Online Safety Policy

Responsibility for oversight and update of this Policy	Headteacher and IT Lead
Last updated	March 2025
Policy review cycle	Annually
Latest policy Review date	March 2026
h://Policies/Online Safety Policy	

Developing the roots to grow and wings to fly

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
- 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) 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

It also refers to the Department'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 School Standards Committee

The school standards committee has overall responsibility for holding the headteacher to account for its implementation.

All governors will:

- Ensure that 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 1).

Members of the governing body will:

- meet with the Designated Safeguarding Lead / Online Safety Lead
- receive reports termly of online safety incidents in the Ensuring Excellence Report
- check that provision outlined in the Online Safety Policy is taking place as intended
- ensure that the filtering and monitoring provision is reviewed, at least annually.
- report to School Standards Committee

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.

The Headteacher will take the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks

The headteacher will provide termly reports on online safety incidents in the Ensuring Excellence Report to the School Standards committee.

3.3 The Designated Safeguarding Lead (DSL)

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSL takes 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 other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged 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
- Liaising with other agencies and/or external services if necessary
- Providing reports on online safety in school to the governing board

This list is not intended to be exhaustive.

3.4 IT Support

The IT support is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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 on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on Acceptable Use of the School's ICT Systems and the internet (appendix 1), and ensuring that pupils follow the school's terms on acceptable use
- Knowing that the Headteacher 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 reporting to the IT support team using the portal **and** the School Bursar who liaises with the Internet provider.
- Working with the DSL to ensure that any online safety incidents are logged 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 and carers are encouraged to support the school in reinforcing the online safety messages provided to learners in school.

Parents and carers are expected to:

- Ensure their child has read, understood (at an age-appropriate level) the terms on acceptable use of the school's ICT systems and internet (guidance on this can be found on the school website: Our School/Safeguarding/On-line Safety) and also in appendix 2.

Parents and carers 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 factsheet - 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.

4. Educating pupils about online safety

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

All schools have to teach:

- Relationships education and health education in primary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private

- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

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

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies and weekly online safety inputs to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

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 or MyEd app. This policy will also be shared with parents and carers.

The school will let parents and carers know:

- What systems the school uses to filter and monitor online use – this information is available on our website: Our School/Safeguarding/Filtering & Monitoring
- 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 children will be interacting with online - this information is available on our website: Curriculum/Computing

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher.

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

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 and the issue will be addressed in assemblies and online safety lessons.

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

The school also signposts information on cyber-bullying to parents and carers so that 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 Artificial intelligence (AI)

Generative artificial intelligence (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 Bard.

Chadsmead Primary Academy 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.

Chadsmead Primary Academy will treat any use of AI to bully pupils in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to read 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.

More information on the acceptable use agreements are available on the school website: Our School/Safeguarding/Filtering & Monitoring

8. Pupils using mobile devices in school

Year 5 and 6 pupils may bring mobile devices into school, but are not permitted to use them during the school day, including before and after school clubs. Further details are available in the Mobile Phone Policy

9. Staff using work devices outside school

Staff members using a work device outside school must not use the device in any way which would violate the school's terms of acceptable use.

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
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date by always installing the latest updates

If staff have any concerns over the security of their device, they must seek advice from IT support.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, parents will be contacted. 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 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, 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 undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors receive training on online safeguarding issues as part of their safeguarding training.

Volunteers receive appropriate training and updates, if applicable.

12. Monitoring arrangements

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

This policy will be reviewed every two years. At every review, the policy will be shared with the school standards committee.

13. Links with other policies

This online safety policy is linked to our:

Child protection and safeguarding policy

Behaviour and Restorative Relationship Policy

Child on Child Abuse Policy

Anti -Bullying Policy

Mobile Phone Policy

Staff Code of Conduct Policy

Data protection policy and privacy notices

Complaints procedure

Appendix 1:

This will be accessed through Smart Log

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking the permission details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT support know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.

Appendix 2:

This is discussed with children at an age-appropriate level.

This is available on the school website: Our School/Safeguarding/Online Safety

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: PUPILS AND PARENTS/CARERS

When I use the school's ICT systems (like computers/ipads) 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 click on 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 school work only
- I will 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 when I have finished using it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

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