The Coppice Primary School

Online Safety Policy

‘Children have the right to enjoy childhood online, to access safe online spaces, and to benefit from all the opportunities that a connected world can bring to them, appropriate to their age and stage. As they grow older, it is crucial that they learn to balance the benefits offered by technology with a critical awareness of their own and other’s online behaviour and develop effective strategies for staying safe and making a positive contribution online’ (Education for a Connected World)

Written by	Val Juneman
Approved by Trustees	Nov 2023
Date for Review	Nov 2024

Online Safety Policy

1. School Vision:

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

2. Purpose:

- 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 Online Safety. The policy should be read in conjunction with the Schools Online Safety Curriculum developed by Project Evolve (https://projectevolve.co.uk/).

3. This document is intended for:

- All teaching and school management staff
- All teaching assistants and pupil support staff
- School trustees
- Parents
- Inspection teams

4. Aims and objectives:

Our school aims to

- Safeguard our pupils in all that they do online.
- Educate our pupils about all aspects of Online Safety and how to recognise what is safe or not safe and to understand what to do if things go wrong.
- Inform staff, parents and carers on what measures they need to take to ensure our children are kept safe when using online resources.
- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and trustees.
- Deliver an effective approach to online safety, which empowers the school to protect and educate the whole school community in its use of technology, including mobile and smart technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

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, antisemitism, 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 scams.

5. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, 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' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

6. Roles and Responsibilities:

6.1. The Trustees

- The Trustees have overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
- The Trustees will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All trustees will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on the Staff (and volunteer) ICT acceptable policy.
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

6.2. The Headteacher and designated safeguarding lead (DSL)

- The Headteacher who is also the DSL is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Headteacher and DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff (and volunteers) understand this policy and that it is being implemented consistently throughout the school
- Working with the ICT lead, infrastructure and broadband contractors, and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the School Child Protection and Safeguarding Policy.
- Ensuring that online safety logs produced by Senso are checked regularly.
- Ensuring that any major/critical online safety incidents monitored by Senso are dealt with appropriately and logged on MyConcern in line with this and/or other relevant policies (i.e. Child Protection and Safeguarding Policy)
- Ensuring that all staff are provided with up-to-day training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports regarding online safety in school to the board of trustees.

This list is not intended to be exhaustive.

6.3. The network infrastructure and broadband contractors.

The infrastructure and broadband contractors are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files (Smoothwall filtering).
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy (Senso monitoring).

This list is not intended to be exhaustive.

6.4. Computing Lead

The Computing Lead is responsible for:

- Taking a lead role in establishing and reviewing the Online Safety Policy.
- Planning and ensuring all pupils are provided with a current Online Safety curriculum to help them learn how to protect themselves (and others) online and understand what to do if things go wrong.
- Provide advice for staff and the wider school community and signposting relevant training and resources
- Liaising with the relevant technical support teams and other outside agencies

- Meeting with the DSL to discuss issues and actions
- Communicating up-to-date Online Safety information to the wider school community.

This list is not intended to be exhaustive.

6.5. All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the Staff (and volunteer) ICT acceptable policy and ensuring that pupils follow the school's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged on MyConcern 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 anti-bullying 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'

This list is not intended to be exhaustive.

6.6. Parents and Carers

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy

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

6.7. 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 Staff (and volunteer) ICT acceptable policy.

7. Educating pupils about online safety

Pupils will be taught about online safety as part of the computing curriculum.

Taken from the National Curriculum computing program of study:

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 school has adopted the resources created by Project Evolve. Project Evolve is a toolkit based on the UKCIS framework "Education for a Connect World' that covers knowledge, skills, behaviours and attitudes across eight stands of online life from Early Years through to eighteen, guiding educators as to the areas they should be discussing with children as they develop their use of online technology.

8. Educating parents about online safety

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

Online safety will also be covered during parents' evenings.

The school will let parents know:

- Which systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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

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

9. Cyber-bullying

9.1. Preventing and addressing 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 1 person or group by another person or group, where the relationship involves an imbalance of power.

To help prevent cyber-bullying, we will ensure, through our Online Safety Curriculum, 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.

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

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school anti-bullying 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

9.2 Examining electronic devices

The headteacher, (or any member of staff authorised to do so by the headteacher), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the DSL or deputy DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy.

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

10. Acceptable use of the internet in school

All users of school devices (pupils, parents, staff, volunteers and trustees) have to agree to the acceptable use of the school's ICT systems and the internet via the pop-up message when they sign onto any school device. Visitors will be expected to read and agree to the school's terms on acceptable ICT 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.

All internet activity is filtered via Smoothwall. All network activity is monitored via Senso, which tracks and logs all user activity on our school network. The DSL is alerted to any activity which is deemed high risk or urgent and monitors daily logs and implements actions on any recorded incidents as appropriate.

11. Pupils using mobile devices in school

Year 5 and 6 Pupils may bring mobile devices into school, but are not permitted to use them during the school day or on the school premises at the start or end of the school day.

Any use of mobile devices in school by pupils must be in line with the schools Child's Mobile Phone agreement and parents/carers need to return a signed acceptance before a child can bring their mobile phone into school.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

12. 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
- 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 by always installing the latest updates

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

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 the DSL.

13. How the school will respond to issues of misuse (also see the Staff and Volunteer ICT Acceptable Use Policy)

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

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

14. Training

All new staff members will receive training, as part of their induction, on safe internet use, cyber security 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).

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 up the risks
- 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 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.

Trustees 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.

15. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety using MyConcern safeguarding software.

This policy will be reviewed every year by the Computing Lead. At every review, the policy will be shared with the board of trustees. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

16. Links with other policies

This online safety policy is linked to our:

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

17. 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?
Online Safety 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 year.

Review Date by Trustees: Nov 2023

To be reviewed: Nov 2024