Coppermill Primary School

e-Safety Policy

Ratified by the C&A Committee on: 21 January 2015

To be reviewed: Every 2 years

Next review: Spring 2017

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Coppermill with respect to the use of ICT-based technologies
- Safeguard and protect the children and staff of Coppermill
- Set clear expectations of behaviour and codes of practice relevant to responsible use of the internet for educational, personal or recreational use
- Have clear structures to deal with online incidences such as cyberbullying

The school aims to/for:

1. A secure school network

This school:

- Has educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network
- Ensures network health through use of Sophos anti-virus software (from LGfL) etc. and network set-up so staff and pupils cannot download executable files
- Ensures all staff and students have signed an acceptable use agreement form (Appendices 1 &2) and understands that they must report any concerns

2. Monitoring school network usage

This school:

- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access
- In conjunction with its technical contractors, the school monitors internet use as well as files saved on the system and deals with any known inappropriate content or behaviour

3. Its internet safety curriculum

This school:

- Teaches the basics of e-safety, through Zip it, Block it Flag it
- Uses a progressive e-safety and digital literacy education programme as part of the computing curriculum
- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas

4. Staff and parent training

This school:

- Trains staff at least once a year on up-to-date issues regarding internet safety and how to teach internet safety in the classroom
- Trains staff on dealing with e-safety issues appropriately
- Offers training to parents at least once-a-year as well as providing pamphlets and links to websites such as www.thinkuknow.co.uk

Responsibilities

The **Headteacher** takes overall responsibility for e-safety provision and for data and data security (SIRO). They are aware of procedures to be followed in the event of a serious e-safety incident.

The **Computing Coordinator** ensures that e-safety education is embedded across the curriculum, liaises with school ICT technical staff, communicates regularly with SLT to discuss current issues, review incident logs and filtering, and ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident. The **Computing Coordinator** will also report to the governors, with updates on all computing and e-safety issues at least once a year.

The **Network Technician** reports any e-safety related issues that arise to the Computing Coordinator and ensures the security of the school ICT system. They ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices.

The **School Business Manager** ensures that all data held on pupils on the school office machines have appropriate access controls in place.

Teachers supervise and guide pupils carefully when engaged in learning activities involving online technology in order to reduce risks (including, extra-curricular and extended school activities) and teach e-safety.

Handling E-safety Issues and complaints

The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

If an e-safety issue occurs it will be investigated. If sanctions are required, they may be in the form of:

- interview/counselling by Teacher / Computing Coordinator / Headteacher
- informing parents or carers
- removal of Internet or computer access for a period
- referral to LA / Police

The Computing Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher. Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA safeguarding procedures.

Data Security

We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services /

Family Services, Health, Welfare and Social Services. This specifies using encrypted files to send data via email and use encrypted USB's if data is being transferred physically.

School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.

Equipment and Digital Content

Mobile phones:

The recording, taking and sharing of images, video and audio on any mobile phone or personal camera (or any other personal device) is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

Student mobile phones which are brought into school must be turned off (not placed on silent) and given in to the office at the beginning of the day.

Digital images and video:

In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the admissions process when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs.

Appendices:

1. Acceptable Use Agreement (Staff)
2. Acceptable Use Agreement (Pupils)

APPENDIX 1

COPPERMILL PRIMARY SCHOOL

Edward Road
Walthamstow
E17 6PB

Telephone: (020) 8520 6267
Facsimile: (020) 8520 9755

Headteacher:
Mrs Figen Bektaşoğlu

Acting Deputy Headteacher:
Miss Karlie Walsh

Acceptable Use Agreement: Coppermill Staff

Agreement/e-Safety

- I will only use ICT in school for school purposes
- I will only use my school e-mail address when e-mailing
- I will open e-mail attachments from people I know
- I will not share my ICT passwords
- I will make sure that all ICT contact is responsible
- I know that my use can be checked and I will be contacted if a member of school staff is concerned about e-safety
- I will not take photos or videos of children on my phone

I have read the attached document and I agree to follow the e-safety rules and to support the safe use of ICT at Coppermill Primary School

Name……

Position……

Date……

APPENDIX 2

COPPERMILL PRIMARY SCHOOL

Edward Road
Walthamstow
E17 6PB

Telephone: 020 8520 6267
Facsimile: 020 8520 9755

Headteacher:
Mrs Figen Bektaşoğlu

Acting Deputy Headteacher:
Miss Karlie Walsh

Dear Parent/Carer

ICT including the internet, e-mail and mobile technologies have become an important part of learning in our school.

We expect all children to be safe and responsible when using any ICT.

Yours faithfully

Mrs Figen Bektaşoğlu
Headteacher

✂.....

ICT and e-safety

We have discussed the attached document and my child will agree to follow the e-safety rules and to support the safe use of ICT at Coppermill Primary School

Name:.....

Class:.....

Parent/Carer signature .....

Date:.....

Acceptable Use Agreement: Coppermill Pupils

Agreement/e-Safety

- I will only use ICT in school for school purposes
- I will only use my class e-mail address or my own school e-mail address when e-mailing
- I will only open e-mail attachments from people I know, or who my teacher has approved
- I will not tell other people my ICT passwords
- I will only open / delete my own files
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my e-safety