Woodlands Community Primary School

E-safety Policy

Ratified by Governors	draft
Date for Review	
Signed – Chair of Governors	
Signed – Headteacher	

Reviewed June 2016

This document is to be used with the issued guidance and associated materials as declared on the Wirral LA VLE

eSafety Policy

eSafety Policy

The school has appointed the Head Teacher as the eSafety co-ordinator.
Our eSafety Policy has been written by the school.
It has been agreed by the senior management team.

The eSafety Policy will be reviewed annually. This policy will next be reviewed in **December 2017**

Why is Internet use important?

Why Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the curriculum and a necessary tool for staff and pupils.
- The school Internet access is provided by EXA networks 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.
- Pupils will be educated in the effective use of the Internet
- Pupils will be shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate Internet content

- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector.

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 students world-wide
- Access to experts in many fields for students 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 student use and includes filtering appropriate to the age of students
- Students 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 students in on-line activities that will support learning outcomes planned for the students' age and maturity
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- A planned online safety curriculum is provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities Students / pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students / pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. NB. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- Students / pupils are helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school / academy.

Authorised Internet Access

- The school will maintain a current record of all staff and students who are granted Internet access
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource (See Appendices)
- Parents will be informed that students will be provided with supervised Internet access
- Parents will be asked to sign and return a consent form for student access on entry to the school
- Students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement

World Wide Web

- If staff or students discover unsuitable sites, the URL (address), time, content must be reported to IT Technician/ICT coordinator and recorded in the e-Safety log.
- School Safeguarding Officer will be notified to decide whether any further action is needed.
- School will ensure that the use of Internet derived materials by students and staff complies with copyright law
- Students should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy

Virtual/Online Learning Environment

- Students must sign an AUP explicitly for the VLE. see Appendices
- Parents sign & return student consent form for VLE.

Email

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system.
- If pupils have email accounts they 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.
- Staff to pupil email communication must only take place via a school email address or from within the learning platform and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Password Protection

- School issues passwords for access to computer systems.
- Staff & students are encouraged to change their passwords on a regular basis.
- Students must not disclose passwords to other students.
- Teachers must not share passwords with other students

Social Networking

Social networking and publishing on the school learning platform

- The school will manage access to learning and media sites, and consider how to educate pupils in their safe use e.g. use of passwords and usernames.
- The School will block/filter access to social networking sites and newsgroups unless a specific use is approved
- Pupils will learn about using appropriate language when communicating online
- All users will be advised never to give out personal details of any kind which may identify them, anybody else or their location.
- Pupils must not place personal photos on any social network space provided in the school learning platform.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others
- Pupils will know that some social networks sites have age restrictions and these must be adhered to .
- Pupils, parents and staff will be advised on the safe use of social network spaces
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Students should be advised not to place personal photos on any social network space

Filtering

- The school will work in partnership with EXA and its technical support partner to ensure filtering systems are as effective as possible using *SurfProtect® ,a cloud based solution* and support the Prevent Agenda.
- Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated
- There is a clear process in place to deal with requests for filtering changes .
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the Internet. Nb. additional duties for schools / academies under the Counter Terrorism and Securities Act 2015 which requires schools / academies to ensure that children are safe from terrorist and extremist material on the Internet. (see appendix for information on "appropriate filtering"). •
- The school has provided differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc)

Video Conferencing

- Videoconferencing should be led by the class teacher will be appropriately supervised for the pupils' age

USB memory sticks & other Portable Data Storage Devices

- Staff to consider what data should be stored on USB sticks/other data storage devices
- Sensitive data should be encrypted.

Digital Cameras

- Staff to use school cameras or tablets to photograph students.
- Staff must not use personal equipment to photograph students.
- Storage cards to be cleared when camera returned.

Storage of Photographs

- Photographs to be stored in secure area within school network.
- Photographs to remain on school premises when practicable –ie off site school trips –images only to be downloaded to school network.
- Photographs to be deleted when no longer required.
- Current LA policy is adhered to regarding photographing & publishing images of children

Mobile Phones & Other Hand Held/Communication devices

- Mobile phones & other hand held communication devices should not be used for personal use in the lesson or formal school time (students & staff).
- Sending of abusive or inappropriate messages is forbidden.
- Parents are requested not to take photos of children at school events.
- Taking photographs at any time without the subject's consent is prohibited (Appendix 4).
- Staff should not share personal telephone numbers with pupils and parents. (A school phone will be provided for staff where contact with pupils is required).

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out by the ICT leader and Safeguarding officer
- Mobile phones/ handheld communications devices/ gaming consoles will not be used for personal use during lessons or formal school time.
- The sending of abusive or inappropriate text messages is forbidden

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 Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Students' Images and Work

- Photographs that include students will be selected carefully and will be appropriate for the context.
- Students' full names will not be used anywhere on the Web site, VLE , social media feed or Blog, particularly in association with photographs
- Written permission from parents or carers will be obtained on entry to school before photographs of students are published on the school Web site, social media feed or VLE

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 technical support partner
- Also see the use of 'USB memory sticks and other portable storage devices' section.

Protecting Personal Data

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

Communications Policy

Introducing the E-safety policy to pupils

- Appropriate elements of the E-safety policy will be shared with pupils
- E-safety rules will be posted in all networked rooms.
- Pupils will be informed that network and Internet use will be monitored
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils

Staff and the E-safety policy

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

Enlisting parents' support

- Parents' and carers attention will be drawn to the School E-safety Policy in newsletters, the school brochure and on the school web site.
- Parents and carers will from time to time be provided with additional information on E-safety.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Parents and carers will be reminded that they must not publish any images or comments of performances and other community events on social network sites before and after each event.

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 EXA Networks can accept liability for the material accessed, or any consequences of Internet access.
The school will audit ICT use to establish if the eSafety policy is adequate and that the implementation of the eSafety policy is appropriate every 12 months

Handling eSafety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff, Safeguarding Officer or Headteacher
- 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

Students

- Rules for Internet access will be posted in the ICT classroom
- Students will be informed that Internet use will be monitored

Staff and Governors

- 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, the school brochure and on the school Web site

Visitors

- Visitors to school will be informed about the e-Safety policy at the reception desk
- Rules for visitors clearly displayed (i.e. use of mobile phone/camera/film equipment etc).

Staff AUP

Staff and Governor 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 eSafety 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 eSafety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with students are compatible with my professional role.
- I will promote e-Safety with students 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 email 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: …………………………………………

Printed: …………………………………………………
Date: ……………

Student AUP

eSafety Rules

All students use computer facilities including Internet access as an essential part of learning, as required by the New Curriculum. Both students and their parents/carers are asked to sign to show that the eSafety Rules have been understood and agreed.

Pupil: ***Class:***

Students' Agreement

- I have read and I understand the school eSafety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed: **Date:**

Parent's Consent for Web Publication and display of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent's Consent for Internet Access

I have read and understood the school eSafety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that students 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

Appendix A: KS 2 eSafety Rules

eSafety Rules

These E-safety Rules help to protect students and the school by describing acceptable computer use.

- ➢ I understand the school owns the computer network and learning platform and can set rules for its use to keep me safe.
- ➢ I will only use ICT systems in school, including the internet, email and digital pictures for school purposes.
- ➢ I will only log on with my own user name and password.
- ➢ I will not share my passwords with anyone.
- ➢ I will only use my school email address at school.
- ➢ I will make sure that all messages are responsible, respectful and sensible.
- ➢ I will be responsible for my behaviour when using the Internet/learning platform/ virtual learning environment. This includes resources and the language I use.
- ➢ I will use the forums on the school's learning platform for sharing information sensibly.
- ➢ I will not give out any personal information about myself or anyone else when using the internet.
- ➢ If I accidentally come across any material that makes me uncomfortable I will report it to a teacher.
- ➢ I will not download or install software.
- ➢ I will respect the privacy and ownership of others' work on-line at all times.
- ➢ I understand the school may watch my use of the school's computer systems and learning platform.
- ➢ I understand that I will only be allowed to use the school equipment and systems by following these rules.

Appendix B: Key Stage 1 eSafety rules

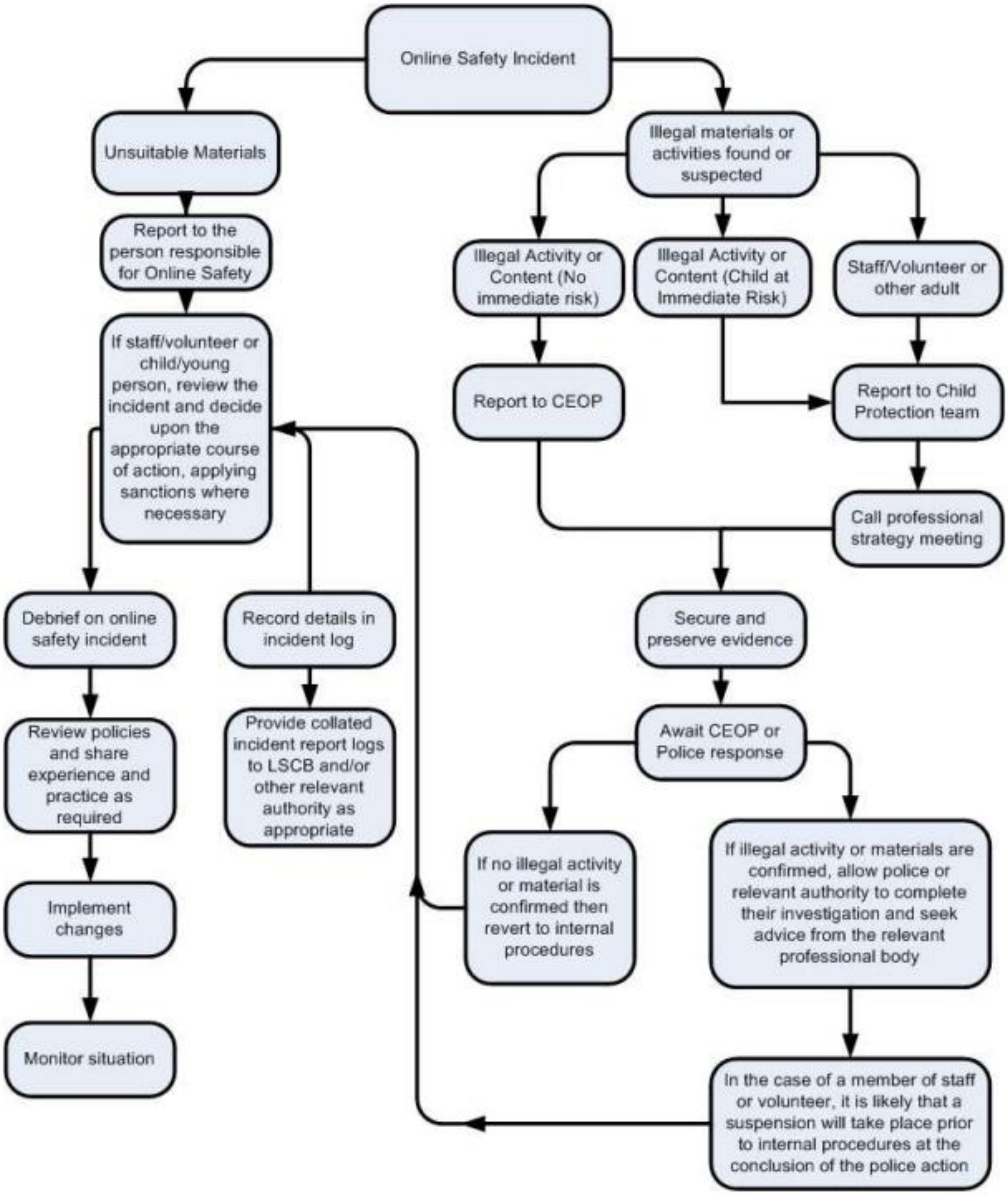
Think Before You Click

Use these rules to stay safe when using the Internet

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 the screen, I will always tell an adult

My Name	
My Signature	

Appendix C: Flowchart for responding to eSafety incidents


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Appendix D: eSafety Audit

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

Has the school an eSafety Policy that complies with CYPD guidance?	Y/N
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at:	
And for parents at:	
The designated Child Protection Teacher/Officer is:	
The eSafety Coordinator is:	
Has eSafety training been provided for both students and staff?	Y/N
Is the Think U Know training being considered?	Y/N
Do all staff sign an ICT Code of Conduct on appointment?	Y/N
Do parents sign and return an agreement that their child will comply with the School eSafety Rules?	Y/N
Have school eSafety Rules been set for students?	Y/N
Are these Rules displayed in all rooms with computers?	Y/N
Is Internet access provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access?	Y/N
Has the school filtering policy been approved by SMT?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SMT?	Y/N

Appendix E: Are you an eSafe school?

Do all your staff… ☐ Understand e-safety issues and risks? ☐ Receive regular training and updates? ☐ Know how to escalate an issue of concern? ☐ Know how to keep data safe and secure? ☐ Know how to protect themselves online? ☐ Know how to conduct themselves professionally online? ☐ Know about the updated e-safety guidance for QTS standard Q21: Health and well-being?	Does your school… ☐ Have a nominated e-safety co-ordinator? ☐ Audit its e-safety measures? ☐ Have a robust AUP? ☐ Use a **IWF approved content filtering and firewall** supplier for internet services? ☐ Include e-safety measures in Section 4b of your SEF? ☐ Keep an incident log and monitor your measures? ☐ Handle cyberbullying issues well? ☐ Raise awareness of the issues, e.g. through holding an assembly?
Do your learners… ☐ Understand what safe and responsible online behaviour means? ☐ Receive e-safety education at appropriate places across the curriculum? ☐ Get the opportunity to improve their digital literacy skills? ☐ Know the SMART rules? ☐ Know how to report any concerns they may have?	Do your parents and governors… ☐ Understand e-safety issues and risks? ☐ Understand their roles and responsibilities? ☐ Receive regular training and updates? ☐ Understand how to protect their children in the home?

This can be on the network

Appendix F: Website log

Request to **unblock** a website to be used by Staff and/or Pupils for educational purposes.

Website Address	Reason	Staff	Date	Agreed Y/N	H/T Sig

Request to **block** a website.

Website Address	Reason	Staff	Date		H/T Sig

Appendix G: eSafety Incident Log

Date	Staff	Incident	Action