CALDECOTE
PRIMARY SCHOOL
Happy, Healthy, High-Achieving

Online Safety Policy

September 2026

Introducing our Online Safety Policy

"It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate. The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk: [...the 4 Cs]" Keeping Children Safe in Education 2025

1.1. At Caldecote we believe that the use of technology in schools brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively.

The use of these exciting and innovative technology tools in school and at home has been shown to support learning and promote pupil achievement. Yet at the same time, we recognise that the misuse of technology can put users of technology at risk within and outside the school.

1.2. The risks they may face can broadly be categorised into the 4 C's; **Contact**, **Content**, **Conduct, and Commerce** (Keeping Children Safe in Education 2022) and may include:

- Access to harmful, illegal or otherwise unsuitable content including gaming, gambling sites, sexually explicit material and websites with extremist ideologies and images
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet, including the sharing of Self-Generated Indecent Images
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others
- Cyber-bullying
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading or streaming of music or video files
- Phishing or financial scams
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. Online safety issues can also affect adults who work or are associated with the school and this will be referenced in more detail later in this policy.

1.3. The purpose of this policy is to describe the safeguarding measures in place for adults and children in school in relation to online safety, including:

- The policies and practice embedded in our school and followed by the whole school community
- The infrastructure and how it is set up to keep pupils safe online, including filtering, monitoring, and preventing and responding to online safety incidents

- A progressive, relevant age-appropriate online safety curriculum for all pupils which (as a minimum) meets the requirements of the National Curriculum for Computing and the statutory Relationships and Health Education

1.4. Online safety in schools is primarily a safeguarding concern and not a technology one. Therefore, this policy should be viewed alongside other Safeguarding policies and approaches including, but not limited to:

- Safeguarding and Child Protection
- Personal Social and Health Education (PSHE)
- Safer Working Practices
- Data Protection / GDPR Policy
- Anti-Bullying Policy
- School Complaints Procedure
- AI Policy
- Mobile Phone- Free School Policy
- Code of Conduct for all Adults Policy
- Whistle Blowing Policy

1.5. This policy must be read alongside the staff and pupil Acceptable Use Policies attached as appendices. These AUPs outline the expectations and sanctions which apply to staff and pupil use of technology.

The development of our online safety policy involved:

- The Headteacher
- The Designated Safeguarding Lead
- The Computing Subject Leader
- The PHSE Lead
- Cambridgeshire Local Authority (The ICT Service)
- The Governor responsible for Safeguarding

1.6. This policy may also be partly reviewed and / or adapted in response to specific online safety incidents or developments in the school's use of technology. It has been shared with all staff and is readily available on the school website and has also been made available to parents.

1.7. All staff must be familiar with this policy and all staff and pupils must sign the relevant Acceptable Use Policy before being allowed to access school's systems (see appendices). As online safety is an important part of our school's approach to safeguarding, all staff have a shared responsibility to ensure that the policy and practices are embedded. This will be monitored by the Headteacher, the Designated Safeguarding Lead and governors as appropriate.

1.8. Technologies regularly used by pupils and staff include:

Staff:

- Staff laptops / iPads /desktops - staff devices can also be used at home in accordance with the staff AUP, particularly with regard to GDPR.
- Staff have access to school systems beyond the school building (e.g. School cloud Server, Microsoft, SIMS).
- Class cameras and other peripherals such as visualisers and Interactive Whiteboards
- Staff level internet access
- Staff Microsoft Outlook Email
- School accounts and APPS (eg Seesaw, Edukey, Insight, LW assessment, Mathletics)

Pupils:

- Curriculum laptops / iPads / desktops including filtered access to the Internet and pupil level access to areas of the school network
- Cameras and peripherals including programming resources
- Cloud platforms providing pupils with access within and beyond the school gates: Mathletics, Seesaw

Where the school changes the use of existing technology or introduces new technologies which may pose risks to users' safety, a risk assessment will be completed to show how the risk is being mitigated and reduced to an acceptable level.

The Online Safety Curriculum

2.1. When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. The need for a progressive, age appropriate online safety curriculum is clearly documented in the National Curriculum for Computing (England) and the statutory Relationship and Health Education.

2.2. At Caldecote we believe that a comprehensive programme of online safety education is vital for developing our pupils' ability to use technologies safely. We believe that just as children learn how to swim by going to a swimming pool so they will learn safe life-long online behaviours by accessing and using a range of online services including the World Wide Web.

2.3 Our online safety curriculum is taught through the Caldecote Computing Curriculum and is based on the Cambridgeshire Progression in Computing Capability Materials, TEACH Computing and materials from UKCIS's Education for a Connected World. It also forms part of the PHSE curriculum which follows the PHSE Association's Curriculum Model and POL Ed.

This is achieved using a combination of:

- Discrete and embedded activities drawn from a selection of appropriate materials
- Key online safety messages are delivered and reinforced through cross curricular opportunities
- Focus events to raise the profile of online safety for our pupils and school community
- A flexible curriculum which is able to respond to new challenges as they arise.

Continued professional development

3.1. In accordance with KCSiE guidance, staff at Caldecote receive safeguarding and child protection training at induction and at least annually. This training covers online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring. Safeguarding, child protection and online safety training is regularly updated during staff meetings and through updates from the school's Computing, Online Safety and Designated Safeguarding Leads, as well as training from external providers where appropriate.

3.2. The Head Teacher, DSL and Lead governor are responsible for ensuring the DfE filtering and monitoring standards are met. These identified individuals will receive more in-depth online safety training to support them in keeping up to date and reviewing the school's approach, policies and practice.

3.3. New staff receive information on the school's acceptable use policy as part of their induction, including advice on Protecting their Professional Reputation Online.

3.4 All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.

Mobile phones and use of mobile data in school

4.1. The school recognises that devices with access to 4G, 5G and wireless connectivity present significant safeguarding, online safety, privacy and distraction risks within the school environment. Devices can provide unrestricted internet access, social media access, messaging, image sharing and recording capabilities that may circumvent the school's filtering and monitoring systems.

4.2. Our aim is to provide a calm, safe and distraction-free learning environment where children can focus on their learning and feel secure. The Department for Education (DfE) expects schools to operate mobile phone free environments throughout the school day, including lessons, corridors, breaktimes and lunchtimes. In primary school, mobile phones are rarely needed. Our mobile phone-free policy explains how we keep everyone safe by limiting the use of mobile phones and similar devices.

Monitoring and averting online safety incidents

5.1. The school keeps children safe when using online technologies through a combination of online safety education, filtering and monitoring children's online activity and reporting incidents, including following Safeguarding procedures where appropriate.

5.2. The school's technology infrastructure is designed to minimise the risks associated with adult and pupil use of technology. Safeguards built into the school's infrastructure include:

- Antivirus/EDR Protection via IKICT
- Email Filtering for all accounts using Barracuda Email Protection via IKICT
- Full BMR Backups of the Schools Servers via IKICT
- Full Backup of Microsoft 365 using Barracuda Email Protection via IKICT
- Education grade internet content filtering, with different levels for both Pupils and Staff provided by Netsweeper via Oakford Internet Services
- Education grade network firewalls protecting the Schools Network, provided by Oakford Internet Services
- Education Internet Connection, provided by Oakford Internet Services
- Users Microsoft 365 Accounts are protected with enforced MFA in addition to just password logins
- Phishing Protection training for all Staff and Governors provided by Phishline via IKICT
- LA support for the Schools MIS.

5.3. Staff also monitor pupils' use of technology and, specifically, their activity online. This is achieved through a combination of:

- Appropriate levels of supervision when pupils are using online technologies. Staff to monitor and log concerns using My Concern
- Use of additional reporting tools to monitor and investigate pupil use of the internet and school provided devices including: Use of the weekly filtering report from Oakford to monitor, check and log activity and action accordingly (see log form) by Head teacher and DSL
- Safeguarding Concerns resulting from monitoring logged and actioned through My Concern

5.4. Staff use of the schools' internet can also be monitored and investigated where needed.
A system of staff and pupil passwords is in place to enable appropriate access to the school network.

- All members of staff have individual, password protected logins to the school network / cloud service / MIS systems.
- Pupils are assigned devices at the start of each lesson, which allow staff to monitor internet use.
- Visitors to the school can access limited parts of the school system using a supply login and password.
- The wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the school office.

- School staff and pupils are not permitted to connect personal devices to the school's wireless network and a guest wireless key is issued to visitors on a case-by-case basis.

5.5. Whilst we recognise that it is impossible to totally eliminate the risks associated with the use of technology, these safeguards are in place to help minimise these risks to an acceptable level.

5.6. By adhering to this policy, we aim to foster a responsible and inclusive environment for the use of technology in education upholding privacy, fairness, and transparency for the benefit of all involved.

Appendices:

1. Filtering Log
2. EYFS/ KS1 AUP Agreement
3. KS2 AUP Agreement

Online Safety Filtering Monitoring LOG

Log of information regarding unsafe use of school technology following weekly filtering report

Date	Year Group	Name	Details	My Concern log made

KS1 Safe User Agreement

When I use computers, iPads and other technology at school:

- I will use school equipment carefully.
- I will only use technology when an adult says I can.
- I will only go on websites, apps and games that my teacher chooses.
- I will keep my password secret and tell my teacher if someone knows it.
- I will not share personal information about myself or my family.
- I will be kind and respectful when using technology.
- I will not send messages or do anything online that could upset other people.
- I will ask an adult before taking or sharing photos, videos or recordings.
- I will only use AI tools or apps if my teacher says I can.
- I will not use technology to change pictures or videos of other people.
- If I see something that worries, upsets or confuses me, I will stop and tell a trusted adult straight away.
- I understand that adults in school may check what I am doing online to help keep me safe.

I will do my best to follow these rules because they help to keep me and my friends safe.

If I do not follow these rules, my teacher may:

- Talk to me about my choices.
- Talk to my parents or carers.
- Stop me using some technology for a while.
- Take other action to help keep everyone safe.

Class name:

Date:

Pupil signatures:

KS2 Safe User Agreement

I will use technology safely, responsibly and respectfully at school and at home, making positive choices when using the internet, apps, games and digital devices.

When using school technology:

- I will use the school's computing equipment (including laptops, iPads, cameras and other devices) with care and respect.
- I will use school technology for learning activities and schoolwork unless I have permission from a member of staff to do otherwise.
- I will only use the internet when a teacher or teaching assistant has allowed me to do so.
- I will only access websites, apps, games and online services that have been approved by my teacher.

Keeping accounts safe:

- I will keep my passwords private and tell an adult if I think someone else knows them.
- I will not share my password with anyone or try to use another person's account.
- I understand that my teacher may change my password if needed to help keep me safe.

Respecting other people:

- I will only delete my own files unless a teacher gives me permission to delete someone else's.
- I will not look at other people's files or work without their permission.
- I will not switch off another person device without their permission.
- I will be kind and respectful when using technology.
- I will not use technology to bully, upset, embarrass, threaten, exclude or harm anyone.

Staying safe online:

- I will not give personal information about myself or others online, including surnames, addresses, phone numbers, passwords or any information that could identify me, my family or my friends.
- If I need to create an online name, I will use one that does not reveal personal information.
- I will never arrange to meet someone I only know online.
- I will only open emails (home based only), links or attachments that I know are safe or that an adult has approved.
- If I am unsure about an email, website, message or attachment, I will ask an adult for help.

Photographs, videos and recordings:

- I will not take, share, upload or record photographs, videos or audio recordings of other people without permission from a member of staff.
- I will never post photographs or videos of other people online without permission and will not share names alongside images.

Artificial Intelligence (AI):

- I will only use AI tools, apps or websites when my teacher has given permission.
- I will not use AI or any other digital tools to create, change or share images, videos or recordings of other people.

Class:
Date:
Pupil signatures: