Online Safety Policy

Northway Community Primary School

To be read in conjunction with the ICT and Acceptable User Policy

Approved by:	K.McKenzie	**Date:** 10.1.25
Last reviewed on:	January 2025	
Next review due by:	January 2026	

Contents

---

1. Aims

Our school aims to:

> Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors

> Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, 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, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

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

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

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

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 in schools

> Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

> Relationships and sex education

> Searching, screening and confiscation

> Education for a Connected World framework - 2020 edition

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.

A named link governor will meet with appropriate staff to discuss online safety, and monitor online safety logs as provided by the head teacher.

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 or college 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.

3.2 The Headteacher

The headteacher 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) and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSLs take lead responsibility for online safety in school, in particular:

> ensuring that staff understand this policy and that it is being implemented consistently throughout the school

> Working with the Computing lead, network manager, IT 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 child protection policy

> Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

> 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 (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

This list is not intended to be exhaustive.

3.4 The Network Manager

The network 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 as set out in the Monitoring and Filtering Policy

> Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

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 (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 (see Appendix 5) and dealt with appropriately in line with this policy

> 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 headteacher of any concerns or queries regarding this policy

> Inform staff if there are E-Safety incidents which could cause harm or upset for their child so that we can support them in school as well

> Ensure they have adhered to the permission for their child to use the internet in school.

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

> What are the issues? – UK Safer Internet Centre

> Hot topics – Childnet International

> Parent resource sheet – Childnet International

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, 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).

4. Educating Pupils about Online Safety

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

The E-Safety curriculum is based on the guidance set out in Education for a Connected World 2020

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

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.

5. Educating Parents about Online Safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be made available to parents.

Parents will be informed about concerns or issues involving their child by the class teacher or DSL/Headteacher if appropriate.

The school will inform parents, via this policy and the ICT & Acceptable User Policy, what systems the school uses to filter and monitor online use.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the class teacher who will liaise with 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 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 are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes both as part of Computing and PSHE lessons. In addition, class teachers will respond to the needs of the class should any issue arise or be reported.

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, 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 DSL or deputy DSLs 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, the authorised staff member will:

> Make an assessment of how urgent the search is, and consider the risk to other pupils and staff

> 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.

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 Child Protection 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.

7. Acceptable Use of the Internet in School

At the beginning of each academic year, class teachers will share an acceptable user policy with all children in child friendly language. This will be signed by all children in the class to show that they agree to it and then displayed within the classroom as a reminder.

Governors and visitors will sign an acceptable user policy to acknowledge they understand the terms on which they use school devices. Parents will also sign an acceptable user policy to set out how they communicate with 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.

More information and copies of the Acceptable User Policies that stakeholders sign is set out in the ICT and Acceptable User policy.

8. Pupils using Mobile Devices in School

Pupils may bring mobile devices into school, but are not permitted to use them during the school day or on the school premises. All mobile phones must be handed to the class teacher or school office during morning registration where they are stored securely until the end of the day.

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

9. 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

> 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.

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 ICT manager.

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 Inclusion, Relationships & 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 and disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and staff meetings).

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 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 and Filtering Arrangements

As per the 'Keeping Children Safe in Education' legislation, school have appropriate filtering practices in place to ensure that ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school IT system. Furthermore, as per, the 'Revised Prevent Duty Guidance: for England and Wales', schools have a duty to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering.

The internet is filtered through the school's internet provider and using Senso's content filter. Senso's cloud-based, category web content filter manages all school networked devices to filter and block harmful or inappropriate content. This filtering is appropriately adapted for devices used by KS1 and EYFS children, those used by KS2 children and staff.

Senso allows school to monitor children's internet use. When the filter is triggered by a child, the Senso software screenshots evidence of how the filter was triggered which is added to a log. The Senso software automatically prioritises reports by their importance. The head teacher is responsible for reviewing the filtering log weekly and reported to the Governing body termly. Through Senso, real time alerts are set up so that safeguarding triggers that breach the filter are sent to the head teacher so that these can be actioned immediately to keep children safe.

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

> ICT and internet 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?	
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?	