CHURCHILL
SCHOOL

Acceptable Use of ICT Policy

Introduction

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 Behaviour, Bullying, Data Protection and Security.

Good Habits

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

- Responsible ICT use by all staff and students; 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 including the effective management of content filtering.
- National Education Network standards and specifications.

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 students who show a responsible and mature approach to its use. Our school has a duty to provide students with quality Internet access

Students 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 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 DFE

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

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
- 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
- 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 the office staff or Network Manager
- Senior Managers 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

Email

- Students may only use approved e-mail accounts on the school system
- Students must immediately tell a teacher if they receive offensive e-mail
- Students 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 will block access to social networking sites and newsgroups unless a specific use is approved

- Students will be advised never to give out personal details of any kind which may identify them or their location
- Students should be advised not to place personal photos on any social network space
- 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

Video Conferencing

- IP video conferencing 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 video conference call
- Video conferencing 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 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 Executive Principal, Headteacher or a designated member of the Senior Management Team 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, or any publications, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of students are published on the school Web site
- Work can only be published with the permission of the student 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 appropriate bodies

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.

The school cannot 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

Sanctions

Violation of E-Safety rules will result in sanctions being applied to students or staff involved.

Sanctions will be set dependent on the nature of the offence. The following are guidelines – each case being judged dependent on the type of infringements, the frequency and the status of the person/s involved.

How will infringements be handled?

Whenever a student or staff member infringes the E-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

The following are provided as exemplification only:

Students

Category A infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends

- Use of unauthorised instant messaging / social networking sites

[Possible Sanctions: referred to class teacher /E-Safety Coordinator]

Category B infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups
- Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it

[Possible Sanctions: referred to Class teacher/E-Safety Coordinator / removal of Internet access rights for a period / removal of phone until end of day / contact with parent]

Category C infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

[Possible Sanctions: referred to Class teacher / E-Safety Coordinator / Headteacher / removal of Internet and/or Learning Platform access rights for a period / contact with parents / removal of equipment]

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform relevant bodies as appropriate

Category D infringements

- Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988

- Bringing the school name into disrepute

[Possible Sanctions – Referred to Head Teacher / Contact with parents / possible exclusion / removal of equipment / refer to Community Police Officer]

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider

Staff

Category A infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or licence e.g. installing unlicensed software on network

[Sanction - referred to line manager / Headteacher. Warning given.]

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

[Sanction – Referred to Headteacher / Governors and follow school disciplinary procedures; report to Human resources, report to Police]

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Child Pornography found?

In the case of Child Pornography being found, the member of staff should be **immediately suspended** and the Police should be called.

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html

How will staff and students be informed of these procedures?

- They will be fully explained and included within the school's E-Safety / Acceptable Use Policy. All staff will be required to sign the school's E-Safety Policy acceptance form.
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate E-Safety / acceptable use form.
- The school's E-Safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
- Information on reporting abuse / bullying etc. will be made available by the school for pupils, staff and parents.
- Staff are issued with the 'What to do if..?' guide on E-Safety issues, (see Appendix E).

Communication of Policy

Students

- Rules for Internet access will be published in students Link Books, on the school's website, and the VLE
- Students will be informed that Internet use will be monitored

Staff

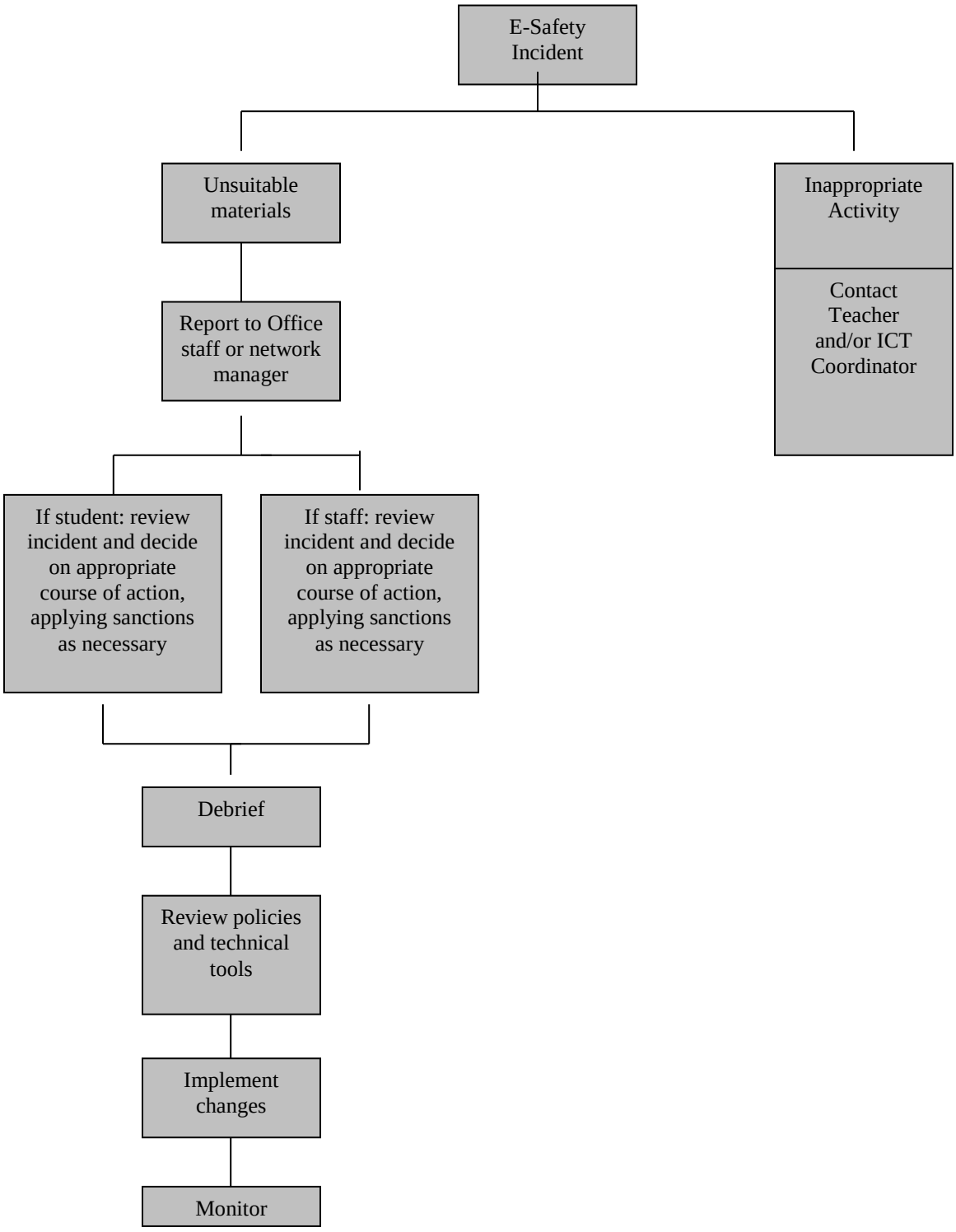
- All staff will be given the School E-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff who manage filtering systems or monitor ICT use will be supervised 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 published on the school Web site

Appendix A

Flowchart for responding to E-Safety incidents in school



Appendix B

E-Safety Rules

These E-Safety Rules help to protect students 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 will 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

E-Safety Audit – Secondary Schools

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/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 E-Safety Coordinator is:	
Has E-Safety 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 E-Safety Rules?	Y/N
Have school E-Safety 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 D

E-Safety Policy - Staff Handout
What to do if…..

An inappropriate website is accessed <u>unintentionally</u> in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the head teacher/e- safety officer and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered

An inappropriate website is accessed <u>intentionally</u> by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the head teacher and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the head teacher should then:
   - Remove the PC to a secure place.
   - Instigate an audit of all ICT equipment by the school's ICT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.
   - Identify the precise details of the material.
   - Take appropriate disciplinary action (contact Personnel/Human Resources).
   - Inform governors of the incident.
4. In an extreme case where the material is of an illegal nature:
   - Contact the local police or High Tech Crime Unit and follow their advice.
   - If requested, remove the PC to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including E-Safety anti-bullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence.
4. Inform the sender's e-mail service provider.
5. Notify parents of the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at www.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement of police and social services.

All of the above incidents must be reported immediately to the head teacher and E-Safety officer.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology:

they must be able to do this without fear.

Review

This policy will be reviewed in line with the school's policy review programme.

Author	**Date**	**Frequency of Review**
Georgina Ellis	Autumn Term 2017	Three Yearly
Adopted by the Governing Body Date: Signed	**Reviewed** Date: Signed	**Reviewed** Date: Signed