Little Stoke Primary School

Online Safety Policy

Review Details

Date reviewed	November 2025
Next review due	November 2026
Document location	Teachers Shared Drive - Policies

Signed	Dan Ross	Claire Bruford	Key changes
			To be updated annually due to rapid evolution of online risks. Point 13: statement added to Data Protection. Point 4: statement

			added about pupils and staff being prepared for future risks. 3.7: use of school sytems used offsite, cross referenced to point 1. Appendix 3 added – definitions.

Contents

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
- This policy applies to use of digital technologies and school-related online activity both on-site and off-site, including home or remote access.

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 filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those 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

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

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in 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
- 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
- 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

IT systems at LSPS are managed by Integra IT. The IT manager is responsible for ensuring that the following systems are in place:

- 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
- Regularly conducting a full security check and monitoring the school's ICT systems.
- 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 reporting directly to Integra IT and making the DSL aware of incidents by logging using CPOMS.
- Following the correct procedures by informing DSL and liaising with Integra IT as they are the only ones who are able to bypass filtering 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 on CPOMS 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
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7 Use of school systems beyond the school site

The school recognises that pupils may access school-provided systems, platforms, or online services from outside the school environment (during homework, remote learning). Online safety expectations apply in all such contexts. Access to school systems from home or off-site must only take place via approved accounts and secure log-ins.

- Pupils should ensure that devices used off-site are protected with appropriate security (passwords, antivirus, secure Wi-Fi).
- Filtering and monitoring arrangements will extend, wherever technically possible, to remote access and school-issued devices used off-site.
- Where incidents online occur outside school but have an impact on members of the school community, these will be dealt with under the school's safeguarding and behaviour procedures.

- Parents and carers will be reminded regularly of the need to supervise online activity at home and to report concerns to the school's Designated Safeguarding Lead (DSL).

3.8 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

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

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary 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

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.

The school recognises that online platforms and technologies evolve rapidly, including areas such as social media challenges, live-streaming, gaming, encrypted messaging, wearable and virtual-reality devices, and AI-generated or manipulated content. Pupils will be taught to understand and evaluate risks associated with emerging technologies and new online behaviours. Staff will receive regular updates and training to ensure they can identify and respond to new or developing online safety issues.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and 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 subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so 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 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can 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

If inappropriate material is found on the device, it is up to HT and DSL 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

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 Bard.

Little Stoke 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.

Little Stoke Primary will treat any use of AI to bully pupils in line with our anti-bullying and 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.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (see ICT and internet acceptable use policy). 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 and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

Mobile/electronic devices from home are not allowed in classes. If a child needs to bring a device in school, for example for contact with parents/carers outside of school hours, the device must be left with the school office in the morning and collected at the end of the day.

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 by always installing the latest updates

Staff members must not use the device in any way that 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 Integra IT.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. Training

All new staff members will receive relevant training, as part of their induction.

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, 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 deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. Incidents should be reported through CPOMs. Reports can be generated as incidents will be logged using the Online Safety Incident category.

This policy will be reviewed annually, or sooner if there are relevant changes needed, by the 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 code of conduct
- Data protection policy and privacy notices. (Monitoring systems will comply with data protection law; logs will be kept securely and access limited to authorised staff; retention and deletion schedules applied in line with UK General Data Protection Regulation (UK GDPR) and the Information Commissioner's Office (ICO) standards.)
- Complaints procedure
- ICT and Internet acceptable use policy

Appendix 1: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	

ONLINE SAFETY TRAINING NEEDS AUDIT	
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?	

Appendix 2: Integra IT Q and A in relation to online safety systems

1. Is your filtering provider:

a. A member of Internet Watch Foundation (IWF)?

Yes, the company we use that provides the filtering platform is a member of the IWF.

b. Signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)?

Yes, the company provides a specific filtering category that contains this list.

c. Blocking access to illegal content including child sexual abuse material (CSAM)?

Yes, we use the categories provided by the filtering provider to ensure content is blocked.

In addition to the above, we use a separate reporting system that notifies us within 60 seconds if anyone on the network attempts to access any content on these lists.

2. Is the school's filtering operational and applied to all:

a. Users, including guest accounts?

Yes, our filtering monitors all devices using the wider network, regardless of who the device belongs to.

b. School owned devices?

Yes, our filtering monitors all devices using the wider network, regardless of who the device belongs to.

c. Devices using the school broadband connection?

Yes, our filtering monitors all devices using the wider network, regardless of who the device belongs to.

3. Does the filtering system:

a. Filter all internet feeds, including any backup connections?

Yes, our filtering monitors all devices using the wider network, regardless of who the device belongs to. All connections implemented or managed by Integra IT are subject to the filtering.

b. Be age and ability appropriate for the users, and be suitable for educational settings?

Yes, we utilise authentication to age-appropriate filtering. By default (with no authentication provided) the applied filtering levels are the most restrictive while being appropriate for the youngest users of the network.

c. Handle multilingual web content, images, common misspellings and abbreviations?

The filtering system is capable of handling all character sets (languages). It does not scan the content of images. Misspellings are included within the categories and can also be added manually.

d. Identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them?

Yes, we are able to block based on category and application type, we have automated/dynamic application filters that automatically block all known and new/emerging bypass technologies (VPNs, Proxy servers, etc…) for all users/devices on the network.

e. Provide alerts when any web content has been blocked?

Yes, all network & internet use is logged. All attempts to access blocked content or blocked applications or bypass attempts raise alerts. In addition to these we also block applications that are not deemed appropriate for use on the network, some of these applications (facebook, Instagram, X (formally twitter), etc…) are tied in to many websites that are used everyday by schools, we do not generate alerts on these blocks as they are expected to occur.

4. Has the provider confirmed that filtering is being applied to mobile and app content?

Apps use many different methods to display their content. Some we are able to filter and others we cannot.

By default though, we block (in their entirety) mobile apps that are not specifically requested by schools.

5. Has a technical monitoring system been applied to devices using mobile or app content?

Schools can add additional monitoring to these devices if they wish.

6. Does the filtering system identify:

a. Device name or ID, IP address, and where possible, the individual?

Yes

b. The time and date of attempted access?

Yes

c. The search term or content being blocked?

Yes

7. Are there any additional levels of protection for users on top of the filtering service, for example, SafeSearch or a child-friendly search engine?

Yes, we enforce network wide safesearch (for all users) and restrict access to only search engines that fully support safesearch. This includes some mediated and/or child specific search engines, e.g. kiddle.co, kidrex.org, kidzsearch.com, safesearchkids.com,

swiggle.org.uk, etc…

Kiddle.co and kidzsearch.com are very good at providing safe image searches too!

8. Does the monitoring system review user activity on school and college devices effectively?

(For example, does it pick up incidents urgently, through alerts or observations, allowing prompt action to be taken; and is the response recorded?

Yes, the monitoring system generates an alert within 60 seconds. Currently these alerts are sent to 3rd line IT staff for investigation. If the alert requires a response from school, a service ticket is generated and sent to the DSL for the school.

We believe we have been able to tune most false positives out of the system, so our intention is to have these alerts raised directly to the DSL for investigation in the near future.

It will never be possible to accurately remove all false positives from the system, but they have been sufficiently reduced to minimise unnecessary alert emails.

9. Does the monitoring system ensure that incidents, whether of a malicious, technical, or safeguarding nature are picked up urgently?

The system generates the alerts as quickly as possible within 60 seconds. This ensures the relevant staff are aware that an incident needs to be investigated

Appendix 3: definitions

AI (Artificial Intelligence)
Computer systems or software capable of performing tasks that normally require human intelligence, such as recognising patterns, generating text or images, or making decisions.

Acceptable Use Policy (AUP)
A set of rules outlining how school ICT systems, networks, and devices should be used safely and responsibly by pupils, staff, and visitors.

Behaviour Policy
The school's separate policy that sets expectations for pupil conduct, including behaviour online and on digital platforms.

BYOD (Bring Your Own Device)
When pupils or staff use personally owned devices (such as phones, tablets, or laptops) for school-related activities.

Child-on-Child Abuse
Any form of physical, sexual, emotional, or online abuse committed by one child towards another, including online bullying or image-based abuse.

Commerce Risk
Online risks involving financial exploitation, scams, or advertising that targets children (one of the four UKCIS risk categories).

Contact Risk
The risk of harmful contact from others online, such as grooming, exploitation, or unwanted messages.

Content Risk
The risk of children being exposed to harmful or inappropriate material online (violent, sexual, extremist, or misleading content).

Conduct Risk
The risk of children behaving in a way online that increases their own or others' exposure to harm (for example, sharing personal information, bullying, or illegal downloading).

Cyberbullying
Bullying behaviour that takes place over digital devices, through messaging, social media, gaming platforms, or image sharing.

Data Breach
An incident where personal data is lost, accessed, disclosed, or destroyed without authorisation, intentionally or accidentally.

Designated Safeguarding Lead (DSL)
The senior member of staff with lead responsibility for child protection, including online safety, within the school.

Digital Footprint
The trail of information left by a person's online activity, including social media posts, website visits, and shared data.

Filtering
A technical measure used to restrict access to inappropriate or harmful online content on the school network.

Monitoring
The process of reviewing and analysing activity on the school's ICT systems to identify potential safeguarding or policy concerns.

Online Safety (or E-Safety)
Practices and measures designed to protect children, staff, and the school community from online harm and to promote responsible, safe use of technology.

Phishing
A form of cybercrime where individuals are tricked into revealing sensitive information (such as passwords) through deceptive messages or websites.

Remote Learning
Any learning activity taking place outside the school site using online platforms or digital communication tools.

Safeguarding
The process of protecting children from maltreatment, preventing impairment of their health or development, and ensuring they grow up with safe and effective care.

School Systems/Networks
All hardware, software, internet services, and digital platforms provided or approved by the school for educational or administrative use.

Sexting/Youth-Produced Sexual Imagery
The creation or sharing of sexual or nude images by children under 18, including via messaging or social media.

Social Media
Websites and apps that allow users to create and share content or interact with others (e.g. Instagram, TikTok, YouTube, X/Twitter, Snapchat).

Wearable Technology
Smart devices worn on the body (e.g. smartwatches or fitness trackers) that collect or transmit data.

This glossary is reviewed annually to ensure definitions remain consistent with statutory guidance and current technological developments. Definitions include current and emerging terms relevant to online safety practice.