Coates Lane Primary School

"Happiness at the heart, shaping children of the future."

ONLINE SAFETY POLICY

DATE AGREED: OCTOBER 2024

REVIEW DATE: OCTOBER 2026

Coates Lane Primary School Online Safety Policy

Aims

Our 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 us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

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 seminudes and/or pornography), sharing other explicit images and online bullying; and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

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, 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.

Roles and responsibilities

The Governing Body

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

The governor who oversees online safety is Mrs Thompson. Mrs Thompson will report regularly to the governing body. All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college 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.

The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and back up DSL are set out in our Safeguarding and Child Protection Policy. The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the ICT Lead, Schools ICT Support and other staff, as necessary, to address any online safety issues or incidents
- Ensure that any online safety issues and incidents in line with the school child protection policy Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the governing board

The ICT Technician

The ICT Technician is 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 fortnightly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Security strategies will be discussed with the school's internet provider and Lancashire Education Authority.

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
- Adhere to the rules and restrictions in relation to the use of mobile phones in school
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendix 1/2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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 behaviour 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'

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1/2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? – UK Safer Internet Centre

Homepage - UK Safer Internet Centre

Hot topics – Childnet International

Parents & carers | Childnet

Parent resource sheet – Childnet International

Getting involved in Safer Internet Day – resources for parents and carers | Childnet

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 terms on acceptable use (appendix 2). Visitors will also be informed about the use of mobile phones in school when signing in by a member of staff.

Online Filtering and Monitoring Systems

Coates Lane Primary School uses **Netsweeper** website **filtering**. It is updated on a regular basis and keeps pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material. Netsweeper confirmed that their service fully meets the issues identified in a specific checklist by UK Safer Internet Centre (Date of assessment June 2018).

School buy into the Local Authority service for all ICT support. This includes having specialist technicians who are there anytime for school, they constantly update security and other systems in school as well as provide a report to the headteacher of any high trigger words used in searches.

Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum. All schools have to teach:

- 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.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- 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.
- Pupils may only use approved e-mail or message accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail or messages.
- Pupils and staff will use equipment responsibly with a learning and teaching focus.
- YouTube access is available for staff to use to enhance the delivery of the curriculum.
- All staff will take precautions and will assess the suitability of all videos presented.
- Staff are expected to scrutinise the content of any video they intend to play, prior to presenting it within a lesson. This allows us to maintain a safe learning environment for our children whilst reaping the benefits from the YouTube platform.
- YouTube access remains inaccessible for pupils.

- Electronic communication sent to an external organisation should be written carefully in the same way as a letter written on behalf of the school, and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- The safe use of social media and the internet will also be covered in other subjects where relevant.
- Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND. 5

Educating Parents about Online Safety

The school will raise parents' awareness of internet safety in Newsletters or other communications home, and in information via our website and a monthly newsletter that school subscribe to. This policy will also be shared with parents. Online safety will also be covered during parents' evenings. In addition we hold online safety days in school.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with any member of staff or the headteacher.

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 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. The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class on a regular basis and some issues will be addressed in assemblies.

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, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training. The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour 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 consider whether to report the incident to the police if it contains illegal material. They will also work with external services if it is deemed necessary to do so.

Examining Electronic Devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be used to:

- Cause harm and/or
- Disrupt teaching and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material or
- Retain it as evidence (of a criminal offence or a breach of school discipline) and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on Searching, screening and confiscation in schools - GOV.UK (www.gov.uk)

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

Pupils using Mobile Devices in School

Mobile phones for children are not permitted in school. All mobile phones brought into school by pupils are held in the school office until the end of the school day.

Staff using Mobile Phones in School

Staff mobile phones should be stored securely in bags or cupboards, not kept out on desks/surfaces in the classroom. Staff are not permitted to make or take phone calls on their mobile phones in lesson time. Phone calls can be taken/made in breaks/lunchtime but in a quiet private area away from children or other staff. Staff are NOT permitted to take any images of pupils/school on their mobile phones.

Visitors using Mobile Phones in School

Visitors to school are only permitted to use their mobile phones in school in a quiet private area away from children and other staff. Parent visitors attending assemblies/plays may take photographs of their child, but these must be of their child only and must only be used for personal use.

Staff using Work Devices outside of School

Staff members using a work device outside of school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2. Staff must ensure that their work device is secure and password protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using outside of school. Any USB devices containing data relating to the school cannot be used due to threat of loss (GDPR Regulations). If staff have any concerns over the security of any device, they must seek advice from the ICT Technician. Work devices must be used solely for work activities. During school trips, staff

will be required to take the school iPad for photo's and their carry mobile phones. Contact details will be left with the base contact for emergency purposes.

How the School will Respond to Issues of Misuse

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

Where a staff member misuses the school's ICT system or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. 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.

Training

All new staff members will receive training, as part of their induction, on safe internet use 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 (e.g. through emails and staff meetings). 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.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Separate training sessions focussed on online safety are also delivered to governors.

Volunteers will receive appropriate training and updates if applicable.

Dealing with Incidents

In the event that a Digital Safety incident occurs, that contravenes the Acceptable Use Policy, it is important that the protocol below will be followed.

It is important to distinguish between illegal and inappropriate use of ICT. All incidents will be logged in the incident log.

Illegal Offences

Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities e.g. Police, CEOP, Internet Watch Foundation (IFW)

In the event of any suspected illegal material or activity, school will always report the content to the Internet Watch Foundation Eliminating Child Sexual Abuse Online | Internet Watch Foundation IWF

Examples of illegal material are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

More details regarding these categories can be found on the IWF website.

eSafety across the Curriculum

Digital safety is embedded in all areas of the computing curriculum. Other issues such as Cyber-bullying and 'Grooming' are discussed in PSHE sessions. Where necessary, class teachers will differentiate their teaching to ensure all pupil remain safe when using technology.

Digital Safety – Raising Staff Awareness

All staff, upon starting work at school, are required to agree to the schools Acceptable Use Policy. Staff training updates for Digital Safety will be delivered as necessary, with a minimum of once an academic year. All training and advice will be delivered by the Headteacher and Computing Subject Leader. All staff are expected to promote and model responsible use of ICT at all times, and all staff are responsible for promoting Digital Safety whilst using ICT.

Digital Safety – Raising Parents/Carers Awareness

At Coates Lane, we offer regular opportunities for parents/carers to be informed about Digital Safety, including the benefits and risks of using various technologies. This takes place through:

- School Newsletter
- Online Safety Newsletter provided through a subscription for this specific purpose

Monitoring Arrangements

Staff in school use CPOMS to add behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4

Links with other Policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Staff Code of Conduct
- Pupils and Parents acceptable use agreement

Appendix 1

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPIL, PARENTS AND CARERS

Please review the attached School Internet Acceptable Use Policy, sign and return this permission form to the School Office.

- I will only use IT in school for school purposes.
- I will only use my class email address or my own school email address when emailing.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not tell other people my passwords.
- I will only open/delete my own files.
- I will make sure that all IT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately.
- I will not give out my details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using IT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I know that my use of IT can be checked and that my parent/carer contacted if a member of school staff is concerned about my e-Safety.

Dear Parent/Carer

ICT including the internet, email and mobile technologies etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any IT. Please read and discuss these e-Safety rules with your child and return this slip. If you have any concerns or would like some explanation, please contact school.

We have discussed this and …… (child's name) agrees to follow the e-Safety rules and to support the safe use of IT in school.

Parent/Carer Signature ……

Parent/Carer Name …….. Date ……

Appendix 2

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3 - Online Safety Training Needs – Self Audit for Staff

Name of staff member/volunteer:	Date:
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4 – Online Safety Incident Report Log

Online safety incident report log				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident


WE ARE A ...
FAIRTRADE
SCHOOL
FAIRTRADE
INVESTORS IN PEOPLE
Healthy School
change
4 life
Eat well
Move more
Live longer
SCHOOL GAMES
GOLD
2016/17
SOCIAL
SCHOOL
AWARD