Wood Field Primary School

ONLINE SAFETY POLICY

Updated April 2025
Review date April 2026

Sections of this policy:

1 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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2 Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department'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.

3 The 4 key categories of risk

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

● Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

● Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

● Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

● Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

4 Educating pupils about online safety

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

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

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Wider detail of the topics covered can be found on the school website on the 'Online Safety at School' page.

5 Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the head teacher and/or the Designated Safeguarding Lead (DSL).

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

6 Cyber-bullying

Definition

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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

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 classes, and the issue 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 (PSHCE) 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 (see section on Training for more detail).

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 the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

7 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 screening, searching and confiscation.

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 Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet See Acceptable Use policy) Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the Acceptable Use policy.

9 Pupils using mobile devices in school

Year 5 and 6 pupils may bring mobile devices into school once permission has been gained from their parent/carer. The pupils must not have their phones switched on during school hours, and must hand them into their class teacher at the start of the day to be locked away for safekeeping.

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

10 Staff using work devices outside school

Staff members using a work device outside 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 the Acceptable Use policy.

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 it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT coordinator.

Work devices must be used solely for work activities.

11 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 proportionate.

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

12 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 (for example through emails and staff meetings).

The DSLs 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.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection policy.

13 Filtering & Monitoring arrangements

Web filtering is a technology that stops users from viewing certain URLs or websites by preventing their browsers from loading pages from these sites.

Wood Field Primary's internet filtering is provided by the London Grid for Learning (LGfL). This provides a significant number of layers of protection ensuring that content that could be deemed as inappropriate is not able to be viewed by pupils or staff.

The DSL logs behaviour and safeguarding issues related to online safety. All incidents are logged on My Concern. These may be informed by Smoothwall.

Smoothwall Monitor is a real-time, digital monitoring solution that flags incidents as they happen. Monitoring both keystrokes and screen views, designated individuals are informed, through a variety of means, when users try to view or type harmful content. Nominated members of staff are immediately sent an Alert when an

incident has taken place. This allows the DSL to react immediately and appropriately.

14 Remote Learning

Remote learning is defined as an educational program designed to provide continuation of learning for students under conditions that prohibit the learner and teacher from being in the same physical space. Where remote learning is necessary, staff at Wood Field will endeavor to support and facilitate your child's continued learning. Google Classroom will be the learning platform in which we will use to support an online classroom experience for teachers and pupils. It enables online communication to support distance education in which we can communicate tasks and activities for your children to complete.

All of our Online Safety policy will remain in place when remote learning is taking place and will be expected to be followed by staff, pupils and parents or carers.

Staff:

- Where staff are interacting with children online, they will continue to follow our Staff Code of Conduct and follow our online teaching and learning policy.
- Staff will consider activities carefully when planning – online access within school will have internet content filtering systems in place that are unlikely to be replicated in the home environment.
- Staff will be responsible for monitoring communication online to ensure it is relevant and suitable for the learning platform.
- All communication is public to all participants in their Google Classroom to help safeguard all children and staff.
- Ensure online learning follows best practice and is in-line with the School's Safeguarding Policy.
- Staff will continue to be alert to signs that a child may be at risk of harm online, and act on any concerns immediately, following our reporting procedures as set out in our Safeguarding Policy
- Staff members using a work device outside 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.
- If live video and/or audio is being used to provide work online, there should be careful consideration of the location that everyone uses to film or record this.

We will make sure parents and carers:

- Are aware of the potential risks to children online and the importance of staying safe online
- Know what our school is asking children to do online, including what sites they will be using and who they will be interacting with from our school
- Are aware that they should only use reputable online companies or tutors if they wish to supplement the remote teaching and resources our school provides
- Know where else they can go for support to keep their children safe online and whilst using social media platforms.

Pupils:

- All pupils would have been taught the importance of online safety. They will know to use technology safely and respectfully, keeping personal information private; how to behave when online including what is acceptable and unacceptable behavior and how to report concerns. This learning (as discussed in more detail in Section 3) must be followed when learning remotely.
- Children will be reminded frequently that the learning platform is purely for learning. Any communication between peers and/or teachers must be relevant to the work provided. Staff will have the ability to stop unnecessary communications from taking place.
- All communication is public to all participants in their Google Classroom to help safeguard all children and staff.
- Pupils are aware of the schools Behavior Policy and this should be followed when working remotely.
- We will make sure children know how to report any concerns they have back to our school, and signpost them to other sources of support too.
- We will ensure students know who they can contact within the school for help or support.

15 Links with other policies

This online safety policy is linked to our:

- Safeguarding and Child Protection policy
- Behaviour policy - Wood Field
- Behaviour policy – Oak Field
- Capability of Staff policy
- Data protection policy and privacy notices
- Complaints policy
- Computing policy