Part of the Exceed Academies Trust
Together we Exceed

COPTHORNE PRIMARY SCHOOL

Online Safety Policy

Date of issue	Review date	Date ratified by Governing Body
October 2021	October 2022	October 2021

	Print name	Signature	Date
Head Teacher	Miss S Ngenda		
On behalf of Governing Body	Mr P Gerrard		

Rationale

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.

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

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.

Legislation and guidance
This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2021, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

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 Faye Pearson.

The role of the Governor will include:

- Attending E-Safeguarding committee meetings
- Monitoring of the Online 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 Online safety) of members of the school community, though the day to day responsibility for Online safety will be delegated to the Online safety Coordinator: Mr Jabran Darr
- The Head/Leadership team are responsible for ensuring that the Online 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/Online safety Coordinator are aware of the procedures to be followed in the event of a serious Online safety allegation being made against a member of staff. This is detailed within the Safeguarding and child protection policy.

- The Head/Online safety Coordinator are also aware of 'Actions upon discovering inappropriate or illegal material' guidance from Bradford Innovation Centre team.

Online Safety Coordinator:
The role of the Online 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 Online safety incident taking place
- Receiving and reporting reports of Online safety incidents and recording all incidents in the Online 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 Online safety Committee meetings
- Monitoring and reviewing the Online 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 Online safety technical information and updates the Online 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 Online safety matters and the current Online 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 Online safety/ICT policies.
- Understand the process for reporting Online safety incidents within the school including recording the incident in the Online safety log
- Report any suspicious misuse or problems to the Online safety Coordinator for investigation
- Ensure that all digital communications with pupils should be professional and only carried out on official school systems
- Ensure that Online safety issues are embedded in all aspects of the curriculum
- Ensure that Online 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 Online 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 Online 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
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- 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 Online 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 Online safety/PSHE lessons to share any Online safety concerns with a trusted adult. ICT systems and equipment in accordance with the Online 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 Online safety files.

Pupils are encouraged through Online safety/PSHE lessons to share any Online safety concerns with a trusted adult.

Parents/Carers

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

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

- Parent/Carer assemblies on Online safety delivered by the children in each year group.
- Online 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 Online safety and parental resources are available on the school website.
- Parents' views are sought annually in the Online safety questionnaire.
- Information is also shared via letters and newsletters.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

Educating pupils about online safety

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

- A planned Online safety programme is delivered through ICT and PSHE in the form of 'You Me PSHE'
- Pupils are taught in all lessons to be aware of the content that they access online 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

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

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 Online 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.

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or Class Dojo. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with children.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

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/Online 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 Online 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/Online safety lessons and through the pupil Online 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.

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
- Classes all have a Class Dojo page
- We upload children's work and notices to the school Twitter page
- 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 Online 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 Online 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 Online 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.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school’s terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from a member of the Virtue ICT support team.

How the school will respond to issues 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/Online 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. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

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:

- All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
- All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).
- An annual audit of staff Online 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 Online 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

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring the impact of the policy

The school will monitor the impact of the policy using:

- Logs of reported Online 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 Online safety parents’ meetings.

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

Reviewing the policy

This policy will be reviewed every year by the E-Safeguarding Committee. At every review, the policy will be shared with the governing board.

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

Miss S Ngenda (Head of School, Designated safeguarding Lead)
Mr J Darr (Computing Coordinator)
Mrs F Pearson (Governor with responsibility for E Safeguarding)

Our school uses Vitue ICT technicians. The committee will consult them 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 Online safety incidents recorded within the Online 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.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: Internet Code of Conduct

Copthorne Primary School

Internet Code of Conduct for All Staff

Supervision

I will always supervise children when they are using the internet.

Giving out Personal Details

I will remind children not to give out personal information on the internet. I will never disclose confidential information about children on Social Media Sites such as Facebook or Twitter.

E-mail

I will only use school provided e-mail when communicating about work or with work colleagues.

I will keep my personal email for my personal life and will not use my school email as a login for Social Media Sites such as Facebook or Twitter.

Search Engines

I will only allow the children to use the search engines approved by school, such as Primary Safe Search. I will set a good example for children at all times and should I need to search the Internet when children are present, I will also use these sites.

Educational Sites

I will remind children to only use their own account and not allow family members to use their account when using educational sites eg: Mathletics, Purple Mash and Spellodrome.

Blogging and Social Media

When adding to blogging and Social Media Sites (such as Facebook or Twitter), I will not write or display anything that I think will target or upset other people. I will never discuss staff or pupils by name on Social Media Sites, as I understand that this may bring my professionalism into disrepute. I will remind the children of this each time we add to our school blog.

Meeting people through the Internet

I will ensure children in my care understand that not everyone they ‘meet’ on-line is who they say they are and that some people can pretend to be someone else.

E-Safety

I will remind the children that if they come across something that is rude, racist or upsetting that they should follow the steps below:

- Turn the computer screen off! Do not turn the PC off.
- Put your hand up and ask for a teacher to come straight over.
- **DO NOT** show other students what you have seen or discuss with them.
- Wait for someone to come over and help you.
- The adult will then tell you what to do next.
- The adult will report this to members of the ICT team.

Reliability and plagiarism of Information

I will remind the children to ask 'Is it true?' and to always check where the information has come from, if possible with another website.

I will follow advice regarding copyright and will not use resources that are copy protected in my lessons.

User Accounts/Central Storage

I will remind the children to only log onto the network as themselves and to never change or delete other people's work that is saved on the school network.

I will set a good example for the children and always log on to the computer as myself.

Signed: ______________________
Name: ______________________
Date: _____________________

Signature of Computing Co-ordinator: _______________________