



E-SAFETY POLICY

FEBRUARY 2017

Copperfield Academy
E-Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

It is the responsibility of all persons connected with the school to be vigilant in reporting any e-safety concerns to the E-Safety Coordinator or the Safe Guarding Lead.

E-Safety throughout the school

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 the e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the EIS including the effective management of Web filtering.
- National Education Network standards and specifications.

The Policy is available for staff at: www.copperfield.kent.sch.uk

And for parents at: School Office or www.copperfield.kent.sch.uk

The Designated Child Protection Coordinator is: Gemma Clark

The e-Safety Governor is: Tony Moffatt

1. WRITING AND REVIEWING THE E-SAFETY POLICY

The e-Safety Policy is part of the School Development Plan and relates to other policies

including those for ICT, bullying and for child protection. The school has appointed the

Headteacher as the e-Safety Coordinator.

- Our e-Safety Policy has been written by the school, building on the Kent e-Safety Policy and government guidance. It has been agreed by senior leadership and approved by governors.

- The e-Safety Policy was revised by Mrs Sowden-Mehta

TEACHING AND LEARNING

2.1 Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.2 Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include 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 in research, including the skills of knowledge location, retrieval and evaluation. Refer to appendix 3 – Teaching, Learning and the Internet

2.3 Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and 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 in KS1 and KS2 will be taught about e-Safety using CEOPs guidance and schemes of work. Pupils will be taught that the following are not permitted within school and the community; displaying offensive messages or pictures, using obscene language, harassing, insulting or attacking others (whether on or off school premises or within/outside of normal school hours), damaging computers, computer systems or computer networks, violation copyright laws, using others people's logons/passwords, trespassing in others' folders, work or files, intentionally wasting limited resources. Through the CEOPs scheme, pupils are also taught the importance of not involving themselves in any of the above actions in or outside of school.
- The school will run the nationally recognised 'Think U Know' e-Safety and then use the guidance and material to support e-Safety teaching and learning within school.
- Pupils should be directed to specific websites checked by their teacher and use a child friendly safe search when possible e.g. www.askkids.com or <http://kids.yahoo.com>

2.4 E-Safety and portable equipment

This section covers all portable equipment whether owned by the school or by other persons and brought onto school grounds. Section 2 of the e-Safety Policy can be read with reference to portable equipment.

The school provides portable ICT equipment such as laptop computers, word processors, digital microscopes, and digital cameras to enhance the children's education and to allow staff to make efficient use of such equipment to enhance their own professional activities.

- No portable equipment or devices will be used to harm or embarrass another person.
- No portable equipment or devices will be used to bully or intimidate another person.
- Equipment such as laptop computers are encouraged to be taken offsite for use by staff in accordance with the ICT Code of Conduct for Staff. Staff are required to sign a disclaimer accepting full responsibility for the equipment in their care, and that the equipment is fully insured from the moment it leaves the school premises.
- No files should be transported off the school site on a memory stick, laptop or similar that contain any personal information about a pupil or staff including a pupil or staff's full name.
- All files leaving the school site should be encrypted and should only be accessible using a 'strong' password. A strong password:
 - Needn't be a word at all. It can be a combination of letters, numbers and keyboard symbols.
 - Is at least seven characters long. Longer passwords are harder to guess or break.
 - Does not contain your user name, real name, or company name.
 - Contains a mix of upper and lower case letters, numbers and keyboard symbols (i.e. ` ~ ! @ # \$ % ^ & * () _ + - = { } | [] \ : " ; ' < > ? , . /)
 - Is changed regularly.

2.5 Managing Internet Access

2.5.1 Information system security

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

2.5.2 The School's Learning Platform

- Pupils and staff should only access the platform through their own logons.
- Use of the learning platform by staff and pupils will indicated automatic agreement to the schools e-safety policy including the e-safety rules and the ICT Code of Conduct for Staff.

- It is explicitly forbidden for staff or pupils to upload into any area, material that could be considered to be offensive, racist or sexist.

2.5.3 E-mail and messaging including the use of these facilities on the Learning Platform

- 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 written permission from their parents and teacher.
- E-mail sent to an external organisation 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.
- Message content should not cause offense or be likely to cause offense.
- Attachments sent to pupils should not be opened unless a staff member gives permission.
- Pupils should be taught to scan attachments before opening.
- Any incidents involving inappropriate use of e-mail should be dealt with by the class teacher in conjunction with the e-Safety Coordinator. Parents should be informed.
- Pupils should be reminded to write polite, friendly non-offensive messages and Emails.

2.5.4 Published content on the school website (Learning Platform)

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

2.5.5 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. Staff should consider using group photographs rather than full-face photos of individual children.

- Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
- All forums, wikis and other 'resources ' on the learning platform should only be viewed by the persons they related to, e.g. a class or key stage. They should never be made public. This includes newsletters. Nb – by making a resource public, it will become discoverable on the internet through search engines. The remove the link form the search engine may take a matter of months.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school learning platform.
- Work can only be published with the permission of the pupil and parents/carers.
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

2.5.6 Managing filtering

- The school will work with the Trust, DfES and EIS to ensure systems to protect pupils are reviewed and improved.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective, and reasonable.
- If staff or pupils come across unsuitable on-line materials an online incident record should be made and reported to the e-Safety Coordinator.

2.5.8 Internet use at home

- Parents and Carers will be advised to contact their own Internet Service Providers to explore home filtering and child controls.
- Parents are advised not allow their child unsupervised access to the internet.
- Parents should be advised to visit the e-Safety section of the school website for further information on e-Safety at home.

2.6 Managing videoconferencing

- 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.

2.7 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.
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The use by pupils of cameras in mobile phones will be kept under review.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location. A member of school staff should be present at all times when these are in use. Staff will use the school phone system where contact with pupils is required or where mobile phones are used to capture photographs of pupils.

2.8 Protecting personal data & Data Transfer

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Staff are responsible for keeping sensitive pupil data secure when taken off the school site.
- Encrypted USB memory sticks should be used to transfer files between home and school.
- Staff are expected to check files brought into school are free from viruses.

3. POLICY DECISIONS

3.1 Authorising Internet access

- All staff must read and sign the ICT Code of Conduct for Staff before using any school ICT resource.

- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form for use of the internet in school.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

3.2 Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the Academy nor KCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

3.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with initially by the E-Safety Coordinator.
- All e-Safety incidents will be recorded in the format shown in Appendix 1. This is known as the 'E- Safety Incident Record.
- A copy of the E-Safety Incident Record will be sent to the head teacher, and the Child Officer (if this is not the same person). One copy will be stored in the pupil or staffs file. One copy will be kept by the e-Safety Coordinator.
- Any complaint about staff misuse must be referred to the head teacher.
- 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 may be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

When handling complaints about the way the school has dealt with an e-Safety incident, all complaints will be dealt with in accordance to the school complaint procedure/policy.

4. COMMUNICATIONS POLICY

4.1 Introducing the e-safety policy to pupils

- E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly. See appendix 2 – E-Safety Rules
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- e-Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.

4.2 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 are required to sign the ICT Code of Conduct for Staff.
- CPD meeting will be arranged to raise the awareness of e-Safety.
- New staff, as part of their induction pack, will be given an up-to-date copy of the e Safety policy.

4.3 Enlisting parents' support

- Parents and carers attention will be drawn to the School e-Safety Policy in newsletters and by sending out e-safety leaflets.
- The school will maintain a list of e-safety resources for parents/carers.
- All parents will be given a copy of the Appropriate Use Policy which they will need to read with their children, and it will need to be signed by both parties and returned to school.

4.4 Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.

Appendix 1
E-Safety Report Form

E-Safety incident	Date:		Time:		
Name of member of staff (discovering the incident)					
Child(ren) involved. (Or other adults if no children)					
Nature of incident	Accidental access to inappropriate material.	Intentional access to inappropriate material.	Cyber Bullying	Grooming	Other
Details					
The events occurred					
Does the event warrant direct Policy involvement? (Yes if...)					

Head Teacher/ Deputy headteacher					
(Staff)	Personnel Contact made with	Recommended action	Action applied	C of Gov	
Other					
Children	Contacted Person	Date		Time	
	Interviews parents/ carers	(append notes of interview)			
File four copies	Top Copy to HT	Second copy to Child Protection Officer	Third copy child's file	Personnel file	KCC

Appendix 2 – E-Safety Rules

- I will always use what I have learned about e-safety to keep myself safe and will tell a teacher if something makes me worried or unhappy. When sending a message or email, I will not give my home address or phone number, or arrange to meet someone.
- I will only use school ICT equipment for my school work and not to upset or bully other people or create a bad impression of my school.
- I will take responsibility for my own use of all ICT equipment and will use it safely, responsibly and legally e.g.
 - I will not use a personal email account in school
 - I will not open any email attachments without checking with an adult
 - I will make sure that my work does not break copyright
- I will not go on any unsuitable or illegal web sites on purpose. If I go on any by mistake I will tell a teacher straight away
- Any work I display on the learning platform will be work that I know I would want my family and friends to see.
- I will tell a teacher if I can see a website that is inappropriate or receive any unwanted emails or messages (such as spam).
- I will look after school ICT equipment and report any damage to a teacher straight away.
- I will only use the usernames and passwords I have been given and I will keep them secret (including learning platform usernames and passwords).
- I will use the learning platform to transfer files between home and school. I will not use a flash drive (USB memory stick) in school.
- I will save only school work on the school network and will check with my teacher before printing.
- I will log off or shut down a computer when I have finished using it.

I also understand that:

- **All of my work and internet activity on school ICT equipment and learning platform can be monitored and that there are consequences if I do not use the equipment sensibly, safely and responsibly.**

All pupils need to use computer facilities including Internet access as an essential part of learning; as required by the National Curriculum.

- **It is good practice for these rules to be followed at home as well as in school.**