



Yeadon Westfield Infant School

ONLINE SAFETY POLICY 2025

Review 2026

This school is committed to safeguarding and promoting the wellbeing of all children, and expects our staff, governors and volunteers to share this commitment. This policy should be read in conjunction with all other school policies.

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- 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, misinformation, disinformation (including fake news), conspiracy theories, 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 the user 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

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 headteachers and school staff](#)

- 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

The governing board

- has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
- will ensure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.
- will ensure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually
- will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
- will ensure that the school teaches pupils how to keep themselves and others safe, including online.
- will ensure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness.

The board will review [the DfE's filtering and monitoring standards](#),

All governors will:

- make sure they have read and understood this policy
- agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)
- ensure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures
- make sure 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 making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL and DDSL) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

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

- in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- working with the governing board to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- working with the ICT provider to make sure the appropriate systems and processes are in place
- working with the ICT provider and other staff, as necessary, to address any online safety issues or incidents
- managing all online safety issues and incidents in line with the school's child protection policy
- responding to safeguarding concerns identified by filtering and monitoring
- making sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- making sure 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
- Liaising with other agencies and/or external services if necessary
- providing regular reports on online safety in school to the headteacher and/or governing board
- undertaking annual risk assessments that consider and reflect the risks pupils face
- providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

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 and making sure that pupils follow the school's terms on acceptable use
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes
- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to make sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure 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.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy

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

- What are the issues? – [UK Safer Internet Centre](#)
- Help and advice for parents/carers – [Childnet](#)
- Parents and carers resource sheet – [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 and expected to read and follow it.

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 **EYFS** children do not have access to the internet.

In **Key Stage (KS) 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

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/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. The policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers 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/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

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

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 1 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 encourage them 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.

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 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so 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 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.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher 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. Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

We recognise that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

We will treat any use of AI to bully pupils very seriously.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (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 and restrict access through filtering systems where appropriate.

Pupils may not bring mobile devices into school.

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
- 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 is locked if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use. Please see Acceptable Use Policy.

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 IT provider.

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 our policies on acceptable use. 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 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

Staff, governors and volunteers

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, e-bulletins and staff meetings).

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:
- Abusive, threatening, harassing and misogynistic messages
Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- 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 and deputy 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 and safeguarding policy.

Pupils

All pupils will receive age-appropriate training on safe internet use.

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

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

Acceptable Use Agreement for pupils and parents/carers

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
 - I select a website by mistake
 - I receive messages from people I don't know
 - I find anything that may upset or harm me or my friends
- Use school computers for schoolwork only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer or other device when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Yeadon Westfield Infant School Acceptable Use Agreement

To ensure that staff are fully aware of their responsibilities with respect to ICT use, they are asked to sign this acceptable use agreement.

- I understand that the network is the property of Yeadon Westfield Infant School and agree that my use must be compatible with my professional role.
- I understand that Yeadon Westfield Infant School's ICT systems may not be used for private purposes, without permission from a member of the Senior Leadership Team (SLT).
- I understand that personal mobile phones may only be switched on in out of school hours and lunch times.
- I will not take any photographs with any other camera than the school cameras. This includes mobile phone cameras, which will not be used for taking photographs of any of the children and families within the school, without specific permission from a member of the SLT, or on school trips/visits.
- I understand and agree that the school may monitor my network, Internet and mobile technology use to ensure the safety of all staff and children.
- I will respect ICT system security and understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will only install software I have a legitimate licence for.
- I will not disclose any password or login name to anyone, other than, where appropriate, the staff responsible for maintaining the school system.
- I will take all reasonable precautions to secure data or equipment taken off the school premises. I will ensure all removable media, such as USB pen drives, CDs, external hard drives or portable devices taken away from school are encrypted.
- I will report any incidents of concern to the designated person for child protection.
- I will ensure that my electronic communications with parents and carers are compatible with my professional role and cannot be misinterpreted.
- I will promote e-safety with the children e.g. in the use of passwords, to start the development of a responsible attitude towards using technology.
- I will respect copyright and intellectual property rights.
- I will use my Office 365 e-mail account for school correspondence; I will not send any school correspondence through a personal e-mail account.
- When posting to the Youtube social media channel, videos are to enhance teaching and learning. I will only post videos and pictures that I have viewed from start to finish, making a full assessment of its suitability for the intended audience. I will not publish material that violates copyright law.

Yeadon Westfield Infant School may exercise its right to monitor the use of the school's computer system, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system

is or may be taking place, or the system is or may be being used for criminal purposes or for sorting unauthorised or unlawful text, imagery or sound.

Signed _____ Date _____

Full name (printed) _____

E-mail address: _____