

Chestnuts Primary Online Safety Policy



Approved by:	SLT	Date: September 2026
Last reviewed on:	September 2026	
Next review due by:	September 2027	

Contents

1. Aims 3
 2. Legislation and guidance
 3. Roles and responsibilities
 4. Educating pupils about online safety
 5. Educating parents about online safety
 6. Cyber-bullying
 7. Acceptable use of the internet in school
 8. Pupils using mobile devices in school
 9. Staff using work devices outside school
 10. How the school will respond to issues of misuse
 11. Training
 12. Monitoring arrangements
 13. Links with other policies
- Appendix 1: KS1 acceptable use agreement (pupils)
- Appendix 2: KS2 acceptable use agreement (pupils)
- Appendix 3: Acceptable use agreement (parents)
- Appendix 4: Acceptable use agreement (staff, governors, volunteers and visitors)
- Appendix 5: online safety training needs – self audit for staff
- Appendix 6: online safety incident report log

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, 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](#)

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, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure 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 their safeguarding needs.

All governors will:

- Ensure 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 (DSL)

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 ensuring 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 ensure 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

- 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

- Undertaking annual risk assessments that consider and reflect the risks children 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 The ICT manager

The ICT manager 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 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 on a monthly basis

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

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 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 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)

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 letting the DSL know on CPOMS and by word of mouth

Following the correct procedures by ICT support staff if they need to bypass the filtering and monitoring systems for educational purposes

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/carers

Parents/carers are expected to:

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

Ensure 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](#)

Online safety topics for parents/carers – [Childnet](#)

Parent 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

At the beginning of each half term, teachers will deliver a stand alone online safety lesson. They will continue to address e-safety points throughout their Computing units when these opportunities arise. The curriculum has progression built into it, ranging from personal and non-personal information to reliable sources and grooming (please see link below).

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

- Use technology safely and respectfully, keeping personal information private
- Identifying good secrets and bad secrets
- 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*
- *The importance of a positive digital footprint and how this can affect them later in life*
- *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.

5. Educating parents 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 virtual learning environment (VLE). 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 one 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 are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils through class work and shared assemblies, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects

where appropriate. This is explicitly addressed through our online safety curriculum and the Jigsaw scheme of work in PSHE.

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 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 consider whether the incident should be reported to the police if it involves illegal material, and will 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 DSL.

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 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 DSL and 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 if 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](#)

Our behaviour 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 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 Gemini.

Chestnuts Primary 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.

Chestnuts Primary 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 whilst they are still being developed and should carry out a risk assessment 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 it, including, but not limited to, pupils and staff.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-4). 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 is set out in the acceptable use agreements in appendices 1, 2, 3 and 4

8. Pupils using mobile devices in school

Pupils may not bring smart mobile devices into school under any circumstances. See mobile phone policy.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

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 – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- 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 – always install the latest updates

Staff members must not use the device in any way which 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 Mitchel Chappel (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 policies on ICT and internet acceptable use.. 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 disciplinary procedures/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).

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years but usually once per year. 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 logs behaviour and safeguarding issues related to online safety using our safeguard software.

This policy will be reviewed every year by the Headteacher and Deputy Headteacher. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures and staff handbook
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable usage agreements (AUPs)

Appendix 1: KS1 acceptable use agreement (pupils)

KS1 acceptable use agreement

Name _____

This is how I keep safe online

I only use devices, apps, sites or games when a trusted adult says so

I ask for help if I am stuck or not sure

I tell a trusted adult if I am worried, scared or confused

If I get a funny feeling in my tummy, I talk to an adult

I look out for my friends and tell someone if they need help

I know people online aren't always who they say they are

I know anything I do online can be shared and might stay online forever

I don't keep secrets or do dares or challenges online

I don't change clothes or get undressed in front of a camera

I am always kind and polite online

My trusted adults are _____

Appendix 2: KS2 acceptable use agreement (pupils)

KS2 acceptable use agreement

At school we use computers, and other resources connected to the internet and our wireless network. These rules will keep us safe and help us to be fair to others.

- I will keep my passwords for login in to any computer or application to myself – if I think others know my passwords I shall tell my teacher.
- I shall use the online activities and sites which school allows me to access from home appropriately.
- I will not bring in memory sticks into school unless I have been given permission.
- I will not use my own mobile device/ phone in school unless I am given permission from my teacher.
- If the computer asks for an update, I shall check this with my teacher.
- I will only use the computer for things my teacher has told me to.
- I will not use the internet to access unsuitable material.
- The messages I send will be polite and respectful. I will always report anything that I feel is unkind or makes me feel unsafe or uncomfortable to my teacher.
- I will not reply to any nasty messages.
- In school, I will only use my school e-mail and only e-mail people my teacher has approved.
- I will always keep my personal details private (e.g my name, mobile phone number, family information, journey to school, pets, hobbies).
- I will not register my details with online activities and websites without the permission of my teacher.
- I will not share files or photos without the permission of my teacher. • I will not copy text or pictures from the internet and pretend it is my own work.
- I will never meet an online friend without taking a responsible adult who I know with me.
- I understand that the school will check my computer files and will monitor the Internet sites I visit.
- I will treat computer equipment, like all school equipment, with care and respect.
- I know that if I break the rules I might not be allowed to use a computer.

I agree to follow this acceptable use policy

Name_____

Appendix 5: 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?	
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?	