WOODNEWTON
a learning community

Woodnewton – A Learning Community

E-Safety Policy

May 2014

E-Safety Policy

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 Talk Straight, including the effective management of content filtering.
- National Education Network standards and specifications.

E-Safety Audit – Woodnewton

This quick self-audit will help the senior management team (SMT) assess whether the e-safety basics are in place.

Has the school an e-Safety Policy that complies with CYPD guidance?	Y
Date of latest update: May 2014	
The Policy was agreed by governors in: May 2014	
The Policy is available for staff at: School and on the school's website	
And for parents at: School and on the school's website	
The designated Child Protection Teacher/Officer is: Ellen Wallace	
The e-Safety Coordinator is: Richard Smyton	
Has e-safety training been provided for both pupils and staff?	Y
Is the Think U Know training undertaken?	Y
Do all staff sign an ICT Code of Conduct on appointment?	Y
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	Y
Have school e-Safety Rules been set for pupils?	Y
Are these Rules displayed in all rooms with computers?	Y
Internet access is provided by an approved educational Internet service provider and complies with DfE requirements for safe and secure access.	Y
Has the school filtering policy has been approved by SMT?	Y
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y

School e-Safety Policy

The school has appointed an e-Safety coordinator.

Our e-Safety Policy has been written by the school.

It has been agreed by the senior management team and approved by governors.

The e-Safety Policy will be reviewed annually.

This policy will next be reviewed May 2015.

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;
- 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

- 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 and 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 the Talk Straight helpdesk via the e-safety coordinator or network manager.
- 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.

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

School blocks/filters 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 Academy Trust and Talk Straight 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.

Mobile Phones

Mobile phones will not be used for personal use during lessons or formal school time and children's phones must be left at the office. The sending of abusive or inappropriate text messages is forbidden.

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.

Published Content and the School Web Site

The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published. A Vice principal 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, Twitter, Blog, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the public school website.

Work can only be published with the permission of the pupil and parents.

Parents and visitors are asked not to post any pictures or multimedia taken in school to any online space.

Information System Security

School ICT systems capacity and security will be reviewed regularly. Virus protection will be installed and updated regularly.

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 Academy Trust 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 Principal. 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 all networked rooms. 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 prospectus and on the school web site.

Referral Process – Appendix A

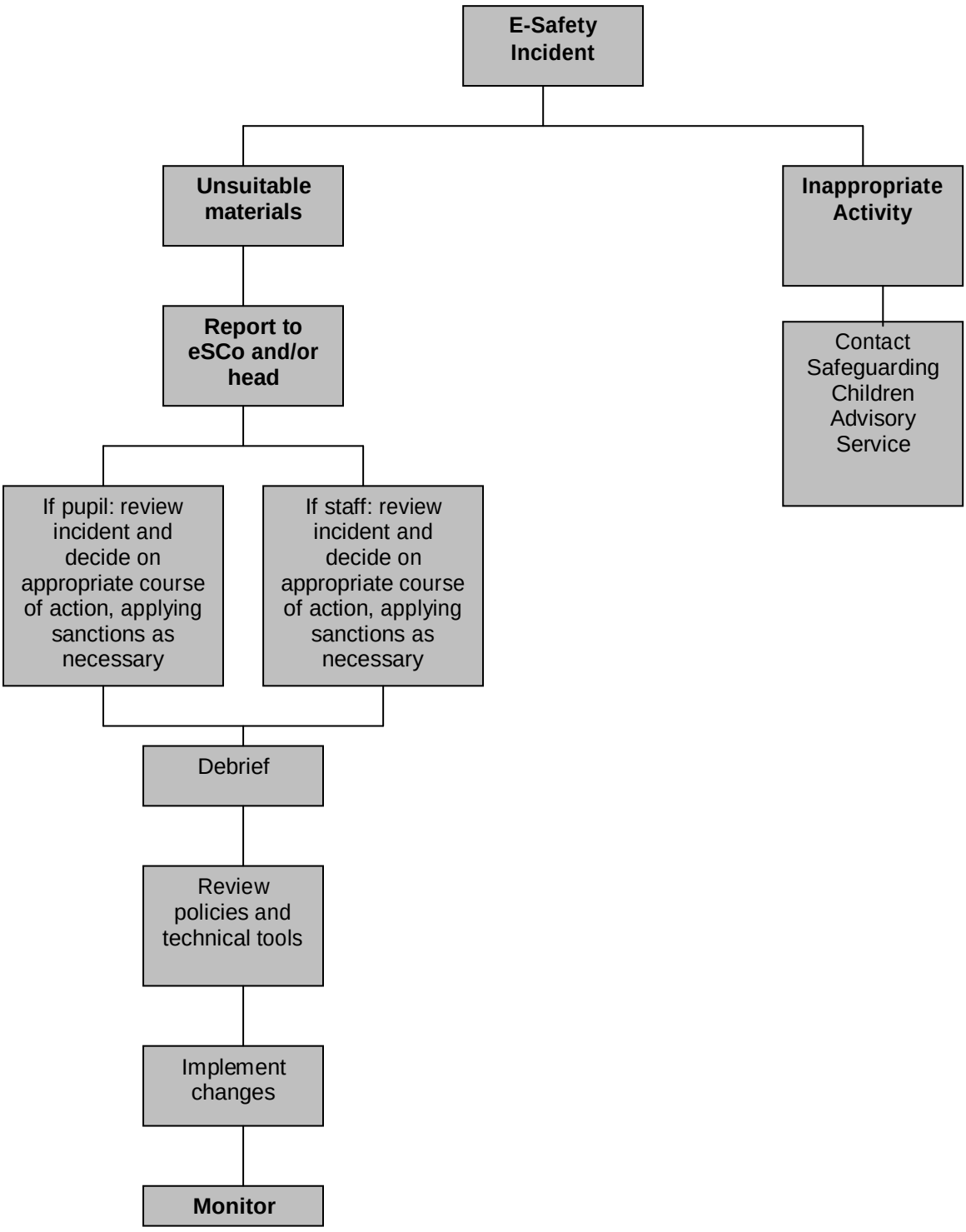
E-Safety Rules– Appendix B

Letter to parents – Appendix C

Staff Acceptable Use Policy – Appendix D

Appendix A

Flowchart for responding to e-safety incidents in school



Think then Click!

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.

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.
- 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.

Woodnewton

e-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Parent/Guardian's Consent for Web Publication of Work and Photographs

I agree that _____'s work may be electronically published. I also agree that appropriate images and video that include them may be published subject to the website and learning platform in line with the school policy that individual photographs will not be accompanied by pupil names.

Parent/Guardian's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for _____ to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	**Date:**
Please print name:	

Please complete, sign and return to the school

Staff Information Systems 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 Child Protection Coordinator.

I will ensure that any electronic communications with pupils are compatible with my professional role.

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.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …… Capitals: …… Date: ……..…

Accepted for school: …….. Capitals: ……..…….