The Coppice Primary School E-Safety and Cyberbullying Policy

‘The Internet and other technologies such as mobile phones and games consoles have become an integral part of children's and adults’ lives. ... It is therefore **vital** that children, parents and carers are aware of the way in which they use the Internet, understand the risks of going **online** and understand how to use the Internet safely and responsibly’.

Written by	Lucie Cooper
Approved by Trustees	March 2019
Date for Review	March 2022

E-safety and Cyberbullying Policy

1 School Vision:

'Happy, confident and successful learners that are well prepared for life'

2 Purpose:

2.1 The school recognises that technology plays an important and positive role in everyone's lives, both educationally and socially. This policy has been written to help all members of the school community understand both the benefits and the risks, and to equip children with the knowledge and skills to be able to use technology safely and responsibly. This policy reflects the school values and philosophy in relation to the teaching and learning of E-Safety. The policy should be read in conjunction with each year group's E-Safety curriculum planning and the Purple Mash Computing Scheme of Work.

2.2 This document is intended for:

1. All teaching and school management staff
2. All teaching assistants and pupil support staff
3. School governors
4. Parents
5. Inspection teams

2.3 Aims and objectives:

The aims of this policy are to ensure that:

- We safeguard the pupils in the real and virtual world.
- Pupils, staff and parents are educated to understand what cyberbullying is and what its consequences can be.
- Knowledge, policies and procedures are in place to prevent incidents of cyberbullying in school or within the school community.
- We have effective measures to deal effectively with cases of cyberbullying.
- We monitor the effectiveness of prevention measures.

3. Cyberbullying:

3.1 The Department for Education define cyberbullying as when: *one person, or a group of people, tries to threaten or embarrass someone else using a mobile phone or the internet.*

3.2 Mobile, Internet and wireless technologies have enabled millions of people to communicate and access information quickly and effectively. However, their popularity provides increasing opportunities for misuse through 'cyberbullying'. It's crucial that children use their mobiles and the Internet safely and positively, and that they are aware of the consequences of misuse. School staff, parents and pupils of The Coppice Primary School must work together to educate our children on e-safety in order to reduce incidents of cyberbullying and deal with it effectively as and when it does occur.

3.3 Unlike other forms of bullying, cyberbullying can occur anytime and anywhere where there is access to a mobile phone or an Internet-enabled device. Cyberbullies can communicate their messages to a wide audience with speed, and can often remain anonymous to their victim.

4. Types of cyberbullying:

- **'App' bullying:** The newest, and arguably most concerning form of bullying. Hundreds of new apps are developed and released every day. Many of these have communication functions, e.g. Whisper, Ask FM, Kik, Tumblr, Instagram and Snapchat. Some, such as Snapchat, are specifically designed so that conversations are fleeting and not permanently stored. Bullies can use this to send abusive messages which quickly become unprovable.

- **Online bullying:** sending abusive messages when they are using social networking sites/online chat functions / chatrooms. These may be typed messages (e.g. Facebook or Instagram) or, more recently, spoken messages via a microphone or headset. An increasing number of online games now offer chat functions. These can be PC-based games, or consoles with Internet functions, such as Xbox 360 or Xbox One, via Xbox Live.

- **Email bullying:** uses email to send bullying or threatening messages, often using a pseudonym email address or using someone else's name to pin the blame on them.

- **Bullying through instant messaging (IM)** is an Internet-based form of bullying where children and young people are sent unpleasant messages as they conduct real-time conversations online. This may be text or video based. (Skype, for example, offers both.)

- **Bullying via websites:** this includes creating personal websites and blogs in order to spread defamatory information about others.

- **Text message bullying**: sending texts that are threatening, abusive or cause discomfort.

- **Picture/video-clip bullying:** this can involve sharing embarrassing photos or videos of the victim or it can involve sending threatening or aggressive images/footage to the victim.

- **Phone call bullying:** this may consist of silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. Perpetrators often block their numbers or use a different phone so as to bully anonymously.

5. How do we tackle cyberbullying?

5.1 School staff, parents and pupils of The Coppice Primary School need to work together to prevent cyberbullying and to tackle it whenever it occurs. Although schools may not be able to control how children use technologies outside of the school, they recognise that children can only learn effectively if they feel happy and safe. Cyberbullying can have a massive negative impact on a child's emotional wellbeing and therefore it is very much a school concern.

5.2 At The Coppice Primary School, we take cyberbullying as seriously as any other form of bullying. Any incidents involving pupils will be addressed in accordance with our Anti-bullying and Behaviour policies (available to view on the school website).

8. Roles and Responsibilities:

8.1 Headteacher:

The Headteacher who is also the Designated Safeguarding Lead will take overall responsibility for the coordination and implementation of cyberbullying prevention and response strategies. The Head, in consultation with staff will:

- Ensure that all incidents of cyberbullying both inside and outside school are dealt with urgently and will be managed and/or escalated in line with the procedures set out in the school's Anti-bullying Policy, Behaviour Policy and Safeguarding and Child Protection Policy as soon as the school is made aware.
- Ensure that all policies relating to safeguarding, including cyberbullying are reviewed and updated regularly.
- Ensure that all staff know that they need to report any issues concerning cyberbullying to the Designated Safeguarding Lead.
- Ensure that parents/carers are informed and attention is drawn annually to the cyberbullying policy so that they are fully aware of the school's responsibility relating to safeguarding pupils and their welfare. The Cyberbullying Policy is available at all times on the school website.

8.2 Subject Leader:

- Ensure that all pupils are given clear guidance on the use of technology safely and positively both in school and beyond including how to manage their personal data and how to report abuse and bullying online.
- Provide annual training for parents/carers on online safety and the positive use of technology
- Provide annual training for staff on online safety
- Plan and deliver a curriculum on online safety in computing lessons which builds resilience in pupils to protect themselves and others online.
- Plan a curriculum and support staff in delivering a curriculum on online safety which builds resilience in pupils to protect themselves and others online.

8.3 The Classroom Teacher:

It remains the responsibility of each teacher to:

- Have sufficient knowledge to deal with cyberbullying in school and report more serious / prolonged incidences of cyberbullying to the Senior Designated Person for Safeguarding (SDP) and the ICT coordinator.
- To use the curriculum to teach pupils about e-safety. This includes the risks of new technologies, the consequences of their misuse (including legal implications), and how to use them safely.

8.4 The Technician:

- All Internet usage on the school site (by staff, pupils and visitors alike) is monitored and checked using Policy Central software.

- Onsite firewalls are continually updated and harmful sites blocked.
- Security systems are in place to prevent our internal server from unauthorised access.

9. Parents and Carers:

- Don't wait for something to happen before you act. Make sure your child understands how to use these technologies safely and knows about the risks and consequences of misusing them.
- Make sure your child knows what to do and who they can talk to if they or someone they know are being cyber bullied.
- Encourage your child to talk to you if they have any problems with cyberbullying. If they do have a problem, contact the school, the mobile network or the Internet Service Provider (ISP) to help you take action.
- Parental control software can place restrictions on email and website access.
- Visit **www.thinkuknow.co.uk** and **www.ceop.police.uk** for more information.
- Make sure you understand the consequences of misusing the Internet and how the actions of parents and carers online can cause distress to children.

10. Advice for pupils of The Coppice Primary School:

- Remember, bullying is not something to be ashamed of. It can be stopped and it can usually be traced but you need to speak out. Tell someone that you trust, such as a teacher, family member or call an advice line, such as ChildLine: 0800 1111. You can also visit websites such as **www.ceop.police.uk/safety-centre** for online help.

- If you are frightened or angry, try not to show that to your bully. Try to keep calm and talk to someone as soon as possible.

11. Cyberbullying of Coppice Staff:

11.1 Cyberbullying affects adults as well as children. Incidents of bullying or defamation of Coppice staff will be addressed immediately. In severe or persistent cases, this may include the school seeking legal advice.

12. Education Law:

12.1 The Education and Inspections Act 2006 (EIA 2006) outlines some legal powers which relate more directly to cyberbullying.

12.2 Head teachers have the power 'to such an extent as is reasonable' to regulate the conduct of pupils when they are off the school site.

12.3 The Act also provides a defence for staff in confiscating items such as mobile phones from pupils.

13. Civil and Criminal Law:

13.1 There is not a specific law which makes cyberbullying illegal but it can be considered a criminal offence under several different acts including Protection from Harassment Act (1997), Malicious Communications Act (1988), Communications Act (2003) Obscene Publications Act (1959) and Computer Misuse Act (1990).

13.2 Guidelines issued by the Crown Prosecution Service (CPS) in December 2012 explain how cases of cyberbullying will be assessed under current legislation. The 'CPS Guidelines' can be downloaded online.

Information taken from www.cybersmile.org

14. Anti-radicalisation measures: (see also 'Anti-radicalisation policy')

14.1 The Coppice Primary School is committed to safeguarding and promoting the welfare of all its pupils. We recognise that safeguarding against online radicalisation is no different from safeguarding against other forms of online abuse. E-safety is integrated into our computing lessons and across the curriculum, where children are accessing online resources. Children are taught about and encouraged to discuss the possible risks associated with speaking to people online. They are encouraged to share their worries with a responsible adult.

15. Equal Opportunities & Inclusion

15.1 We believe that all pupils, regardless of race, class or gender, should have the opportunity to develop their knowledge of E-Safety and Cyberbullying.

It is our goal to ensure this by:

- Ensuring all children follow the Computing Scheme of Work.
- Ensuring all children have the same access to E-safety lessons.
- Monitoring the children's ICT use to ensure equal access and fairness of distribution of ICT resources.
- Providing materials and software which are in no way class, gender or racially prejudiced or biased.
- Making children and parents aware of relevant websites that can be accessed outside of school to help develop knowledge of E-safety and Cyberbullying.

16. Further Advice for Coppice Families:

16.1 If you are having a problem with cyberbullying, it is natural to feel lots of emotions: confusion, fear, anger and embarrassment, amongst others. When you have these feelings, it is sometimes difficult to think straight and see what you need to do to seek help. The following advice is designed to help you deal with cyberbullying quickly and safely:

- **Screen capturing:**

Undoubtedly, the most useful thing to have when dealing with cyberbullying is evidence. Unfortunately, lots of apps now have 'anonymous' functions which means that unkind messages may disappear before you are able to get help from a trusted adult.

- **Laptop / PC screen capturing:**

If you come across cyberbullying of yourself or someone else, use the 'print screen' button to take a capture of the screen. (See diagram.)

When you have pressed the button, you can then open up Microsoft Office 'Word' (or 'Paint' if you do not have Office installed) and then use 'ctrl + v' to paste the screen capture. (Press and hold the ctrl button and then press v.)

If this does not work, you can always use a camera to take a photograph of the screen.

- **OS X (Mac) screen capturing:**

Press ‘shift + command + 3’ and this will take an instant screen snapshot that will automatically save to your desktop.

- **iPad / iPhone screen capturing:**

Find your ‘Sleep/Wake’ button (the one that turns your device on and off when you press and hold) and your ‘Home’ button (the circular button at the bottom with the little white square).

Push these two buttons simultaneously. Do not hold them down, just push and then release. You should hear a camera shutter and see a white flash on the screen. The screen capture will now be saved in your photos folder.

- **Screen capturing on other internet-enabled devices:**

There are many devices out there on which children may be accessing websites and online apps. If you do not know how to screen capture, it is well worth finding out. Googling ‘screen capture + device name’ will give you guidance on how to perform this task.

For example, ‘screenshot Samsung Galaxy Note’ or ‘screen capture HTC One’

- **Text/video messaging**

Never reply to abusive text or video messages. If the problem persists, your mobile service provider (e.g. O2, Orange, Vodafone) should have a number for you to ring for advice. They can also help you change the number, if needed. Visit your service provider website for details.

Don't delete messages from bullies. You don't have to read them, but keep them as evidence.

Text harassment is a crime. If the calls are simply annoying, tell an adult. If they are threatening or malicious, report them to the police, taking with you all the messages you've received.

- **Phone calls**

If you get an abusive or silent phone call, don't hang up immediately. Instead, put the phone down and walk away for a few minutes. Then hang up or turn your phone off. Once they realise they can't get you rattled, callers usually get bored and stop bothering you. If abusive, you could report it to your provider or if extreme and persistent to the police.

Always tell a trusted adult. Get them to support you and monitor what's going on.

Don't give out your phone number and never leave your phone lying around.

If you don’t recognise a caller, let it divert to voicemail instead of answering it. Don't leave your name on your voicemail greeting. You could get an adult to record your greeting. Their voice might stop the caller ringing again.

Almost all calls nowadays can be traced, even if the number is withheld.

If you receive calls that scare or trouble you, make a note of the times and dates and report them to the police. If your mobile can record calls, take the recording too.

- **Emails**

Never reply to unpleasant or unwanted emails; the sender wants a response so don't give them that satisfaction.

Keep the emails as evidence – do not delete! If the problem is persistent, you can show these emails to a trusted adult who will be able to help you.

Never reply to someone you don't know, even if there's an option to 'unsubscribe'. Replying simply confirms your email address as a real one.

- **Web bullying**

If you are being bullied because someone is writing about you on a blog or website, tell a trusted adult immediately or use 'Childline' to seek advice.

- **Chat rooms / Instant Messaging / Apps:**

Never give out your name, address, phone number, school name or password online. Use a nickname and NEVER give out photos of yourself.

Don't accept emails or open files from people you don't know.

Tell your parents or carers if you feel uncomfortable or worried about anything that happens when using chat rooms, instant messaging or a communication app.

17. Three steps to staying happy and safe:

1. Respect other people - online and off. Don't spread rumours about people or share their secrets, including their phone numbers, passwords and photos.
2. If someone insults you online or by phone, stay calm and get evidence.
3. 'Do as you would be done by.' Think how you would feel if you were bullied. You're responsible for your own behaviour – make sure you don't distress other people or cause them to be bullied by someone else.

18 Data Protection Statement:

The procedures and practice created by this policy have been reviewed in the light of our GDPR Data Protection Policy.

All data will be handled in accordance with the school's GDPR Data Protection Policy.

Name of policy	Content	Reason for policy	Who does it relate to?	Where is it stored?
E-Safety and Cyberbullying Policy.	This policy has been written to help all members of the school community to understand both the benefits and the risks, and to equip children with the knowledge and skills to be able to use technology safely and responsibly.	To educate staff, children and parents of the risks associated with technology and how to best equip children with the knowledge and skills to stay safe online.	All teaching and school management staff All teaching assistants and pupil support staff School governors Parents Inspection teams	School PDrive. School Website.

As such, our assessment is that this policy:

Has Few / No Data Compliance Requirements	Has A Moderate Level of Data Compliance Requirements	Has a High Level Of Data Compliance Requirements
	x	

This policy will be reviewed every three years.

Review Date by Trustees: March 2019

To be reviewed: March 2022