Lymington Junior School

Computing & E-Safety Policies

'Partnership in Learning'

Lymington Junior School E-Safety Policy

Context:

E-Safety encompasses Internet technologies, VLEs and electronic communications such as mobile phones, digital cameras and wireless technology. This policy recognises the need to educate all members of the school community about the benefits and risks of using ICT technology and provides safeguards and guidance for all users, to enable them to control their online experiences.

Lyminton Junior School's e-safety policy will operate in conjunction with other policies and guidance including those for Pupil Behaviour, Bullying, Learning and Teaching, ICT, Data Protection and Safeguarding Children.

Good Habits

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

- Responsible ICT use by all staff and pupils
- Guidance for safe and appropriate use of ICT technologies shared explicitly with all pupils and staff.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from HCC's associated Grid for Learning including the effective management of content filtering.
- National Education Network standards and specifications.

School e-Safety Policy

Internet Use

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.
Pupils will have access to the Internet both inside and outside of school and will need to learn how to evaluate Internet information and to take care of their own safety and security.
Staff will have access to the Internet and both inside and outside of school and will need to learn how to evaluate the appropriateness, safety and security of all websites/web pages used, linked, or signposted to pupils Internet information and to take care of their own safety and security.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff and pupils must read and agree to the 'Acceptable 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 pupil access to the Internet.

Safe Use Of The Internet

- The Computing curriculum will begin with a module on e-safety every year.
- If staff or pupils using the school network discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the Red Team or network manager (Mrs Hutchings).
- School 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.

Messaging, E-Mail & Social Networking

LJS recognises that members of the school community have access to the Internet and messaging/social networking sites outside of school and makes the following recommendations:

All Members of the school community will be taught that they:

- Must immediately inform an adult/ member of staff if they receive offensive message.
- 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 is not allowed.
- E-mails sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Are not permitted to forward chain letters.
- Should never to give out personal details of any kind which may identify them or their location

- Should not place statements, personal photos or content on any social network space which could bring the school into disrepute

In addition to this,

- The school Network, through HCC filters should block access to social networking sites unless a specific use is approved.

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.

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

Published Content and the School Web Site

- The contact details on the school web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content of school web site pages is accurate and appropriate.

Publishing Pupils' Images and Work

- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained each year before photographs of pupils are published on the school Web site

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 the Local Authority 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.
- 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.

Communication of Policy

Pupils

- Rules for Internet access will be posted in the ICT Suite.
- Rules for Acceptable Usage of the Internet will be explicitly shared with pupils.
- 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.

Parents

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

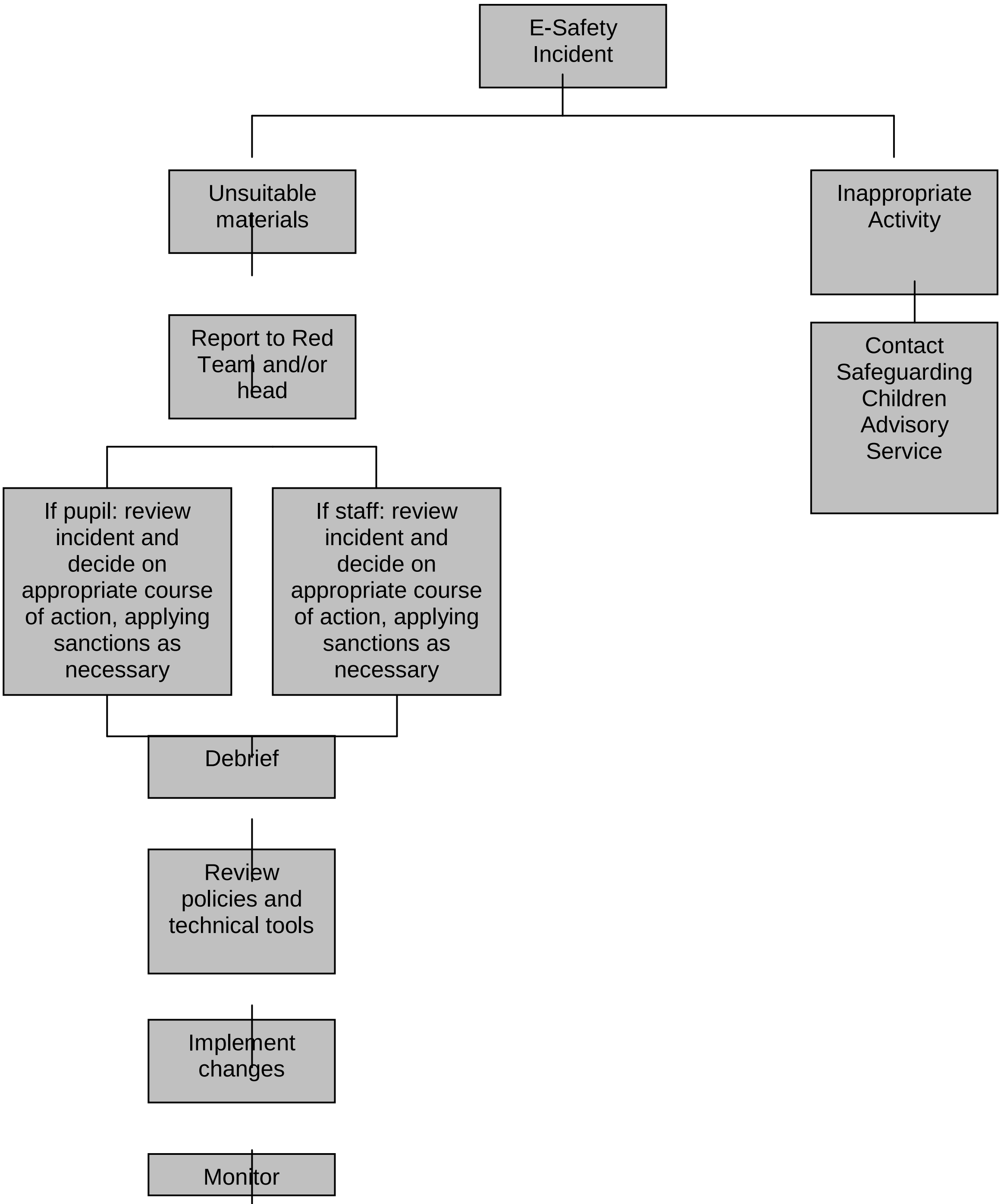
Flowchart for responding to e-safety incidents in school – Appendix A

E-Safety Rules (Pupils) – Appendix B

Staff Acceptable Use Policy – Appendix C

Appendix A

Flowchart for responding to e-safety incidents in school


E-Safety Incident
Unsuitable materials
Inappropriate Activity
Report to Red Team and/or head
Contact Safeguarding Children Advisory Service
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
Debrief
Review policies and technical tools
Implement changes
Monitor

(Adapted from Becta – E-safety 2005)

Appendix B

E-Safety Rules

These e-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.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, or blogs/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.

Appendix C

Staff Acceptable Use Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Safeguarding Lead (DSL).
- I will ensure that any electronic communications with pupils are compatible with my professional rôle.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information 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.