



Online Safety Policy

Little Ealing Primary School

Author of policy	Halina Rooney
Policy owned by	Teaching and Learning
Last amendment date	January 2026
Approved by GB	February 2027
Renewal cycle	Annual
RENEWAL DATE	February 2027

LITTLE EALING PRIMARY SCHOOL Online Safety Policy

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, governors and volunteers
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver a practical 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 four key categories of risk

1. **Content:** being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
2. **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 to groom or exploit them for sexual, criminal, financial or other purposes
3. **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
4. **Commerce:** risks such as online gambling, inappropriate advertising, phishing and/or financial scam

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.

Roles and responsibilities

The Governing Body

The governing body:

- has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation
- 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
- will 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.

- 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).
- ensure children are taught how to keep themselves and others safe, including keeping safe online
- must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness
- will review the DfE 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

The governor who oversees online safety is the Safeguarding Governor, or deputy Safeguarding Governor, in their absence.

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
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school 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

The Headteacher

The Headteacher is responsible for:

- ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- maintaining the approved AI tools list (as detailed in our separate AI Policy)
- monitoring AI-related incidents.

The designated safeguarding lead (DSL)

Details of the school's DSL [and deputy] are set out in our Child Protection and Safeguarding policy.

The DSL and the Deputy DSL support staff to ensure they understand that online safety is everyone's responsibility by:

- 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 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 on CPOMS 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
- When requested, provide regular reports on online safety in school to the Headteacher and/or governing body.

The ICT support team (TurnlTon) and the School Business Manager (SBM)

The ICT support team with support from the SBM, are responsible for:

- Ensuring an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated regularly to assess the 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
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

Filtering and Monitoring

The school meets the DfE's filtering and monitoring standards, which are reviewed annually by the governing body in consultation with our IT provider and DSL.

Website filtering

- The school subscribes to LGfL for broadband access, including a subscription to WebScreen 3 for web filtering. It is designed specifically for schools and blocks harmful and inappropriate content.
- No web filtering system is 100% effective. Most exposure to inappropriate content that young people encounter is because of their own or others' behaviour. Therefore, to protect our students from inappropriate content, we prioritise student responsibility when using online services rather than relying solely on web filtering.
- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is impossible to guarantee that unsuitable material will never appear on a school computer. Therefore, the school cannot accept liability for the material accessed or any consequences of Internet access.
- If staff or pupils discover an unsuitable site, it must be reported to the DSL/Deputy DSL.

Securus, an online safety and monitoring software solutions expert for the education sector, conducts a full security check and monitoring of the school's ICT on a daily basis and generates monthly reports that are sent to the Headteacher, DSL and another Safeguarding Lead.

Their proactive approach ensures that their monitoring software can pre-empt detection of new and emerging threats alongside established sources and types of online risk. Their primary focus is to monitor, safeguard and protect the welfare and online safety of children. Their safeguarding team monitor activity daily for incidents of concern.

Incident 'Captures' are graded by severity. Severity 1 is low risk, up to Severity 5 being high risk. When a capture of concern is detected, their safeguarding team will analyse and determine the level of risk from the detailed evidence and ascertain whether it is a false/positive capture or one of greater concern.

Severity 4 and 5 captures generate email alerts that are immediately sent to the designated school contacts (Headteacher, DSL, Safeguarding Lead) for their attention and urgent action. For Severity 5 captures, the school will receive a telephone call which is also backed up by an SMS message. Real-time Dashboard is available via the Securus Hub and Regular Reports are sent to the designated staff.

Managing Internet Access Information system security

- School ICT systems maintenance and security, including the monitoring and updating of virus protection, is managed by external service providers, currently, 'TurnlTon'.

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/Deputy DSL are responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes
- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL/Deputy 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'
- Reading and following our separate AI Policy, including only using approved AI tools and not entering personal data into AI tools

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child understands the acceptable use of the school's ICT systems and Internet

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
- Hot topics – Childnet
- Parent resource sheet – Childnet

Visitors and members of the community

Visitors and community members who use the school's ICT systems or the Internet will be made aware of this policy by the DSL/SBM when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Educating pupils about online safety

Pupils will be taught about online safety as part of their curriculum.

Following the National Curriculum, we must teach:

- [Relationships education and health education](#) in primary schools

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

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
- How to recognise AI-generated content including deepfakes, understand AI risks and use AI responsibly.

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.

Education parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, such as the weekly newsletter, in information via our website or Class Dojo. This policy will also be shared with parents/carers.

The school will arrange online safety workshops routinely.

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.

Teaching and learning

Why Internet use is important

- The Internet is an essential element in 21st-century education, business and social interaction. Therefore, the school must provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use (e.g. cyberbullying, banter, grooming, youth-produced sexual imagery).
- Pupils will be educated in the effective use of the Internet in research, including knowledge location, retrieval and evaluation.
- Pupils will be taught how to evaluate Internet content.
- The school will ensure that Internet derived materials by staff and pupils comply with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The school will use assemblies to raise pupils' awareness of the dangers encountered online and may also invite speakers to talk to pupils about this.
- Safer Internet Day will be recognised and celebrated yearly, with a range of activities to raise awareness of topical online-safety issues.
- Pupils will be advised on personal information and where/when it is appropriate to share.
- Pupils will be taught the importance of being a responsible digital citizen.

- Pupils will be taught about the digital footprint they are creating and must consider how their online activities now could impact them in the future.

Pupil Email

- Pupils will be taught and practise appropriate use of email.
- The students' email systems will be closed to LEPS – Users cannot email accounts outside of LEPS, and users outside of LEPS cannot email users inside the school.
- Pupils and staff will not email each other, except where required to train students to use email.

Cyber-bullying

Definition

Cyberbullying 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.)

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. In addition, 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

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 appropriate subjects.

All staff, governors and volunteers (where appropriate) receive training on online safety which will include cyber-bullying, its impact and ways to support pupils as part of safeguarding training.

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 cyber-bullying incident, 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 necessary.

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 evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher
- Explain to the pupil why they are being searched, 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 headteacher and DSL (or deputy in their absence) 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/carers 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 immediately, who will, with the support of the headteacher, 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](#)

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

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, Google Bard, and other AI-powered tools.

The school has a separate, comprehensive AI Policy that sets out our detailed approach to the safe and responsible use of AI tools. All staff, governors and volunteers must read and understand our AI Policy.

This section provides a summary of key safeguarding considerations related to AI. For full details on approved tools, risk assessment processes, data protection requirements, and staff responsibilities, refer to our separate AI Policy.

AI Safeguarding Risks

We recognise that AI has many uses to help pupils learn and can support staff workload, but it also presents safeguarding risks including:

- AI can be used to create or access inappropriate, harmful or illegal content

- **Deepfakes:** AI-generated images, audio or video that look real, including deepfake pornography using someone's likeness without consent
- **Bullying and harassment:** AI can be used to bully, harass or humiliate others
- **Misinformation and bias:** AI can generate convincing but false information and may perpetuate discrimination
- **Data protection risks:** AI tools may process, store or train on personal or sensitive data
- **Fake intimacy:** AI chatbots can create false sense of intimacy or offer harmful advice to vulnerable pupils

We will treat any use of AI to bully, harass or harm pupils in line with our anti-bullying and behaviour policies.

All staff and pupils must:

- Only use AI tools that appear on the school's **approved AI tools list** (maintained in our separate AI Policy)
- **Not enter personal or sensitive data** into AI tools unless strictly necessary and approved by the DSL
- Report any concerns about AI use to the DSL immediately
- Follow all requirements set out in our separate AI Policy

Staff must also:

- Not download or install AI-based browsers (such as OpenAI's Atlas) on school devices
- Complete a risk assessment (via the DSL) before using any new AI tool
- Understand how to spot and correct errors or bias in AI outputs

Responding to AI-Related Incidents

Any incidents involving AI will be managed through our existing safeguarding procedures:

- All AI-related incidents must be **logged on CPOMS**
- The DSL will assess and respond in line with our child protection, behaviour, and anti-bullying policies
- Where incidents involve illegal content or serious harm, the DSL will consider whether to report to the police

Examples of incidents that must be reported include: pupils using AI to create inappropriate content, AI-generated deepfakes, use of AI to bully others, or unauthorised use of AI tools.

Teaching About AI

Pupils will be taught about AI safety and responsible use as part of our computing and PSHE curriculum, including:

- Recognising AI-generated content, including deepfakes
- Understanding AI risks (misinformation, bias, harmful content)
- Using AI responsibly and critically evaluating AI outputs
- How to report concerns about AI use

Governance and Links to Other Policies

The Headteacher has oversight of the school's AI approach, ensures it is implemented consistently and is responsible for maintaining the approved AI tools list and ensuring staff training on AI safety. The governing body reviews our approach to AI safety at least annually as part of safeguarding oversight.

Ofsted won't inspect AI as a standalone area, but inspectors may consider our staff's use of AI and how we respond to others using AI, including the impact on pupils. We don't create specific materials for inspection - instead, our clear strategy and culture around AI (detailed in our separate AI Policy) is embedded in our day-to-day safeguarding and teaching practice.

For comprehensive information on our approach to AI, including approved tools, risk assessment processes, data protection requirements, intellectual property considerations, and detailed staff guidance, see our separate AI Policy.

This AI section should be read in conjunction with our:

- **AI Policy** (comprehensive detail)

- Child Protection and Safeguarding Policy
- Data Protection Policy
- Behaviour and Anti-Bullying Policies

Acceptable use of the Internet in school

All pupils, parents/carers, staff, and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet.

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.

Pupils using mobile devices in school

Only pupils in Year 6 may bring mobile devices into school. They must be brick phones only; they are not allowed smart phones. The phones must be handed to their class teacher/cover teacher when entering the classroom. The phones will be locked away safely and returned to the children at the end of the day.

Staff using work devices outside school

All staff members will take appropriate steps to ensure that school devices, remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least eight 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 them to a new device
- Make 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 the Headteacher, the DSL/Deputy DSL.

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 this 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 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 that involve illegal activity or content, or otherwise severe incidents, should be reported to the police.

Training

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

All staff members will receive refresher training at least once each academic year as part of safeguarding training and 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, 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 the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term
- understand the safeguarding risks with AI and how to use AI tools safely (as set out in our separate AI policy).

The DSL/Deputy DSL will undertake child protection and safeguarding training at least every two years, including online safety. They will also update their knowledge and skills on online safety at regular intervals and at least annually. Governors will receive training on online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable. Our child protection and safeguarding policy have more information about safeguarding training.

How will this policy be communicated?

This policy can only impact practice if it is a (regularly updated) living document. It must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the school website.
- Available to staff in the Teacher Data folder on Google Drive.
- Integral to safeguarding updates and training for all staff (especially in September refreshers).
- Reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible languages appropriate to these groups).
- AUPs issued to the whole school community, on entry to the school, with annual reminders of where to find them if unchanged, and reissued if updated after an annual review.

Data Handling and GDPR

The Headteacher will work with the DPO, DSL, Deputy DSL and Governors to ensure a GDPR-compliant framework for storing data, but ensure that child protection is always put first and data-protection processes support careful and legal sharing of information

School website

- The contact details on the Website should be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully

- Pupils' full names will not be used anywhere on the Website, particularly in association with photographs.
- Permission to show pupils' faces in photos or videos online will be requested from parents/guardians through written consent when pupils join the school.

Social networking and personal publishing

The school does not permit pupils to access private social or gaming accounts on the school network. The school actively discourages parents/guardians from knowingly allowing children to use age-inappropriate social networks outside of school. Should the staff be made aware of incidents or activities on these social networks, which directly affects the children's behaviour or attitudes, then the school reserves the right to take action regarding their accounts. This may include discussions with parents, information letters or reporting the child's access to the respective organisations/companies.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit, and a risk assessment will be carried out before use in school is allowed.

Handling Online Safety complaints

- The Headteacher will deal with complaints of Internet misuse.
- Any complaint about staff misuse must be referred to the Headteacher; any complaint about the Headteacher must be referred to the Chair of Governors.
- Complaints of a child protection nature must be dealt with in accordance with school Safeguarding and Child Protection Procedures.

Community use of the Internet

All use of the school Internet connection by the community and other organisations shall be in accordance with this policy.

Introducing the Online Safety policy to pupils

- Online Safety posters will be posted next to all computers within classrooms and in a prominent place in the computing suite so that all users can see them.
- Pupils are informed that network and Internet use is monitored and appropriately followed up.
- Students across all year groups receive explicit age appropriate Online Safety lessons, and online safety is embedded across the computing curriculum and specific PSHE lessons.

Monitoring arrangements

The staff log behaviour and safeguarding issues related to online safety on CPOMs. This Online policy will be reviewed every year by the DSL and Deputy DSL.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures/Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- AI policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

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

Name of pupil:

When I use the school's ICT systems (like computers) 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 my friends or me

Use school computers for school work only

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

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the school's ICT systems and Internet when appropriately supervised by a school staff member. I agree to the conditions set out above for pupils using the school's ICT systems and Internet and make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

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

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and get onto the Internet in school, I will:

Always use the school's ICT systems and the Internet responsibly and for educational purposes only

Only use them when a teacher is present or with a teacher's permission

Keep my username and passwords safe and not share these with others

Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carers

Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others

Always log off or shut down a computer when I'm finished working on it

Only use AI tools that my teacher has approved and tell a teacher if I see concerning AI content.

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/carers or without adult supervision

If I bring a personal mobile phone or any other personal electronic device into school:

I will not use it during lessons, tutor group time, clubs or other activities organised by the school without a teacher's permission

I will use it responsibly and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

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

Signed (pupil):

Date:

Parent/carers' agreement: I agree that my child can use the school's ICT systems and Internet when appropriately supervised by a school staff member. I agree to the conditions set out above for pupils using the school's ICT systems and Internet and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carers):

Date:

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

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

Name of staff member/governor/volunteer/visitor:

I will not: use my phone during the school timetabled working hours and/or in front of children unless I have received permission from the Headteacher or the Deputy Headteacher in their absence; my phone will be kept safe and out of sight during the school working hours (and on in silent mode if relevant)

When using the school's ICT systems and accessing the Internet in school or outside the 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

Access social networking sites or chat rooms

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 with teachers first

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

Only use AI tools that appear on the school's approved AI tools list

Not enter personal information about myself or others into AI tools

Not download or install AI-based browsers on school devices

I will only use the school's ICT systems and access the Internet in school or outside the school on a work device for educational purposes or to fulfil 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 Headteacher, designated safeguarding lead (DSL), and computing lead know if a pupil informs me they have found any material that might upset, distress, or harm them or others. I will also do so if I encounter any such material.

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

Signed (staff member/governor/volunteer/visitor):

Date:

Appendix 4: 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?	