COPTHORNE PRIMARY SCHOOL

E-SAFETY POLICY

Date of issue	Review date	Date ratified by Governing Body
30th November 2017	November 2018	29th November 2017

	Print name	Signature	Date
Head Teacher	Mrs C Shepherd		
On behalf of Governing Body	Mrs N Hussain		

Copthorne Primary School

E-Safety Policy

Last reviewed: November 2017
To be reviewed: Annually
Written by: Computing Coordinator. Reviewed by SLT and school governors.

Rationale for Policy

At Copthorne Primary School we want to keep all children safe when using ICT. This includes the use of PC equipment and mobile devices such as Ipods, Ipads and Kindles. We want to teach children the correct procedures to follow if they come across something that they should not see or upsets them when working with ICT.
The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, improve Literacy and communication skills, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times.

However, the use of these new technologies can put young people at risk both inside and outside of school. Some of these dangers may include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/Internet games
- Potential for excessive use which may impact upon the social and emotional development and learning of the young person
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- The sharing/distribution of personal images without an individual's consent or knowledge

As with all of these risks, it is impossible to eliminate these completely. It is therefore essential, through good educational provision to build pupils' awareness of the risks to which they may be exposed, so that they have the confidence and understanding to seek advice and to deal with any risks in an appropriate manner.

The E-Safeguarding Committee

Our school has an E-Safeguarding committee which includes the following members:

Mrs C. Shepherd (Head, Child Protection Named Person)
Mrs F. Whalley (Early Years Coordinator and Designated Safeguarding Lead))
Mr J Darr (Computing Coordinator)
Mrs Zenab Bibi (Governor with responsibility for E Safeguarding)

Our school ICT technician is Nikio Bob-Manuel. The committee will consult him regarding any technical issues related to the safeguarding and security of data.

The E-Safeguarding committee will meet twice a year to discuss and review policies and any E-Safety incidents recorded within the E-Safety log. The committee will also discuss and review the progress being made against the school's E-Safeguarding action plan. Meeting minutes will be recorded and filed within the Coordinator's E-Safeguarding files.

Monitoring the impact of the policy

The school will monitor the impact of the policy using:

- Logs of reported E-Safety incidents
- Smooth wall monitoring of network activity
- Discussions at children's groups i.e. digital leaders
- Monitoring planning and evidence of work
- Parental E-Safeguarding data which is gathered annually and through parent feedback at E-Safety parents' meetings.

Information gained from this monitoring will be used to develop staff training, parent meetings, planning and teaching.

Roles and responsibilities:

Governors:

Governors are responsible for the approval of the E-Safeguarding policy and for the reviewing the effectiveness of the policy. This will be carried out at E-Safeguarding Committee meetings. The Governor responsible for E-Safeguarding is Zenab Bibi.

The role of the Governor will include:

- Attending E-Safeguarding committee meetings
- Monitoring of the E-Safety logs
- Reporting/Updating the Governing body at Governors' meetings

Head Teacher and Leadership Team:

The role of the Head and Leadership team includes:

- The Head Teacher is responsible for ensuring the safety (including E-Safety) of members of the school community, though the day to day responsibility for E-Safety will be delegated to the E-Safety Coordinator: Mr Jabran Darr
- The Head/Leadership team are responsible for ensuring that the E-Safety Coordinator and other staff receive suitable CPD to enable them to carry out their duties and to train other colleagues as appropriate
- The Head/E-Safety Coordinator are aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff. This is detailed within the Safeguarding and child protection policy.
- The Head/E-Safety Coordinator are also aware of 'Actions upon discovering inappropriate or illegal material' guidance from Bradford Innovation Centre team.

E-Safety Coordinator:

The role of the E-Safety Coordinator includes:

- The day to day responsibility for E-Safeguarding issues. The Coordinator has a leading role in establishing and reviewing the school's E-Safeguarding policy.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place
- Receiving and reporting reports of E-Safety incidents and recording all incidents in the E-Safety log
- Ensuring that all incidents are dealt with according to the school behaviour policy and that the Head, Class Teacher, Parents and other parties are informed where appropriate
- Coordinating the E-Safety Committee meetings
- Monitoring and reviewing the E-Safety teaching and learning taking place across the school
- Monitoring and reviewing the weekly Smoothwall filtering reports that are received via e-mail on a weekly basis

Technician

The school technician ensures:

- That the school's ICT infrastructures are secure and not open to misuse or malicious attack
- That she keeps up to date with E-Safety technical information and updates the E-Safety Coordinator as relevant
- That monitoring software and antivirus software is implemented and updated

Teaching and support staff

Teaching and support staff will:

- Keep an up to date awareness of E-safety matters and the current E-Safety policy through staff meetings and training sessions
- Read, understand and sign an agreement to use ICT equipment within school acceptably, in accordance with the E-safety/ICT policies.
- Understand the process for reporting E-Safety incidents within the school including recording the incident in the E-Safety log
- Report any suspicious misuse or problems to the E-Safety Coordinator for investigation
- Ensure that all digital communications with pupils should be professional and only carried out on official school systems
- Ensure that E-Safety issues are embedded in all aspects of the curriculum
- Ensure that E-Safety lessons are planned and taught every half term and that the lessons are age appropriate/reflect the needs of the age group.
- Ensure that pupils understand and follow the schools E-safety rules. Training should be provided on these policies at the beginning of each new academic year and for any new starters who join at a later stage
- Ensure that they are aware of the E-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regards to these devices
- Ensure that confidential files are saved in an encrypted file and that the password for this file remains confidential

- Ensure that at the end of the academic year photographs are deleted or, where applicable, stored in an agreed location for school use. At the end of Year 6 all photographs of pupils in that cohort are to be deleted

Named person(s) for child protection

The named persons responsible for child protection are trained in E-safety issues and are aware of the potential for serious child protection issues that may arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate contact with adults/strangers
- Potential incidents of grooming
- Cyber-bullying

Pupils

Pupils are encouraged through E-Safety/PSHE lessons to share any E-Safety concerns with a trusted adult. ICT systems and equipment in accordance with the E-Safety rules. They are briefed annually on the content of these rules which they are then asked to sign. Signature forms require parental signatures as well. Forms are collected and stored within the E-Safety files.
Pupils are encouraged through E-Safety/PSHE lessons to share any E-Safety concerns with a trusted adult.

Parents/Carers

The school will take every opportunity to help parents/carers to understand E-Safety issues. We will raise awareness of the key issues in the following ways:

- Parent/Carer assemblies on e-safety delivered by the children in each year group.
- E-safety rules are included in our school prospectus. Parents are asked to discuss these with their child and are invited to sign the forms to say they have done so.
- Information about E-Safety and parental resources are available on the school website.
- Parents' views are sought annually in the E-Safety questionnaire.
- Information is also shared via letters and newsletters.

Pupil Education

The education of pupils in E-Safety is a crucial part of the school's E-Safety provision. Children need the help and support of the school to recognise and avoid E-Safety risks and to build their awareness of how to keep themselves safe. E-Safety education will be provided in the following ways:

- A planned E-Safety programme is delivered through ICT and PSHE in the form of The Innovation Centre Bradford Scheme of Work and The Spiral Curriculum
- Pupils are taught in all lessons to be aware of the content that they access on line and learn how to validate the accuracy of the information they find
- Rules for acceptable use are shared at the beginning of each academic year and with any new starters as they join school
- Pupils are taught how to search for information safely and safe search engines are used by Teaching Staff

- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet
- Copyright free images and audio sources are shared with the children.
- Pupils are made aware of the process to follow if they see anything online which they find upsetting or which is unsuitable for children
- Pupils know that any events of Cyber-bullying are taken seriously by the school and they understand the importance of sharing their concerns with a trusted adult

Prevent Agenda

Many extremist groups who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences.

- Pupils and staff should be warned of the risks of becoming involved in extremist groups and informed that accessing such websites is against school policies.
- The school ensures that adequate filtering is in place and review filtering in response to any incident where a pupil or staff member accesses websites advocating violent extremism.
- All incidents will be dealt with as a breach of the acceptable use policies and the school's behaviour and staff disciplinary procedures should be used as appropriate.
- The E-safety Coordinator and a named person for child protection will record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the school and whether current school procedures are robust enough to deal with the issue.
- If there is evidence that the pupil is becoming deeply enmeshed in the extremist narrative, schools should seek advice from the Local Prevent Coordinator on accessing programmes that prevent radicalisation. Where there is evidence that their parents are involved in advocating extremist violence, referrals should be made to Michael Churley on 01274 432816.

Staff Education

It is essential that all staff receive regular E-Safeguarding training and that they understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Annual E-Safety staff training to be delivered by the E-Safety Coordinator or a member of the Bradford Innovation Centre team.
- An annual audit of staff E-Safety training will be completed and any training needs identified will be used to plan staff training.
- The annual questionnaire results from parents and pupils will highlight issues relevant to the school and particular year groups. These will be used to direct training
- Planning and E-Safety work will be monitored regularly and will be used to direct training
- Staff will receive a copy of the E-Safeguarding policy annually and sign to agree to acceptable use of ICT equipment.
- Both policies are included in the staff handbook for all members of staff.

Internet provision

The school Internet is provided by the Bradford Learning Network, a DFE accredited educational Internet service provider. All sites are filtered using the Smoothwall filtering system which generates reports on user activity. This will be monitored by the ICT technician.

Managing ICT systems and access

Access to ICT systems is managed by the Technician and ICT/E-Safety Coordinator. All children at the school receive logins and accounts for; the school blog, Mathletics, Education City and other educational software licenced to school. These accounts are managed through administrator privileges which are only known to the Technician and Coordinator. Accounts are created for new starters at the beginning of the academic year and then for new starters that join during the school year. Accounts are deleted annually for any leavers including those children in year 6.

Adult accounts and passwords are also created in the same way. Adults are given accounts for school systems, e-mail and the school blog. Accounts are created and deleted for new starters and leavers when required.

Passwords

All users (staff and pupils) have the responsibility for the security of their user name and password and must not allow other users to access the systems using their log on details (as per Acceptable Use Policies). Any concerns about sharing passwords or log on details must be reported to the E-Safety Coordinator.

- Passwords for new users and replacement (passwords for existing users can be allocated by the ICT technician).
- Members of staff are made aware of the school's password rules through induction and the E-Safeguarding policy.
- Pupils are made aware of the school's password rules through Computing/E-Safety lessons and through the pupil E-safety rules.
- Old user names and accounts are deleted annually.

All pupils have their own individual log in and password for accessing the school's ICT systems and the school blog.

Personal Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

All staff must ensure the:

- Safe keeping of personal data at all times to minimise the risk of its loss or use
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged off" at the end of any session in which they are using personal data

- Ensure that memory sticks where used are password protected
- Ensure that information is saved on secure drives which can only be accessed by password

Use of digital and video images (photographic and video)

- Staff should inform and educate pupils about the risk associated with the taking, use, sharing, publication and distribution of images.
- Staff are allowed to take digital/video images to support educational aims. These images should only be taken on school equipment; personal equipment should not be used for these purposes. All classes now have a class camera for this purpose.
- Parental permission to use photographs on the school website, blog and in the press must be given. Permission slips are stored in the children's files and records are given to each class teacher.
- Photographs will be published without names on the blog, website and in the press. In incidences where names are required (some newspapers) parental permission will be sought.
- Teaching staff are responsible for storing photographs and images safely and securely. Staff will also ensure that images are deleted annually/once the child has left the school.

Management of assets

All ICT assets are recorded on an inventory spreadsheet. Assets that are damaged or surplus to requirements have data removed by the Technician before being collected and destroyed by a reputable company. Certificates are received and filed where this has taken place.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT. However there may be incidents when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

If apparent or actual misuse appears to involve illegal activity such as:

- Child sexual abuse images
- Adult material which breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

Then staff should turn off the monitor/screen of the device, ensure that the device is not shut down as evidence could be erased, and report the matter immediately to the Head/E-Safety Coordinator.

If misuse has taken place which is not illegal it is important that any incidents are dealt with in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

Cyber bullying

Cyber bullying is the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. Examples of electronic communication are social networking web sites and apps, texting, use of other mobile or tablet apps, email or online software. Pupils are taught about cyber bullying through E-Safety and PSHE lessons. Pupils are encouraged to share concerns of cyber bullying with a trusted adult. The adults in school will support the child by:

- Collecting evidence of the bullying taking place by recording the date, time and where possible screen captures
- Advising the child not to forward on messages to other people as this will continue the bullying
- Advising the child not to reply to the messages

Full details of how the school manages incidences of bullying can be found in our Anti-Bullying policy. The school may report serious cyber bullying incidents to the Police.

Social Media

Copthorne Primary School uses Social Media in the following ways:

- A text to Parents system which is managed by the school office. This is used as a reminder service for parents.
- As part of our school website pupils have a blog they can contribute to. All comments and posts are moderated by teachers before they are published. Pupils know that they must not share personal information on the blog or use it to communicate with people they do not know in real life.
- We upload children's work onto the Lendmeyourliteracy.co.uk site and this is managed by the writing coordinator and class teachers. Comments placed on the site are internally moderated by the site to check they are appropriate and children can only comment by logging in with an adult at home.
- All members of staff must keep their personal and professional lives separate on social media. Personal opinions should never be attributed to the school. The *school's* use of social media for professional purposes will be checked regularly by the E-Safety committee to ensure compliance with this policy.

Mobile devices

Staff

Staff must not use mobile phones at any time in front of or in view of the children other than the Head Teacher who may use mobile phones in front of children only to take photos for Twitter or other promotional activities for the school. During teaching time, while on playground duty and during meetings, mobile phones will be switched off or put on 'silent' or 'discreet' mode. When staff sign they acceptable use agreement they agree that they understand they should not use personal devices for photography in school. Only school cameras or devices are to be used.

Pupils

School does not allow children to bring mobile phones into school. As part of our e-safety scheme of work, pupils are taught about the dangers of using mobile phones, the fact that location services can say exactly where you are and how quickly children can post content online before thinking about the consequences.

School mobile devices

The school has iPads available for use with classes. All of the statements included in the e-safety rules for pupils apply to these mobile devices. Pupils know that they must not take pictures of other people without their permission. They are not allowed to download or install apps on any device. These devices are subject to the same levels of internet filtering as all the school computers accessed by children.

E-SAFETY

POLICY

APPENDICES

Appendix 1: Acceptable Use Policy/E-Safety rules Pupils

Dear Parent/ Carer,

ICT including the internet, email and mobile technologies are an important part of learning in our school. We expect all children to be safe and responsible when using any ICT equipment. Please read and discuss these e-safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like to discuss this further please contact the school.

E-safety rules

I will only use ICT in school for school purposes.

I will only use my class email address or my own school email address when emailing.

I will only open email attachments from people I know, or who my teacher has approved.

I will not tell other people my ICT passwords.

I will not take pictures of other people without their permission.

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 equipment and the internet can be checked and that my parent/ carer can be contacted if a member of school staff is concerned about my e-safety.

- -

Parent/Carer Signature

We have discussed this and _____ (child's name) agrees to follow the e-Safety rules and to support the safe use of ICT at Copthorne Primary School.

Child Signature _____

Parent/ Carer Signature: _____

Child’s class:_____ Pupil/Parent Agreement