

Coalbrookdale & Ironbridge C.E. Primary School



Online Safety Policy

Last Review: Autumn 2025

Written by: L. Postance (Designated Safeguarding Lead and Deputy Head teacher)

Review Date: Autumn 2026

Vision Statement

Jesus said: 'Love each other as I have loved you'. John 15:12

Our school motto, 'Living life in all its fullness' is at the heart of everything we do and believe.

At Coalbrookdale & Ironbridge C.E Primary School, we aim to prepare the children in our care to become well-rounded members of society on their journey through school life and beyond.

We strongly believe that children learn best and achieve their full potential when they are happy and feel secure. We strive to provide a safe learning environment with a warm and welcoming atmosphere that fosters a sense of belonging among children, staff, families and the wider community. We value each individual's uniqueness and diversity, promoting respect and acceptance of one another as equals and celebrating the differences that make our community so special.

We have high expectations of the children, and we work hard to support them to become the best that they can be. For our children to flourish, socially and academically, we aim to provide an outstanding education that is both challenging and inclusive. All children are encouraged to embrace the many opportunities, and the support school provides, so that they become curious learners who are motivated and resilient with a 'Can do' attitude. Our aim is to provide the children of Coalbrookdale & Ironbridge with countless positive experiences, along with happy lifelong memories, from their time with us. We also have high expectations of attendance. We encourage families to be at school every day and to arrive on time in order to not miss any learning.

Through our supportive and inclusive Christian ethos, we are proud to foster our school values of trust, responsibility, respect, compassion and perseverance, embedding these within everyday life at school. We believe that the emotional health and wellbeing of the whole school community is fundamental to the ongoing success of our school.

We aspire to make our school a place of excellence where we educate, nurture and value everyone; that ALL children will enjoy learning and achieve their potential.

'Flourishing For All'

This policy, as written, does not discriminate on any grounds, including, but not limited to, age, disability as well as SEND, gender reassignment, gender identity, marriage and civil partnership, race, religion or belief, sex and sexual orientation.

'Let us always meet each other with a smile, for the smile is the beginning of love.' Mother Teresa.

1. Introduction

Writing and Reviewing the Online Safety Policy

This Online Safety Policy complements other key school policies, including those for computing, bullying, behaviour, safeguarding, and child protection. The school has appointed Online Safety Coordinators:

- Mandy Dhaliwal – Headteacher and Designated Child Protection Coordinator
- Louise Postance – Online Safety Coordinator and Designated Safeguarding Lead (DSL)

The policy has been discussed with staff, agreed by the Senior Leadership Team (SLT), and approved by the Interim Executive Board (IEB). It is reviewed bi-annually, or sooner if significant changes in guidance or technology occur.

The school is committed to ensuring every child is safe both in the physical and digital environment. This policy aims to protect pupils, staff, and the school community by providing clear guidance on minimising online risks and responding to incidents.

This Policy document is drawn up to protect all parties: the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

2. Why Internet Use is Important

The Internet is a vital tool for education, communication, and social development. It is embedded in the statutory curriculum and supports both teaching and school management. The school provides high-quality Internet access to promote pupil achievement and professional development.

Children use a wide range of online technologies both in and out of school, including but not limited to:

- Websites and search engines
- Email and instant messaging (e.g. WhatsApp, Snapchat, Kik)
- Voice and video calling (e.g. Skype, FaceTime, Omegle)
- Online forums and chat rooms
- Social media platforms (e.g. Facebook, TikTok, Instagram)
- Gaming platforms (e.g. Discord, PlayStation, Xbox)
- Blogs, microblogs (e.g. Twitter/X)
- Video and podcasting platforms (e.g. YouTube, Spotify)
- Mobile and smart devices with internet access
- Generative AI tools (e.g. ChatGPT, Google Gemini, Microsoft Copilot)

Our Whole School Approach to Online Safety

Creating a safe digital learning environment includes:

- Technological safeguards (e.g. filtering and monitoring software)
- Clear policies and procedures with defined roles and responsibilities
- Curriculum integration of online safety education

Pupils from KS1 to KS2 receive weekly online safety lessons using Project Evolve based on Education for a Connected World resources. Lessons include topics such as misinformation, online grooming, digital footprints, and safe use of AI.

3. Roles and Responsibilities

Leadership Team

The SLT ensures the policy is implemented and monitored through regular reviews, pupil voice, and staff feedback.

Online Safety Coordinator

Louise Postance (DSL) is responsible for:

- Staying up to date with online safety and AI-related guidance
- Disseminating updates to staff
- Overseeing filtering and monitoring systems
- Coordinating staff training and pupil education

Interim Executive Board (IEB)

The IEB oversees and reviews all school policies, including Online Safety, ensuring compliance with statutory guidance.

School Staff

All staff will:

- Promote safe online behaviours
- Foster a 'No Blame' culture to encourage reporting
- Introduce Online Safety rules at the start of each year
- Embed online safety throughout the curriculum
- Receive annual training and ongoing updates via email or briefings

Children

All pupils will:

- Engage in planned online safety lessons
- Sign and follow age-appropriate Acceptable Use Agreements (Appendices 1 & 2)
- Learn to critically evaluate online content, including misinformation and AI-generated material

Parents

Parents will:

- Receive Online Safety information at admission
- Are asked to support school rules at home
- Receive updates via email, text, or the school website
- Are contacted directly if issues arise within specific year groups

4. Internet Use & Management

Internet Use & Management

The school uses Senso monitoring software, as all school do through Telford and Wrekin which runs across all devices and applications. It:

- Alerts the Headteacher to potential breaches
- Captures screenshots for investigation
- Supports safeguarding and behaviour management

Filtering and monitoring systems are reviewed annually in line with UK Safer Internet Centre recommendations. Filtering and monitoring systems apply to AI platforms and generative tools. All users must sign the Acceptable Use Policy (Appendix 1-3) before accessing school ICT resources.

While the school takes all reasonable precautions, it cannot guarantee that inappropriate content will never appear. Pupils are taught:

- What constitutes acceptable use
- How to conduct safe and effective online research
- How to validate information and spot misinformation/disinformation
- Copyright and intellectual property awareness

At Key Stage 1, internet access is limited to adult demonstration and supervised use. At Key Stage 2, pupils are closely monitored during internet use.

5. Online Safety and AI Education

The school recognises the growing role of Artificial Intelligence (AI) in education. AI tools may be used by staff for planning, feedback, and administrative tasks. Pupils may engage with AI tools under supervision, with appropriate safeguards and parental consent.

All AI use must:

- Comply with UK GDPR and data protection laws
- Be risk-assessed before implementation
- Be monitored for accuracy, bias, and safeguarding risks

Pupils are taught to:

- Understand how AI works and its limitations
- Identify AI-generated misinformation
- Use AI responsibly and ethically

Online Safety Education

Monitoring and Accountability

All users are informed that network and internet activity is monitored and traceable to individual accounts. Monitoring is carried out using Senso software, which supports safeguarding by identifying potential risks and enabling timely intervention.

Curriculum Delivery

Coalbrookdale and Ironbridge CE Primary School delivers its online safety curriculum through the Project Evolve framework, which is based on the Education for a Connected World guidance published by the Department for Education. This framework is:

- Sequenced and age-appropriate, building pupils' knowledge, understanding, and digital resilience over time.
- Regularly updated to reflect emerging technologies, platforms, and risks, including misinformation, online grooming, and AI-generated content.

Each year group revisits key themes such as:

- Online relationships
- Self-image and identity
- Privacy and security
- Online reputation
- Managing online information
- Copyright and ownership
- Health, well-being, and lifestyle
- Online bullying

Whole-School Engagement

Online safety is embedded across the curriculum and daily school life. It is taught through:

- Computing lessons
- PSHE sessions
- Safer Internet Day (February), which includes:
 - o Age-appropriate collective worship
 - o Follow-up lessons reinforcing key messages
- NSPCC Speak Out, Stay Safe programme
- Safety Crew-led assemblies and worship sessions
- Cross-curricular links, including literacy, RE, and citizenship

Pupil Voice and Feedback

To ensure relevance and responsiveness:

- Annual pupil surveys include questions on online safety and bullying, helping staff identify gaps in understanding and tailor education accordingly.
- Regular pupil voice activities help track trends in app usage and online behaviours.
- Parent surveys include at least one question on online safety, allowing families to contribute to the school's approach and priorities.

6. Using the Internet for Learning

Using the Internet for Learning

The internet is a vital educational resource. Pupils use it across the curriculum for research, collaboration, and accessing digital learning materials. As part of the Computing Curriculum, pupils are taught to:

- Use search engines effectively
- Evaluate the accuracy, reliability, and bias of online information
- Distinguish between commercial and non-commercial websites
- Investigate the authorship and credibility of web-based content
- Understand copyright and intellectual property rights

Teachers plan internet-based activities carefully to ensure pupils access appropriate and relevant materials. Pupils are encouraged to cross-reference sources and discuss findings to develop critical thinking and digital literacy.

7. Teaching Safe Use of the Internet and ICT

We think it is crucial to teach pupils how to use the Internet safely, both at school and at home. The school uses the SMART rules developed by Childnet and endorsed by the DfE to teach safe online behaviours. These are:

- S – Safe: Keep personal information private. Avoid sharing full names, addresses, passwords, or identifiable images.
- M – Meet: Never meet someone you've only spoken to online. Report any such requests to a trusted adult.
- A – Accepting: Be cautious when accepting files, links, or friend requests. They may contain harmful content.
- R – Reliable: Not everything online is true. Compare sources and check facts before trusting information.
- T – Tell: If something online makes you feel uncomfortable, upset, or confused, tell a trusted adult immediately.

Pupils are regularly reminded of these principles through lessons, assemblies, and classroom discussions. Resources such as ThinkUKnow, Childline, and CEOP are promoted to empower children to seek help when needed.

Suitable and Unsuitable Online Material

Promoting Safe and Purposeful Internet Use

At Coalbrookdale and Ironbridge CE Primary School, we encourage pupils to view the internet as a rich and challenging learning resource. However, we recognise that navigating it safely requires guidance and support. Staff provide pupils—especially younger children—with curated suggestions for suitable websites across the curriculum. All websites and digital resources are checked for appropriateness before being used in lessons or recommended to pupils.

“Staff should be aware of the breadth of issues classified within online safety and understand that it is constantly evolving. Online safety risks are grouped into four areas: content, contact, conduct and commerce.”

— Keeping Children Safe in Education 2025, para 135

Staff receive regular CPD on online safety, led by the Online Safety Coordinator, and follow a daily Online Safety Risk Assessment. This risk assessment is structured around the four key risk categories:

- Content – exposure to inappropriate, harmful or misleading material
- Contact – harmful interactions with others online
- Conduct – personal online behaviour that increases risk
- Commerce – risks from online advertising, scams, and financial exploitation

All staff are trained to identify and mitigate these risks, and the risk assessment is reviewed annually and shared during INSET training.

Non-Education Materials and free Time Use

We believe in guided exploration rather than strict restriction. In addition to curriculum-related content, pupils are encouraged to access child-friendly entertainment and activity websites during free time, such as in wraparound care or at home. These sites offer games, creative tools, and educational content appropriate for their age group.

A selection of recommended links is available:

- On the school website
- In shared pupil folders on the school network

Responding to Unsuitable Material

Despite robust filtering and monitoring systems, pupils may occasionally encounter offensive or distressing content online. Pupils are taught to report such experiences immediately to a trusted adult. The school’s response includes:

1. Recording the website and any linked content
2. Informing the ICT technician
3. Logging the incident in the safeguarding system
4. Discussing the incident with the pupil and their parent/carer
5. Providing follow-up education to help the pupil avoid similar experiences

8. E-mail

Email is a valuable communication tool, and pupils are taught to use it safely and responsibly. Key principles include:

- Never sharing personal information via email
- Not arranging to meet anyone online without adult permission
- Reporting offensive or suspicious emails immediately
- Understanding that chain letters and spam are not permitted

9. Mobile phones and Internet-Enabled Devices

As internet-enabled devices become more common, the school recognises both their potential and associated risks. Pupils are taught:

- The legal and ethical implications of sharing images and personal data online
- How data protection and privacy laws apply to mobile device use
- The importance of digital consent and respectful online behaviour

Personal mobile phones and similar devices are not permitted during the school day. If a pupil requires a phone for travel to and from school:

- It must be handed in to the School Office upon arrival
- It will be securely stored and returned at the end of the day
- Parental consent must be provided in advance

10. Published Content and the School Website

The school website includes only official contact details—address, email, and phone number. No personal information about staff or pupils is published. The Headteacher holds editorial responsibility and ensures that all content is:

- Accurate
- Appropriate
- Compliant with safeguarding and data protection standards

11. Publishing Children's Images and Work

Written consent from parents or carers is obtained before any photographs or videos of pupils are published on the school website, social media, or other digital platforms. A secure log is maintained of pupils for whom permission has not been granted, and this is reviewed and updated regularly.

- Pupils' full names will not be published alongside images or videos unless explicit consent has been obtained.
- Pupil work may be published online to celebrate achievement and learning, but personal identifiers are removed unless permission is granted.
- All published content is reviewed by the Headteacher, who holds editorial responsibility and ensures compliance with safeguarding and data protection standards.

12. Social Networking and Personal Publishing

The school blocks and filters access to social networking sites on all school devices. Pupils are taught:

- Never to share personal details online that could identify them or their location.
- That the use of social networking platforms is not appropriate for primary-aged children, in line with age restrictions and safeguarding guidance.

Regular pupil voice surveys help staff stay informed about the platforms and apps children are using outside of school. This informs staff training and curriculum updates to ensure pupils receive relevant and timely guidance.

13. Managing Emerging Technologies

Emerging technologies are reviewed by Telford and Wrekin ICT support for educational benefit. Before any new technology is introduced in school:

- A risk assessment is carried out, considering safeguarding, data protection, and educational value.
- Staff are trained on safe and appropriate use.

This includes technologies such as:

- AI-powered tools
- Smart devices
- Wearables
- Cloud-based platforms

14. Protecting Personal Data

The school complies with the Data Protection Act 2018 and UK GDPR. Personal data is:

- Recorded, processed, and stored securely
- Transferred only when necessary and with appropriate safeguards
- Made available only to authorised individuals
- The school will not permit AI use involving personal data.

Staff are trained in data protection principles and understand their responsibilities in handling pupil and staff data securely.

15. Deliberate Misuse of the Internet Facilities

The school is committed to safeguarding pupils from online harm, including inappropriate use of the Internet and emerging risks from AI technologies. All pupils must follow the school's Acceptable Use Policy (AUP). Where deliberate misuse occurs, sanctions will be applied proportionately, considering the nature of the incident and any previous misuse.

Monitoring and Reporting

- The school uses Senso and other approved filtering and monitoring systems to detect inappropriate searches, AI misuse, and attempts to bypass security.
- All incidents are reported instantly to the Headteacher and Designated Safeguarding Lead (DSL) for review and action.

Sanctions Framework

Unsuitable Material

Examples: online games, celebrity images, music downloads, sports websites, or non-educational content.

- Initial warning from class teacher.
- Temporary restriction from out-of-school-hours Internet facilities.
- Report to Headteacher.
- Letter to parent/carer.

Offensive or Harmful Material

Examples: nude or semi-nude images, pornographic content, racist, sexist, extremist, or hate material.

- Incident logged and reported to Headteacher and DSL.
- Immediate letter to parent/carer.
- Removal of Internet privileges and username.
- Meeting with parent/carer to re-sign the Internet Use Agreement.
- Removal of out-of-school-hours Internet access.

AI Misuse

Examples: generating harmful or inappropriate content, using AI tools to bypass filters, creating deepfakes, plagiarism, or sharing misinformation.

- Incident logged and reported to DSL.
- Removal of AI access privileges.
- Parent/carer meeting and re-signing of Acceptable Use Agreement.
- Additional digital literacy support provided to pupil.

The school will follow UKCIS guidance on managing nude and semi-nude image incidents and comply with KCSIE requirements.

16. Handling Online Safety Complaints

All complaints of Internet or technology misuse will be logged and reviewed by a senior member of staff and referred to the Designated Safeguarding Lead (DSL) where appropriate.

Any complaint about staff misuse must be referred immediately to the Headteacher and managed in line with KCSIE Part Four and LADO procedures.

Complaints of a child protection nature, including those involving harmful online content, AI misuse, or illegal activity, will be dealt with in accordance with the school's safeguarding and child protection policy.

Where illegal content is suspected (e.g., child sexual abuse material, extremist content), the school will inform the police without delay and follow statutory guidance.

The school takes all reasonable steps to ensure pupils are safe online, including implementing DfE filtering and monitoring standards and supervising access to technology. However, due to the global nature of the Internet and rapid technological change, it is not possible to guarantee that unsuitable material will never appear on a school device. The school will act promptly to address any incident and mitigate harm. Complaints of Internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the headteacher. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Use of the Internet and ICT Resources by School Staff

The school recognises the Internet and ICT resources as essential tools for teaching, learning, and professional development. Staff are encouraged to use these resources responsibly and in line with the school's Acceptable Use Policy (AUP) and safeguarding procedures.

Professional Use

Staff must model safe, responsible, and inclusive ICT use at all times. All online activity should support the school's values and comply with KCSIE 2025, Data Protection Act 2018, and school safeguarding policies. Staff must not upload or share personal or pupil data on external platforms, including AI tools, without prior authorisation.

AI and Emerging Technologies

Staff may only use AI tools for educational purposes where risk assessments have been completed and age-appropriate safeguards are in place. Generative AI must not be used for pupil data processing or to create content that could mislead or harm. Staff should remain alert to risks such as deepfakes, misinformation, and bias in AI-generated content.

Internet and ICT Access

The Internet is available for professional use. Staff accounts and devices must be used securely and in accordance with school policy. ICT resources provided include computers, laptops, tablets, interactive whiteboards, cameras, and approved software. Staff borrowing equipment must complete the loan agreement and ensure devices are kept secure off-site.

Email and Communication

Staff will be provided with a school email address for all professional communication. Emails represent the school and must reflect professional standards. School email accounts may be accessed for safeguarding or operational reasons, with privacy respected.

Social Networking and Online Forums

Staff engaging in online forums or social networking must maintain professional boundaries and uphold the school's reputation. Personal social media use must not compromise safeguarding or professional conduct.

Monitoring and Compliance

All school ICT systems are subject to filtering and monitoring for safeguarding and security. Breaches of this policy will be addressed under staff disciplinary procedures.

Data Protection and Copyright

The school has data protection policy in place – please see separate documentation for more details.

Copyright Compliance

Staff understand that online resources may be subject to copyright and always give appropriate credit when using materials. Staff are aware of this policy, and how it relates to Internet and ICT use, in particular with regard to pupil data and photographs, and follow the guidelines as necessary. The school operates under DfE-provided copyright licences (e.g., CLA, ERA, SPML) and staff must follow licence conditions. Pupils are taught to respect copyright and intellectual property when creating and sharing content.

AI and Intellectual Property

AI tools will only be used under supervision and for age-appropriate educational purposes. Personal or sensitive data must never be entered into AI systems. AI-generated content must be reviewed by staff before use and comply with copyright law. Ownership of AI-generated materials remains with the school or pupil; AI tools will not use submitted work for training without explicit consent.

Appendix 1- Acceptable Use Policy (EYFS and KS1)



Acceptable Use Policy for EYFS and KS1 Children

This agreement will help keep me safe and help me to be fair to others.

- I will always keep my passwords a secret.
- I will ask a teacher or suitable adult if I want to use the computers, iPads, or Chromebooks.
- I will only visit sites which my teacher or a suitable adult has told me are okay to use.
- I will take care of computers, iPads, Chromebooks, and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me or makes me feel unsafe on the screen.
- I will not share my name, address, or pictures online unless my teacher says it is okay.
- I will not use apps or websites that make pictures, videos, or words unless my teacher says it is okay.
- I will be kind and polite when I use technology.
- I know that if I break the rules, I might not be allowed to use a computer, iPad, or Chromebook in school.
- I am aware that anything I do on the computer may be seen by someone else.
- I am also aware that the school's internet and safety filter is maintained and monitored by Telford and Wrekin Local Authority.

Pupil name: _____

Signed (child): _____

Date: _____

Appendix 2- Acceptable Use Policy (KS2)



Acceptable Use Policy for KS2 Children

This agreement will help keep me safe and help me to be fair to others.

- I will take care when using school IT equipment and use it responsibly.
- I will keep my passwords private unless I need to share them with a trusted adult.
- I will inform an adult if I see or receive any unpleasant text, images, or messages.
- I will not interfere with anyone else's passwords, settings, or files.
- I will be careful when downloading material or using files I bring into school because I understand the risks from viruses.
- Any work I upload will be my own, and I will not copy other people's work or use AI to do my work for me.
- I will not use AI tools or apps unless my teacher says it is okay, and I will never use them to make rude or unsafe content.
- I know I need permission to take someone's photograph or video them.
- Any messages I post online or send in an email will be polite and responsible.
- I will not send or forward messages or create material that is meant to upset others.
- I will never share my full name, address, phone number, or passwords online.
- I understand that what I post online can be seen by others and may stay there.
- I will only bring personal devices (smart watches, mobile phones) into school with my teacher's consent and follow school rules for storage.
- I understand that school rules apply to my online behaviour even when I am not in school if it affects others.
- I understand that the school may check my use of IT and contact my parent/carer if they are concerned about my online safety.
- I understand that if I do not follow these rules, I may not be allowed to use school computers or access the internet for a time.
- I am aware that anything I do on the computer may be seen by someone else.
- I am also aware that the school's internet and safety filter is maintained and monitored by Telford and Wrekin Local Authority.

Pupil name: _____

Signed (child): _____

Date: _____

Appendix 3 – Acceptable Use - Staff and Governors

Acceptable Use Policy for Staff and Interim Executive Board Members

This agreement helps keep pupils safe, protect data, and ensure responsible use of technology.

- I will follow the school's safeguarding policies and Keeping Children Safe in Education (KCSIE) guidance at all times.
- I will keep all passwords secure and never share them.
- I will only use school devices, email, and systems for professional purposes and in line with the school's policies.
- I will protect personal and sensitive data in accordance with UK GDPR and the Data Protection Act 2018.
- I will not store or share pupil data on personal devices or unapproved platforms.
- I will ensure that any photographs or videos of pupils are taken and used only with parental consent and for agreed educational purposes.
- I will respect copyright and intellectual property rights when using online resources and creating teaching materials.
- I will not use AI tools to process personal data or create harmful content. AI tools will only be used for age-appropriate educational purposes and under school-approved conditions.
- I will review AI-generated content before use and ensure it complies with copyright and safeguarding standards.
- I will not use technology to bully, harass, or discriminate against others.
- I will report any safeguarding concerns, online safety incidents, or inappropriate content immediately to the Designated Safeguarding Lead (DSL).
- I understand that my use of school systems may be monitored for security and safeguarding purposes.
- I will attend regular staff training to update my knowledge on safeguarding, online safety, data protection, and AI use.
- I know that failure to follow this policy may result in disciplinary action.

Staff/Board Member Name: _____

Signed: _____

Date: _____