



Woodnook Primary School

Online Safety Policy

Approved by governing body – February 2024
Review – February 2025 or before if guidance is updated
The Policy will be published on the school website.

Together we are FAIR in all we do
Friendship, Aspiration, Independence and Respect

Contents

1. Aims
2. Legislation and guidance
3. Roles and responsibilities
4. Educating pupils about online safety
5. Educating parents about online safety
6. Cyber-bullying/Child on Child/Grooming and Exploitation/Online Hoaxes
7. Acceptable use of the Internet in school
8. Pupils using mobile devices in school
9. Staff using work devices outside school
10. Social media
11. Digital and video images
12. How the school will respond to issues of misuse
13. Training
14. Monitoring arrangements
15. Links with other policies

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective and 'sticky' 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 systems to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk also known as The 4C's

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: advice for Head Teachers and school staff](#)

[Relationships and sex education](#)

[Searching, 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

3.1 The governing body

The governing body has overall responsibility for monitoring this policy and holding the Head Teacher to account for its implementation. The governing body will ensure the safeguarding governor as part of safeguarding visits monitors online safety. The governor responsible for safeguarding is Lyndsay Grimshaw.

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 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
- Do all that they reasonably can to limit children's exposure to the risks identified in the 4C's from the school's IT system. The governing body will ensure their school has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They will ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.
- The governing body will consider the number of and age range of their children, those who are potentially at greater risk of harm and how often

they access the IT system along with the proportionality of costs versus safeguarding risks.

3.2 The Head Teacher

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

3.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Head Teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Head Teacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Working with the Head Teacher, ICT manager and other staff, as necessary, to ensure the appropriate filtering and monitoring systems are in place and reviewed regularly.
- Managing all online safety issues and incidents in line with the school child protection and safeguarding policy.
- Ensuring that any online safety incidents are logged in line with the child protection and safeguarding policy (cause for concern forms).
- 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.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Head Teacher and/or governing board

3.4 The ICT manager/ technician

The ICT manager 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.
- Alongside the service provider blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

3.5 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
- 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 (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged in line with the child protection and safeguarding policy (cause for concern forms)
- 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'.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Head Teacher 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 (appendices 1 and 2).

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

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

3.7 Pupils

Pupils are expected to:

- Adhere to the Acceptable use agreement.
- Seek help from school staff if they have any concerns.
- Report online safety incidents and concerns
- **3.8 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 3)

Educating pupils about online safety

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

All schools have to teach:

[Relationships education and health education in primary schools](#)

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
- 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

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.

Educating parents about online safety

The school will raise parents' awareness of Internet safety in various ways including:

- A monthly newsletter highlighting current issues
- The ['Online Safety' page](#) on the school website
- Parents Evening and other events such as parent workshops

This policy is also available to view on the ['Policies and Statements'](#) page of the school website.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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 DSL.

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

Cyberbullying

6.1 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 1 person or group by another person or group, where the relationship involves an imbalance of power.

Types of cyber bullying may include:

Child on child sexual abuse and harassment

- Threatening, facilitating or encouraging sexual violence.
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks.
- Sexualised online bullying, e.g. sexual jokes or taunts.
- Unwanted and unsolicited sexual comments and messages.

- Consensual or non-consensual sharing of sexualised imagery.
- Abuse between young people in intimate relationships online).

Grooming and exploitation

Where an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing.

Child sexual exploitation (CSE) and child criminal exploitation (CCE).

CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the Internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the Internet.

Radicalisation, the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Online hoaxes and harmful online challenges

An online hoax is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms. harmful online challenges refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. An online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of

the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

6.2 Preventing and addressing cyber-bullying

School has a zero tolerance approach to any forms of 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.

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.

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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The Head Teacher, and any member of staff authorised to do so by the Head Teacher, 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 identified in the school rules as a banned item for which a search can be carried out, 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 Head Teacher.
- 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, 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 Head Teacher 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 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.

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 (appendices 1 to 3). 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 all users to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 to 3.

Staff using work devices outside school

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates
- Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.
- 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 Head Teacher.

Social Media

As a school we fully recognise that social media and networking are playing an increasing role within every-day life and that many staff are users of tools such as Facebook, Twitter and Instagram using these for both personal and professional use. We will ensure that both staff and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks.

Staff should:

- Ensure that their profile/posts are kept private to friends where possible, this also includes personal information such as phone numbers, email addresses etc.

- Not accept current or ex-pupils as 'friends' on social media sites such as Facebook. This is to avoid any possible misinterpretation that may arise. We do understand that some staff members have friends within the local community (such as children's parents) and ask that these members of staff take extra precaution when posting online
- Ensure that if their communication is fully public (e.g. blogs/Twitter), that they maintain their professionalism at all times and remember that they are a representative of the school Be aware that electronic texts can sometimes be misinterpreted or misconstrued, so should endeavour to minimise the possibility of this happening
- Not use these media to discuss confidential information or to discuss specific children Check with the ICT Coordinator if they need advice on monitoring their online persona and checking their security settings

Pupils should not be signed up to most social networking sites due to the over-13 age limit. However, we recognise that many are signed up either with or without parental knowledge. We will also ensure that parents are fully aware of how to minimise the risk if their children are using these sites. As a school we will use social media to post information, updates and blog posts. These will stream directly to our school website. We will ensure that we block any followers that appear inappropriate. We will use class pages on the school website to share some examples of children's learning and to communicate with parents. We will follow guidance laid out in this document to ensure children are kept safe. No-one is able to post on the website or write a comment without it being approved by a teacher to ensure that the children are not subjected to any inappropriate comments.

Digital and Video Images

As a school we will ensure that photographs and videos of children:

- Will not be put online if this has been requested by a parent/ carer
- Will not include the child's name without permission from the parents or guardians e.g. if the child has won an award
- Will not be taken by parents/ carers at school events such as sports day and special assemblies

How the school will respond to the issue of misuse

Where a pupil misuses the school's ICT systems or Internet, we will follow the procedures set out in our policies. 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/staff code of conduct. 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 online safety and links to child protection and safeguarding.

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.

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:
 - o Abusive, harassing, and misogynistic messages
 - o Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - o 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 up the risks
- 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 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.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety as per the schools child protection and safeguarding policy. This policy will be

reviewed every year by the head teacher. The policy will be shared with the governing body.

Links with other policies

(All policies can be found on the 'Policies and Statements' page on the school website.

- Behaviour Policy
- Child on Child Abuse Policy
- Complaints Policy
- PSHE Policy
- Safeguarding and Child Protection Policy
- SEND Policy
- Internet Acceptable Use Policies

Appendix 1:

EYFS and KS1 Acceptable Use Agreement (pupils and parents/carers)

The school has installed computers and Internet access to help our learning. These rules will keep us safe and help us to be fair to others:

- I will only use ICT in school for school purposes.
- I will ask permission from a member of staff before using the Internet and I will only be online when an adult is in the room.
- I will only use my login and password and never share these with others.
- I will only open and use my own files.
- The messages I send will be polite and sensible.
- I will never give out my own or other people's name, address or phone number online.
- I will never upload any images of school activities to any social networking site
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- If I see anything I am unhappy with on the computers, I will turn the screen off and tell my teacher or an appropriate adult straight away.
- I understand that the school can check my computer use and that my parents/carers can be contacted if school staff are concerned about my safety.

Signed (Pupil) _____ Class _____
Date _____

Appendix 2:

KS2 Acceptable Use Agreement (pupils and parents/carers)

This document is to provide some guidelines to ensure that you stay safe and act responsibly when using the computers. These rules will be discussed with you as a class before you sign them.

- When using the internet, I will think about the websites I am accessing and how appropriate they are
- If I find a website or image that is inappropriate, I will tell my teacher straight away
- When communicating online (in blogs, messages, email etc) I will think about the words that I use and will not use words that may offend other people
- When communicating online, I will not share personal details such as my email address or phone number
- I understand that people online might not be who they say they are
- I will not look at other people's files or documents without their permission
- I will not logon using another person's account without their permission
- I know that the teachers can, and will, check the files and websites I have used
- I will keep my usernames and passwords secure, but I understand I can share them with appropriate people, such as my parents or teachers
- I will not install any software or hardware (including memory sticks) without permission from an adult
- I understand that if I am acting inappropriately then my parents may be informed and my Internet access may be revoked.

Signed (Pupil) _____ Class _____ Date _____

Appendix 3:

Acceptable Use Agreement (staff, governors, volunteers and visitors)

This document has been written to ensure that staff use the ICT throughout the school appropriately.

Staff should:

- Ensure that they have a secure password
- Ensure that usernames and passwords are not shared with children or other staff
- Ensure that they log off when they have finished using the school network or any online environment.
- Endeavour to remove pictures/files regularly from devices used
- Ensure that online dialogue (e.g. Facebook, blog posts or emails) remains professional at all times
- Ensure that they have read and understood the Online Safety Policy
- Be aware that software or hardware should not be installed without prior consent of the Computing Coordinator or Head Teacher
- Understand that inappropriate use of the school's network may result in some services being removed and further action being taken by the Head Teacher

Signed _____ Print

_____ Date_____

