



Coleridge Primary School

Online Safety Policy

January 2026

Review: January 2027

Contents

1. Aims.....	2
2. Legislation and guidance.....	2
3. Roles and responsibilities.....	3
4. Educating pupils about online safety.....	5
5. Educating parents about online safety	5
6. Cyber-bullying.....	6
7. Acceptable Use of the Internet.....	6
8. Pupil mobile devices.....	7
9. Staff mobile devices	8
10. How the school will respond to issues of misuse	9
11. Training.....	9
12. Monitoring arrangements.....	10
13. Links with other policies.....	10

1. Aims

Coleridge Primary 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 the whole school community to use technology safely, including mobile and smart technology
- Establish clear mechanisms to identify, intervene and escalate online safety incidents appropriately
- Ensure that online safety is recognised as a core element of safeguarding

The four key categories of risk

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

- **Content** – exposure to illegal, inappropriate or harmful content, including pornography, misinformation and fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, and AI-generated or manipulated content
- **Contact** – harmful online interactions such as peer pressure, unsolicited contact, commercial advertising, livestreaming risks, gaming chat functions, and adults posing as children for grooming, criminal, financial or other exploitative purposes
- **Conduct** – harmful online behaviours such as online bullying, misuse of technology, and the making, sending or receiving of explicit images, including consensual and non-consensual sharing of nudes and semi-nudes
- **Commerce** – risks including online gambling, in-app purchases, inappropriate advertising, phishing, scams and financial exploitation

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2025 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 in schools
- The Prevent Duty: safeguarding learners vulnerable to radicalisation.

It also reflects relevant legislation, including but not limited to:

- Education Act 1996 (as amended)
- Education and Inspections Act 2006

- 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.)
- Equality Act 2010

The policy also takes into account of:

- The National Curriculum computing programmes of study.
- The UK Council for Internet Safety (UKCIS) framework *Education for a Connected World*

This policy will be reviewed annually and updated to reflect any future revisions of KCSIE or related statutory guidance.

3. Roles and responsibilities

3.1 The governing body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governor with responsibility for safeguarding will oversee online safety and meet with the DSL and Online Safety Lead as required.

All governors will:

- Ensure they have read and understand this policy
- Ensure that online safety is embedded within the school's wider safeguarding approach
- Ensure that teaching about online safety is adapted appropriately for vulnerable pupils and pupils with SEND

3.2 The headteacher

The headteacher is responsible for ensuring that this policy is implemented consistently and that all staff understand their responsibilities.

3.3 The designated safeguarding lead

The DSL takes lead responsibility for online safety and will:

- Support the headteacher in implementation of this policy
- Work with staff and the network manager to address incidents
- Manage online safety incidents in line with the safeguarding policy
- Ensure incidents are logged and reviewed appropriately
- Ensure incidents of cyber-bullying are addressed in line with the behaviour policy

- Deliver and update staff training
- Liaise with external agencies where necessary

3.4 The network manager

The network manager is responsible for:

- Maintaining appropriate filtering and monitoring systems in line with DfE expectations
- Reviewing monitoring alerts and reports regularly, escalating concerns to the DSL where required
- Ensuring ICT systems are secure, updated and protected against malware
- Blocking access to harmful content where possible
- Logging and responding to incidents appropriately

3.5 All staff and volunteers

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

- Understanding and following this policy
- Implementing online safety procedures consistently
- Reporting online safety concerns promptly to the DSL
- Responding to reports of sexual violence or harassment online or offline
- Maintaining a safeguarding mindset of “it could happen here”

3.6 Parents

Parents are expected to:

- Model safe and responsible use of technology at home
- Monitor and supervise their child’s online activity appropriately
- Report online safety concerns to the school promptly

Parents can access further guidance via:

- [UK Safer Internet Centre](#)
- [Childnet International](#)

3.7 Visitors and members of the community

Visitors using school ICT systems will be made aware of this policy where appropriate and expected to follow it.

4. Educating pupils about online safety

Pupils are taught online safety as part of a broad and balanced curriculum.

Our curriculum follows **Education for a Connected World** and covers:

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, wellbeing and lifestyle
- Privacy and security
- Copyright and ownership
- Understanding artificial intelligence (AI) and recognising its limitations and risks

Pupils are regularly reminded how and to whom they can report concerns about online safety and are encouraged to speak to a trusted adult if something online worries them.

Reporting routes are explained using age-appropriate language and may include speaking directly to a class teacher, teaching assistant, DSL or another trusted member of staff, as well as through class discussions, assemblies and other pastoral activities.

The school actively promotes pupil voice so that children feel confident to raise concerns, including when they are worried about their own online experiences or those of others.

Age-appropriate systems such as worry boxes, check-ins or circle time may also be used to support pupils in sharing concerns.

Teaching is adapted as necessary for vulnerable pupils and those with SEND.

5. Educating parents about online safety

The school raises parental awareness through:

- Letters and electronic communications
- The school website and parent communication platform (ParentHub)
- Parent meetings and workshops

Parents will be informed about:

- The school's filtering and monitoring systems
- Online platforms used for learning
- Expectations around safe and appropriate use at home

6. Cyber-bullying

6.1 Definition

Cyber-bullying is bullying that takes place online and involves repeated, intentional harm where there is an imbalance of power.

6.2 Preventing and addressing cyber-bullying

The school will:

- Teach pupils how to recognise and report cyber-bullying
- Encourage reporting by witnesses as well as victims
- Address incidents in line with behaviour, anti-bullying and safeguarding policies
- Record and review all incidents to identify patterns or emerging risks

The DSL will consider police involvement where illegal material is involved.

7. Acceptable Use of the Internet

The school's internet and ICT systems must be used responsibly and only for educational or professional purposes.

As part of the ICT curriculum, all pupils are explicitly taught to use technology safely and responsibly. This includes learning to:

- Be kind and respectful to others online.
- Never use technology to bully, upset or hurt others.
- Only access websites and use apps approved by the teacher.
- Keep passwords and personal information safe and secure.
- Tell a trusted adult if they see anything online that worries or upsets them.
- Look after school equipment and use it for its intended purpose.

The school uses appropriate filtering and monitoring systems to help protect pupils from harmful or inappropriate online content and to monitor the use of its internet and ICT systems. These systems support the school in promoting safe and responsible use of technology and identifying potential concerns. In addition, teachers actively supervise pupils when they use internet-connected devices during lessons. Staff monitor pupils' online activity as part of their classroom supervision and respond appropriately to any concerns

8. Pupil mobile devices

8.1 Pupils using mobile devices in school

Pupils are not permitted to bring personal mobile devices into school, including phones, tablets, smartwatches or other internet-enabled devices.

If a device is found, it will be confiscated and returned to parents at the end of the school day.

The school accepts no responsibility for loss, theft or damage of personally-owned mobile devices which are brought into school, contrary to the school rules.

8.2 Examining electronic devices

The headteacher, and 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 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 headteacher or 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 staff member in conjunction with the DSL or headteacher 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](#)

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

8.3. Pupils using school devices outside of school

Where pupils are issued school devices, these will be:

- Password protected
- Encrypted where possible
- Filtered and monitored
- Remotely managed

Parents are expected to supervise use at home and report any concerns to the school.

9. Staff mobile devices

9.1. Staff using mobile devices in school

Staff are permitted to bring personal mobile devices into school, and where appropriate these may be connected to the school's wireless network.

Where staff choose to use their personal devices in school:

- Devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for loss, theft or damage of personally-owned mobile devices.
- Staff may use personal mobile devices as part of school activities, however, they may not use personal devices to take photographs or videos of children. School owned iPads or cameras are available for the purpose of taking pictures or videos of children.
- Staff should not use their own mobile phones to contact parents, carers or children within or outside of school, if it can be avoided.

- If staff must use a personal mobile phone to contact parents, carers or children in an emergency, they are advised to enter '141' before dialling, to hide their number.
- For the purposes of school trips and other off site activities, school owned mobile phones are available to use.

9.2. Staff using work devices outside school

In the event of school closures or where staff may need to complete work at home, the school can issue mobile devices for staff to use off site.

Any devices issued by the school to staff will be:

- Password or PIN protected
- Encrypted wherever possible
- Protected by anti-virus and anti-spyware software
- Enrolled in a management system to allow remote tracking, locking and erasure

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

- Not removing or compromising password or PIN protection from the device
- Not sharing the device among family or friends
- Keeping operating systems up to date – always install the latest updates when prompted

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 school's network manager.

10. How the school will respond to issues of misuse

Misuse by pupils will be addressed in line with behaviour and safeguarding policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Misuse by staff will be addressed under disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

All serious or safeguarding-related incidents will be escalated to the DSL, who will determine whether external agencies should be involved.

11. Training

All staff receive online safety training on induction and at least annually thereafter, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

Training covers:

- Online abuse and exploitation
- Peer-on-peer abuse online
- Sexual harassment and harmful behaviours

- Radicalisation and extremism
- Emerging risks including AI, livestreaming and online gaming

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 DDSs 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.

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.

12. Monitoring arrangements

The DSL records and monitors online safety incidents in line with safeguarding procedures.

Filtering and monitoring systems are reviewed regularly, and alerts are acted upon promptly.

This policy is reviewed annually and shared with governors.

It will be updated to reflect any future revisions of KCSIE or related statutory guidance.

13. Links with other policies

This online safety policy is linked to our:

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