



Highworth Combined School & Nursery

Online Safety Policy (incorporating Anti-cyberbullying and eSafety)

This policy was written/updated by:	Brian Stother
--	---------------

Approved by:	Curriculum Committee
---------------------	----------------------

Date approved:	June 2026
-----------------------	-----------

Review date:	June 2029
---------------------	-----------

1. 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

Digital well-being

In line with emerging national evidence on the impact of early smartphone and social media exposure on childhood development, and following DfE, Ofsted, and UK Safer Internet guidance encouraging schools to support parents with digital safeguarding and healthy tech habits, Highworth Combined School and Nursery is working with the Chiltern Area Partnership (CAP) to establish a shared Guiding Digital Childhoods (GDC) approach.

While not a statutory requirement, this work reflects current best practice in online safety leadership and aligns with our duty to promote pupil welfare and resilience (KCSIE, Education Act 2002, Online Safety Guidance 2023). This policy, therefore, includes a GDC Addendum, offering developmental guidance for families and clarifying our collective action commitments as a CAP school (see section 8).

2. 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](#)
- > [Meeting digital and technology standards <https://www.gov.uk/government/publications/preventing-and-tackling-bullying>](#)
- > [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- > [Relationships and sex education \(RSE\) and health education](#)
- > [Searching, screening and confiscation](#)
- > Highworth Combined School Acceptable Use Policy - Staff

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.

Equal Opportunities

Highworth acknowledges its legal duty to make reasonable adjustments for disabled children and children with special educational needs (SEND). This policy has been written in accordance with and meets the requirements of the Equality Act 2010.

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 1)
- › 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)

Details of the school's designated safeguarding lead (DSL) and 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 every 3 years 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 dynamic 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 ICT management

Under the guidance of the headteacher, ICT management is performed by a third-party provider who is responsible for:

- › 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 an appropriate 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 (Online safety incidents are recorded on BehaviourWatch) and dealt with appropriately in line with this 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 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 (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 by notifying either the headteacher or deputy headteacher
- › Following the correct procedures by obtaining prior consent from the headteacher or deputy headteacher 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 (Online safety incidents are recorded on BehaviourWatch) 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 1).

4. Educating pupils about online safety

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

All schools have to teach:

- › [Relationships education and health education](#)

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 people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- › How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- › That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- › The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- › Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- › That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online

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.

4.2 Pupils will be taught practical cyber security skills

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

- › Methods that hackers use to trick people into disclosing personal information
- › Password security
- › How to report a cyber incident or attack
- › How to report a personal data breach

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

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, where necessary. This policy will also be shared with parents/carers.

Online safety will also be covered during parents'/carers' evenings, if relevant.

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. Teachers will discuss cyber-bullying with their classes.

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).

In relation to a specific incident of cyber-bullying, where appropriate 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 as set out in our Behaviour Policy and Screening, Searching and Confiscation Policy, 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

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 or deputy headteacher 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](#)
- › The school Screening, Searching and Confiscation Policy

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

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.

Highworth Combined School 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.

Highworth Combined School will treat any use of AI to bully pupils very seriously, in line with our Behaviour Policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out dynamic risk assessments where new AI tools are being used by the school, 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.

7. Acceptable use of the internet in school

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.

Use of the internet by staff and visitors is covered by the school Acceptable Terms of Use Policy.

More information is set out in the acceptable use agreements and Pupil School Internet Agreement (appendix 1).





8. Pupils using mobile devices in school

Digital well-being

Alongside the other CAP schools, Highworth Combined School and Nursery is committed to supporting children's healthy development and digital well-being through promoting the **Four**

Guiding Principles for Families and **Four Commitments for Schools**, which are the foundations of our taught curriculum.

Guiding Principles for Families:

-  **Delay smartphones until at least Year 9** to allow children to develop social skills and independence free from constant connectivity.
-  **Delay social media until at least age 16** to reduce exposure to harmful comparison, anxiety, and algorithmic content during vulnerable developmental stages.
-  **Phone-free schools** to ensure the school day is focused on learning, play, friendship, and face-to-face communication.
-  **More independence, free play, and responsibility in the real world** to prioritise outdoor play, unstructured time, and real-world experiences as protective factors for good mental health.

School Commitments:

- We will remain **phone-free for pupils throughout the school day**.
- We will **actively teach digital safety, literacy, mindfulness and responsibility** across the curriculum.
- We will **provide consistent guidance, resources and workshops** to support parents.
- We will **model and promote healthy tech use** as a staff body and school culture.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure.

See The Acceptable Use Policy.

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 on behaviour. 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 for 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.

12. Monitoring arrangements

The DSL or other authorised person logs behaviour and safeguarding issues related to online safety. Online safety incidents are recorded on BehaviourWatch.

This policy will be formally reviewed every 3 years by the Curriculum Committee. At every review, the policy will be shared with the governing board. However, change to the policy should not be restricted to happening every 3 years. 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:

- › Child protection and safeguarding policy
- › Behaviour policy
- › Staff disciplinary procedures
- › Data protection policy and privacy notices
- › Complaints procedure
- › Highworth Combined School Acceptable Use Policy - Staff
- › Highworth Searching, Screening and Confiscation Policy



Pupil's School Internet Agreement

- ☺ I will always treat all electronic equipment (including the computers and iPads) with care and respect.
- ☺ I will never send anyone my picture without permission from my teacher or parents.
- ☺ I will never give my password to anyone, not even my best friend.
- ☺ I will only use the Internet when I am with a teacher or adult.
- ☺ When using the Internet, I will follow the instruction given to me by my teacher or adult.
- ☺ I will tell my teacher or an adult straight away if I find something unpleasant.
- ☺ I will never try to find bad words or pictures, or mean or unkind material on purpose.
- ☺ My files will be checked by my teacher to make sure I am keeping to the rules.
- ☺ I will only send polite e-mail messages to the people I know at the addresses my teacher gives me.
- ☺ I will ask my teacher, or an adult, to check my e-mail messages before I send them.
- ☺ I will not give out my address or phone number, or arrange to meet anyone, over the Internet.
- ☺ I will not download software from the Internet.
- ☺ I will log off the computer when I have finished using it.
- ☺ I know that the information on the Internet may not always be true and I may need to check it.

If I don't keep to the rules:

- ☹ I might have to stop using the Internet.
- ☹ My parents might have to be told.

Appendix Two

Be smart on the internet

Childnet International
www.childnet.com

S SAFE Keep safe by being careful not to give out personal information when chatting or posting online. Personal information includes your email address, phone number and password. **ZIP IT**

M MEETING Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.

A ACCEPTING Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages! **BLOCK IT**

R RELIABLE Someone online might lie about who they are, and information on the internet may not be true. Always check information with other websites, books or someone who knows. **?**

t TELL Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online. **THINK U KNOW**
You can report online abuse to the police at www.thinkuknow.co.uk **FLAG IT**

www.kidsmart.org.uk

KidSMART Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.