



Upper Nidderdale Primary Federation

Online Safety Policy

Policy:	Online Safety
This Policy was approved:	November 2022
This Policy was reviewed:	November 2023 December 2024 September 2025
Date of next review:	July 2026
Governor committee responsibility:	Full Governing Body

Contents

1. Aims	2
2. Legislation and guidance.....	3
3. Roles and responsibilities	3
4. Educating pupils about online safety.....	6
5. Educating parents/carers about online safety	7
6. Cyber-bullying	8
7. Acceptable use of the internet in school.....	14
8. Pupils using mobile devices in school.....	14
9. Staff using work devices outside school	14
10. How the school will respond to issues of misuse.....	14
11. Training	15
12. Monitoring arrangements	16
13. Links with other policies.....	16
Appendix 1: online safety training needs – self-audit for staff	17
Appendix 2: online safety incident report log.....	18

1. Aims

The Upper Nidderdale Primary Federation 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

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#) 2025, and its advice for schools on:

- › [Teaching online safety in schools](#)
- › [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- › Relationships and Sex (RSE) and Health 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.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure 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.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board 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).

The governing board will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing board will make sure 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](#), and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the school's safeguarding needs

All governors will:

- Make sure 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)
- Make sure 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

3.2 The headteacher

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

3.3 The designated safeguarding lead/DSL Team

Details of the school's designated safeguarding lead (DSL) [\[and deputy/deputies\]](#) 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:

- Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and 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 manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager 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 (see appendix 5) 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 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 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.

3.4 Schools ICT

SICT is responsible for (with checks by the DSL Team) :

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure 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 monthly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Making 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

This list is not intended to be exhaustive.

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 of the Staff Acceptable use of the school's ICT systems and the internet (appendix 3), and making sure that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- 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 failing.
- 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.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Make sure that 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/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](#)

3.7 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. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum in line with [National Curriculum computing programmes of study](#) and the government's [guidance on relationships education, relationships and sex education \(RSE\) and health education \(for teaching until 31 August 2026\)](#).

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

Pupils in **Key Stage (KS) 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
- › Be discerning in evaluating digital content

By the **end of primary school**, pupils will know:

- › That the internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- › 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, 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 are shared and used online
- › How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted
- › 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 benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- › Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online
- › How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- › Where and how to report concerns and get support with issues online

5. 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 or and through workshops. This 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.

6. Cyber-bullying

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. (See also the school behaviour policy.)

6.2 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 will 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.

6.3 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 from the headteacher
- 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

Authorised staff members may examine, and in exceptional circumstances erase, 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 the headteacher and SLT 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 whether 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/carer 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 (or equivalent) 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](#)

6.4 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. The Upper Nidderdale Primary Federation will adhere to DfE Generative AI: Product Safety Expectations (August 2025)

The Upper Nidderdale Primary Federation recognises 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.

The Upper Nidderdale Primary Federation will treat any use of AI to bully pupils very seriously, in line with our Behaviour and Anti-Bullying policies.

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 by the Upper Nidderdale Primary Federation, 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.

Possible Safeguarding Concerns around AI for staff/parents to be aware of

A. Exposure to Inappropriate and Harmful Content

AI algorithms can surface or generate violent, explicit, or disturbing material, including pornography, hate speech, and graphic violence.

- Personalised feeds may amplify exposure to such content, increasing the risk of desensitisation and trauma.
- Generative AI can create realistic but fake images, text, or video.
- Harmful content can be produced and distributed faster than moderation systems can keep up.
- AI '[companions](#)' have been known to generate harmful responses, including content that encourages self-harm, disordered eating, or suicidal ideation – posing a grave risk to vulnerable children (**see 'Companion Chatbots' below**).

- 'Nudifying' apps powered by AI can non-consensually generate explicit images of children from innocent photos, which may be used for bullying, blackmail, or exploitation (**see also 'AI-Generated Content'**).

B. AI Companion Chatbots and Harmful Advice

- AI-powered '[virtual companions](#)' are increasingly used by children and teenagers, often marketed as tools for emotional support or entertainment. However, these systems and apps can behave unpredictably – and dangerously
- Some AI companions (such as those from CharacterAI and Nomi) have provided harmful advice, including encouragement of self-harm, suicidal ideation, and dangerous dieting behaviours.
- AI companions may present themselves as emotionally intelligent, but they lack real understanding, potentially mishandling sensitive topics in ways that worsen distress.
- Emotional reliance on AI companions can replace real-world support systems, leading to greater isolation and vulnerability.
- [Griefbots](#) – AI companions designed to mimic the personality of deceased loved ones – raise complex emotional and psychological concerns, especially for children.
- These tools are often unregulated and unfiltered, with very limited age verification or guardrails in place.
- AI companions can reinforce or validate harmful beliefs – especially if trained on biased data

C. Online Grooming and Predatory Behaviour

AI is being exploited to enable new forms of child exploitation and abuse.

- AI-powered chatbots and virtual companions may be used to manipulate and groom children (**see 'Companion Chatbots' above**).
- Deepfake technology can generate fake images or videos of children, used for blackmail or coercion.
- AI-generated fake profiles and messages make it harder for children and parents to spot threats.

D. Privacy Violations and Data Exploitation

Children's data is being collected at an unprecedented scale through AI-driven systems.

- AI tools gather information on online activity, location, interests, and learning styles – often without clear safeguards.
- This data may be used for targeted advertising, profiling, or even sold to third parties.
- Within both educational and gaming environments, large volumes of sensitive data may be poorly secured or misused.

- Children from wealthier backgrounds may have better access to high-quality, privacy-respecting AI tools, increasing the digital divide in safety and opportunity

E. Cyberbullying and Online Harassment

AI can be used to create and spread personalised attacks with devastating effects.

- Generative tools can produce abusive messages, fake images, or deepfakes used in cyberbullying.
- 'Nudifying' apps and AI-edited images can be used as tools of humiliation and abuse.
- AI enables bullying that is persistent, highly targeted, and difficult to trace.
- Children may experience significant emotional harm, including anxiety, shame, and social withdrawal

F. Mental Health and Emotional Well-being

AI technologies can influence how children see themselves and the world.

- Overuse of AI-driven platforms may contribute to social isolation, anxiety, and depression.
- Curated content, AI influencers, and real-time beauty filters can distort self-perception and body image.
- AI [companions](#) can create unhealthy emotional dependencies and reduce real-life social engagement (**see 'Companion Chatbots' above**).
- Constant testing and algorithmic grading in education may increase stress and reduce joy in learning (though it is also important to note that, used well, there is also great potential for AI to enhance learning).
- Addictive algorithms – often much more persuasive than earlier recommendation engines – are designed to maximise screen time, shaping behaviour in subtle and sometimes harmful ways.

G. Misinformation, Manipulation, and Deepfakes

AI can blur the line between truth and fiction – with serious consequences for children.

- Children are increasingly exposed to AI-generated misinformation, [fake news](#), and propaganda.
- Deepfake videos and fake audio can be used to deceive, manipulate, or scam children.
- Without strong critical thinking skills, children may struggle to distinguish between reliable and false content.
- AI tools can be exploited to amplify polarisation and radicalise vulnerable individuals, including teenagers, by spreading extremist ideologies

H. AI in Educational Environments

AI offers powerful tools for personalised learning and **exciting opportunities in education**, but also raises new concerns.

- Algorithmic bias may reinforce inequalities in access, grading, and opportunity.
- Over-reliance on AI assessments could stifle creativity, curiosity, and independent thinking.
- Educational AI systems collect detailed student data, which may be insecure or exploited.
- AI tools may be used to complete homework or assignments on behalf of students, undermining learning and contributing to academic dishonesty. New systems and strategies will be needed in order to evolve accordingly.
- Children who lack access to advanced AI tools may fall behind academically, while others could become over-reliant on them.
- That said, AI also has the potential to democratise access to education and improve outcomes, provided it is equitably and safely implemented.

I) AI in Gaming Environments

AI plays a major role in shaping children's gaming experiences.

- In-game purchases can be driven by manipulative AI systems that exploit children's impulses.
- Personalised game content may introduce inappropriate themes or encourage excessive use.
- AI-powered chat features can facilitate grooming and other unsafe interactions with strangers.

J. Risks from AI-Generated Content

The scale and realism of AI-generated content present unique threats.

- Disturbing or false content can be produced en masse, making moderation nearly impossible.
- Deepfakes and synthetic media may be used for blackmail, bullying, or manipulation.
- 'Nudifying' apps can transform ordinary images into non-consensual explicit content, violating children's safety and dignity.
- AI-generated scams and hoaxes – including fake voice messages or videos – may target and deceive children.

7. 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 (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 pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

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

8. Pupils using mobile devices in school

Pupils are not permitted to bring mobile phones or smartwatches into school.

9. Staff using work devices outside school

All staff members will adhere to the Acceptable User Policy. They will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- › Keeping the device password-protected – strong passwords can be made up of [3 random words](#), in combination with numbers and special characters if required, or generated by a password manager
- › 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 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, 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 DSL/SICT.

10. 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 in this policy and 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 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.

11. Training – See Appendix One

11.1 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 deputies 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.

11.2 Pupils

All pupils will receive age-appropriate training on safe internet use, including:

- Going through the child-friendly Acceptable User Agreement.
- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

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

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 2.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Keeping Children Safe in Education 2025
- Child protection and safeguarding policy
- Behaviour policy
- Artificial Intelligence policy
- Staff Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure
- Acceptable Use policy

Appendix 1: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
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/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
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?	

Appendix 2: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident