of staff.
- 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.
- 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

- Schools should block/filter 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.
- Pupils will be advised on the use of the CEOP report button

Filtering

The school will work in partnership with the Local Authority and the Internet Service Provider to ensure filtering systems are as effective as possible.

Video Conferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- 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 school time. The sending of abusive or inappropriate text messages is forbidden.
- Personal mobile phones will not be used for taking photographs of children

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 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’ names will not be used anywhere on the Web site or Blog in association with photographs.
- There is a statement in the Home School Agreement referring to our policy on digital images of children.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection is 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 Enfield Council can accept liability for the material accessed, or any consequences of Internet access.
- The school should 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.
- Parents wishing to complain about e-safety issues should use the established school complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

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 informed about and given access to 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.

Parents

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

E-Safety Incident

Illegal material or activity found or suspected

Illegal activity

Report to IWF and/or police

Report to police

Report to CEOP

(but police if risk of immediate danger)

Report to ICT coordinator and/or e-safety officer

Secure and preserve evidence

If pupil: review incident and decide on appropriate course of action, applying sanctions as necessary

Await police/ IWF/CEOP response

If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations, seeking advice from LEA an Governors on the treatment of the offender/victim

If no illegal material or activity is confirmed, refer to internal disciplinary procedures for staff

Unsuitable materials

Child at risk

Illegal content

If Staff: review incident and decide on appropriate course of action, applying sanctions as necessary

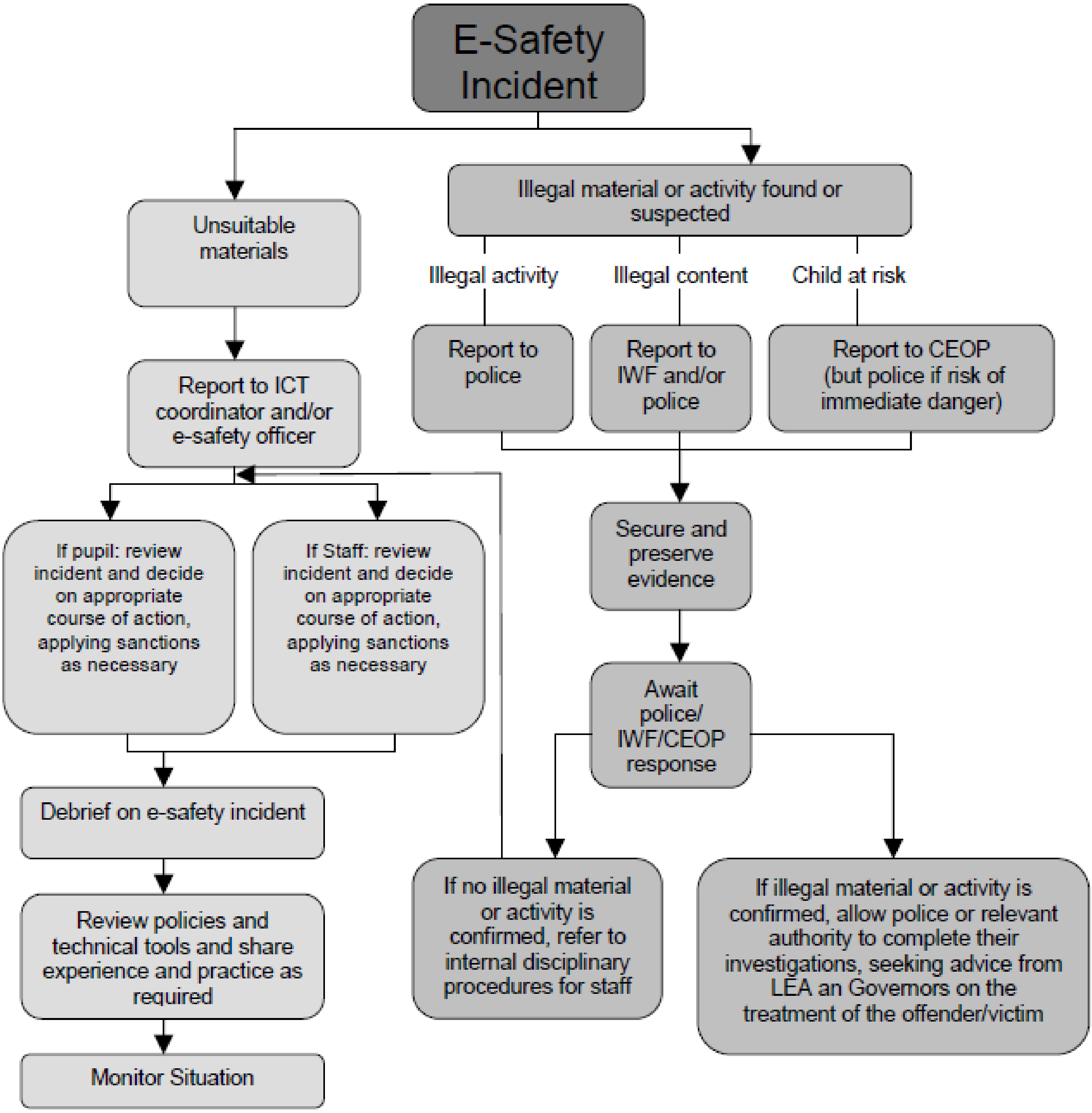
Debrief on e-safety incident

Review policies and technical tools and share experience and practice as required

Monitor Situation

Appendix A

Flowchart for responding to e-safety incidents in school


E-Safety Incident
Unsuitable materials
Illegal material or activity found or suspected
Illegal activity
Illegal content
Child at risk
Report to police
Report to IWF and/or police
Report to CEOP (but police if risk of immediate danger)
Report to ICT coordinator and/or e-safety officer
If pupil: review incident and decide on appropriate course of action, applying sanctions as necessary
If Staff: review incident and decide on appropriate course of action, applying sanctions as necessary
Secure and preserve evidence
Await police/ IWF/CEOP response
Debrief on e-safety incident
Review policies and technical tools and share experience and practice as required
Monitor Situation
If no illegal material or activity is confirmed, refer to internal disciplinary procedures for staff
If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations, seeking advice from LEA an Governors on the treatment of the offender/victim

Adapted from Becta – E-safety 2008

Adapted from Becta – E-safety 2008

Appendix B

Key Stage 2 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.