



**KINGSDOWN
SCHOOL**



**RIVER
LEARNING
TRUST**

ONLINE SAFETY POLICY

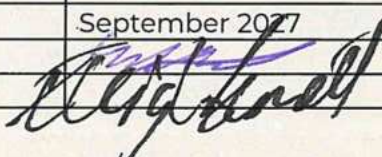
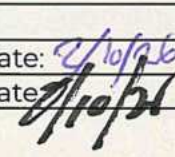
WHOLE SCHOOL VISION, PRACTICE AND PROCEDURES

SEPTEMBER 2026

Team Responsible for Online Safety Policy: Barb Timms (RLT Safeguarding Lead), Matthew Proffitt (RLT IT Director), Kingsdown School DSL

Reviewed: September 2026

Review Date: September 2027

RIVER LEARNING TRUST HEALTH & SAFETY			
Document Type:	Policy Statement		
Document Title:	Online Safety Policy		
Document Date:	Sept 2026		
Review Dates:	September 2027		
Signed:		Date: 2/10/26	Role: Chair of Governors
Signed:		Date: 2/10/26	Role: N/A

This policy has been agreed in consultation with the RLT Central Team and all school stakeholders including the Governing Body, to ensure that it remains fit for purpose. It seeks to ensure that all parties involved in the practicalities of online safety are aware and informed of online safety matters in school and to outline the school's commitment to the safety of all pupils. This policy should be read in conjunction with:

- Child protection and safeguarding policy
- Behaviour Policy
- Mobile Phone Policy
- Data protection policy and privacy notices
- Staff Acceptable Use Policy
- Anti-Bullying Policy.
- Searching, Screening and Confiscation Policy.
- Suspensions and Exclusions Policy.

Contents

1	<u>Introduction</u>	3
2	<u>Roles and responsibilities</u>	4
3	<u>Educating pupils about online safety</u>	6
4	<u>Educating parents about online safety</u>	7
5	<u>Cyber Bullying</u>	7
6	<u>Examining electronic devices</u>	8
7	<u>Acceptable use of the internet in school</u>	9
8	<u>Staff using work devices outside school</u>	10
9	<u>Monitoring and Filtering</u>	10
10	<u>Fake news, Misinformation and Disinformation</u>	12
11	<u>Artificial Intelligence</u>	12
12	<u>AI Deepfakes as Child-on-Child Abuse</u>	14
13	<u>How the school will respond to issues of misuse</u>	15
14	<u>Training</u>	15

1	<u>Introduction</u>	3
2	<u>Roles and responsibilities</u>	4
3	<u>Educating pupils about online safety</u>	6
4	<u>Educating parents about online safety</u>	7
5	<u>Cyber Bullying</u>	7
6	<u>Examining electronic devices</u>	8
7	<u>Acceptable use of the internet in school</u>	9
8	<u>Staff using work devices outside school</u>	10
9	<u>Monitoring and Filtering</u>	10
10	<u>Fake news, Misinformation and Disinformation</u>	12
15	<u>Resources, guidance, and support</u>	15
16	<u>Appendices</u>	17

1. Introduction

1.1 Kingsdown School, as part of the River Learning Trust, recognises that the internet including social media and Artificial Intelligence are a part of all of our lives. We are committed to keeping pupils safe as they explore the benefits of the online world.

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996, 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.

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology.
 - 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, anti-Semitism, 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. This includes harmful interactions with highly realistic generative AI chatbots that simulate human interaction.

- **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. This includes making or sharing AI-generated intimate images, such as deep fakes; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. 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.

All Governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms in 'Staff IT Acceptable Use Policy'
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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.

The Designated Safeguarding Lead.

Details of the school's 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, 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 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 cyberbullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular updates on online safety in school to the Headteacher and/or Governing Body

Cyber Security is a Safeguarding Duty: Protecting pupil data and safeguarding records is no longer just an IT task. If sensitive pupil information or data is compromised, it is viewed as an immediate risk to a child's well being. Because of this, managing our cyber security and information security is now a core safeguarding responsibility shared by the Designated Safeguarding Lead (DSL) and the Senior Leadership Team.

The ICT Team is responsible for:

- Working with the RLT Technical Director of IT to ensure an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Ensuring that any online safety incidents are logged and dealt with appropriately

All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the Staff IT Acceptable Use Policy and ensuring that pupils follow the school's terms on acceptable use
 - Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately

- Ensuring that any incidents of cyberbullying are responded to in line with the school behaviour policy

Parents

Parents 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
- Monitor and supervise their child's online activity whilst in their care and informing the school of any concerns.

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 adhere to the Staff IT Acceptable Use Policy

3. Educating pupils about online safety

Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks.

We aim to equip our pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world.

Underpinning knowledge and behaviours

The online world develops and changes at a great speed. New opportunities, challenges and risks are appearing all the time. This can make it difficult to stay up to date with the latest devices, platforms, apps, trends and related threats.

It is important to focus on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. This teaching could be:

- built into existing lessons across the curriculum
- covered within specific online safety lessons
- covered using school-wide approaches

As part of the statutory [relationships and health education](#) in primary schools and [relationships, sex and health education](#) in secondary schools, pupils are taught about online safety and harms. This includes being taught:

- what positive, healthy and respectful online relationships look like
- the effects of their online actions on others
- how to recognise and display respectful behaviour online

Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives.

This complements the [computing curriculum](#), which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes:

- how to use technology safely, responsibly, respectfully and securely
- where to go for help and support when they have concerns about content or contact on the internet or other online technologies

There are also other curriculum subjects which include content relevant to teaching pupils how to use the internet safely. For example, [citizenship education](#) explores:

- freedom of speech
- the role and responsibility of the media in informing and shaping public opinion
- the concept of democracy, freedom, rights, and responsibilities

Where necessary, teaching online safety will be adapted for pupils who may benefit from a more tailored and structured resource to access messages and advice about online safety risks.

4. Educating parents about online safety

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

If parents 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.

5. Cyber-bullying

Cyberbullying is the use of digital technologies—like social media, messaging apps, and online gaming—to repeatedly harass, threaten, embarrass, or target another person. Unlike traditional bullying, it can happen at any time and can feel inescapable, leaving a lasting digital footprint.

Common Forms of Cyberbullying

- Harassment: Sending abusive, insulting, or threatening messages directly to an individual.
- Exclusion: Intentionally leaving someone out of online groups, gaming sessions, or conversations.
- Impersonation: Hacking or creating fake accounts in someone else's name to send embarrassing or mean messages.
- Outing & Doxxing: Sharing private, sensitive, or embarrassing information, photos, or videos about someone publicly to cause humiliation.
- Trolling/Flaming: Using extreme hostility or deliberately provoking someone in public forums or comments solely to cause distress.

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. Tutors will discuss cyber-bullying with their tutor groups. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover

cyberbullying. This includes Personal Development (PD) and other subjects where appropriate. This topic will be covered in assemblies throughout the year.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training. In relation to a specific incident of cyber-bullying, we will follow the processes set out in our Behaviour and anti-bullying Policies.

Where illegal, inappropriate or harmful material has been spread among pupils, we 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.

All pupils know that they can report any issues, concerns or worries directly to their Tutor, Progress Leader or on SHARPS (School Help Advice Reporting Page). They will be supported and dealt with sensitively and in line with our Behaviour Policy and Child Protection Policy.

6. Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

If a member of staff finds a pornographic image, they may dispose of the image unless they have reasonable grounds to suspect that its possession constitutes a specified offence (i.e. it is extreme or an indecent image of a child) in which case it must be delivered to the police as soon as reasonably practicable.

Members of staff should never intentionally view any indecent image of a child (also sometimes known as nude or semi-nude images). Staff must never copy, print, share, store or save such images.

Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- [UKCIS \(The UK Council for Internet Safety\) guidance on sharing nudes and semi-nudes](#): advice for education settings working with children and young people

7. Acceptable use of the internet in school

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

All staff, volunteers and governors will be expected to read and agree to the Staff Acceptable Use Policy. 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.

Mobile Devices

Mobile devices including smartphones, smart watches etc are not allowed to be used by pupils during the school day. Please refer to our mobile phone policy.

8. 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
- 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 the Staff Acceptable Use Policy. 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 IT Team.

9. Monitoring and Filtering

The Securly Infrastructure

As part of RLT, our school uses **Securly**, a cloud-based web filtering solution, to provide a safe and controlled digital environment. Our implementation is designed to be flexible, applying different levels of protection based on the user's role and age:

Staff & SLT: Standard filtering focused on security and malware. Staff Leadership may have tailored access (e.g., social media) to support school communications and community engagement.

Students: A baseline safety policy is applied to all pupils. We maintain the flexibility to segment policies by Year of Intake to allow for age-appropriate restrictions or via Custom Groups for specific student interventions.

Safeguarding Alerts and Real-Time Monitoring

The system does not merely block content; it actively monitors for signs of risk using sentiment analysis and keyword tracking.

DSL Notifications: Designated Safeguarding Leads (DSLs) receive near real-time email notifications for "Trigger Events," such as searches or activity related to self-harm, cyberbullying, or extremism.

Securly Aware: For formal investigations, DSLs use the Securly Aware portal. This provides advanced context, such as sentiment analysis and flagging history, allowing the DSL to understand the intent behind a student's activity.

Weekly Audits: Every Monday at 9:00 am, DSLs receive an automated summary report covering blocked content (Pornography, Drugs, Gambling, Intolerance, etc.). **Note:** These secure links expire after 24 hours; historical logs can be accessed via the Securly Aware portal.

Account-Based Protection ("The Chrome Rule")

Filtering and monitoring are tied to the user's school account, not the physical device. Our filtering and monitoring systems are tied to the pupil's school account, not just the physical school building or device. If a pupil signs into their school account (such as the Google Chrome browser) on a personal device at home, the school's safety filters and monitoring rules will automatically apply to that session. We do not monitor personal accounts used on personal devices.

School Managed Devices: These are filtered and monitored 24/7, whether used on the school network or at home.

Personal Devices & Home Use: If a student signs into the Google Chrome browser using their school-issued credentials on a personal device (e.g., a home PC or laptop), the school's filtering and monitoring policies automatically apply to that browser session.

Unmanaged Activity: The school does not monitor activity on personal devices when used with personal accounts. Parents and carers are responsible for implementing their own home parental controls for non-school activity.

Continuous Compliance (Policy Validator)

In line with KCSIE requirements to "regularly review the effectiveness" of filtering, the school employs an automated Policy Validator tool.

Monthly Automated Audits: This tool "impersonates" different user roles (Student, Staff, SLT) monthly to ensure filtering rules are active and have not "drifted."

Traffic Light Reporting: Results are categorised into Passes, Warnings (over-blocking), and Critical Fails (safeguarding leaks).

Remediation: The IT team uses these audits to generate a "To-Do" list for immediate fixes, ensuring a transparent audit trail for the Governing Body and external inspectors via a dedicated Evaluation Web Portal.

Defined Responsibilities

DSL & Pastoral Teams: Hold primary responsibility for the active monitoring of alerts and responding to potential risks identified by the system.

IT Support Teams: Responsible for the technical maintenance of the system and performing history reviews strictly upon the formal request of SLT or the DSL. IT Support staff are not alerted to safeguarding triggers and do not proactively monitor student behaviour.

Pupils: Pupils must never attempt to 'jailbreak' or bypass the safety filters on our AI tools. Deliberately tricking an AI system into generating illegal, offensive, or harmful content is a breach of our Acceptable Use Policy

10. Fake news, Misinformation and Disinformation

Misinformation is information that is not true but it is shared and created without the intent to mislead.

Disinformation is information that is not true and is shared and created with the intent to deceive and mislead.

'Fake news' is a term commonly used to describe disinformation and misinformation that is being presented and shared as reputable news.

Misinformation and disinformation are utilised by a range of individuals and organisations, including political groups and extremists. They can use technology to make their content look like it has come from a trusted source and is backed up by factual evidence, and they can create numerous social media accounts to spread disinformation across the internet, making the content go viral. Through the use of things like predictive algorithms, these views can be spread directly to individuals who are most likely to spread and reinforce those messages.

Misinformation and disinformation can mislead children, leading to a range of potential harms – including spreading hatred, intolerance, and mistrust. Extremists utilise disinformation, misinformation, and conspiracy theories to help gain increased exposure for their ideas, as well as attracting those with personal grievances who may be susceptible to their hateful narratives.

Through their PSHE lessons, pupils are taught to recognise:

- online content which tries to make people believe something false is true or mislead (misinformation and disinformation)
- techniques that companies use to persuade people to buy something

- ways in which criminals may try to defraud people online
- ways in which games and social media companies try to keep users online longer (persuasive or sticky design)
- grooming and manipulation techniques used by criminals
- ways to protect themselves from a range of cyber crimes

11. Artificial intelligence

The school recognises that generative Artificial Intelligence (AI) tools are an increasing part of the digital landscape. Our approach is to enable the safe, responsible, and ethical use of these tools for both staff and pupils, in line with our statutory safeguarding duties.

Governance and Statutory Compliance

- **DfE Guidance:** The school adheres to the Department for Education's (DfE) statutory guidance, *Keeping Children Safe in Education (KCSIE)*, and the supporting advice, *Generative AI: product safety expectations*.
- **Mandatory Annual Review (KCSIE):** The Governing Body must document a review of the effectiveness of the school's filtering and monitoring systems, specifically as they apply to generative AI use, at least once every academic year.
- **Cyber Security Duty (KCSIE):** Safeguarding records and child data are now core safeguarding concerns. Compromised data is viewed as an immediate risk to child wellbeing, shifting the management of information security and cyber security from an IT-only task to a core responsibility of the DSL and Senior Leadership Team.

Filtering, Monitoring, and Security

Application of Existing Infrastructure:

- Any use of generative AI tools accessed via school-managed devices or while signed into a school account is subject to the existing filtering and monitoring system (Securly).
- Services like ChatGPT and Grok are blocked for all students across the trust. Gemini is turned off for primary schools and on for secondary schools.
- The Securly sandbox and AI chrome browser extension allows us to alert DSLs to harmful / inappropriate interactions with AI and block students trying to access other 'well known' AI platforms, redirecting them to the sandbox, enabling students to use AI in a safer space.

- **Data Protection:** Staff and pupils **must not** input any personally identifiable information (PII), confidential information, or sensitive data (including student or staff names) into external, public-facing generative AI tools. A pupil's original work (like essays or artwork) belongs to them and must not be uploaded into public AI tools for marking or feedback without explicit permission.
- **System Integrity:** AI products used within the school environment must offer robust protection against unauthorised functional modifications.

School Photography and Image Scraping

While we use our public platforms to share school news and achievements, we are highly aware of the digital risks associated with publishing images online. These risks include location tracking and the automated harvesting (scraping) of photos to generate AI deep fakes.

To protect pupil privacy, the school/trust enforces the following measures for all published photography:

- **Anonymity:** We do not pair clear facial photos with a pupil's full name, preventing bad actors from identifying and targeting specific students, unless explicitly permitted by the parents/carers and the student.
- **EXIF Data Stripping:** We remove all hidden location metadata (such as GPS coordinates) from photos prior to uploading to protect physical safety and location privacy.
- **Parental Consent:** We operate a strict opt-in policy. A child's image will only be published on public-facing school platforms if positive, explicit consent has been granted by their parent or carer

Educational Risks and Acceptable Use

All use of generative AI is governed by the **Staff Acceptable Use Policy** and the school's **Pupil acceptable use agreements**.

Pupils must be educated on the critical risks associated with AI outputs and interaction, including:

Misinformation and Disinformation: AI can produce content that is factually inaccurate, misleading, or designed to deceive, reinforcing the need for critical analysis skills covered in PSHE lessons.

Bias and Stereotyping: AI models may perpetuate or amplify existing societal biases and stereotypes, which pupils must be taught to recognise and challenge.

Harmful Outputs: Pupils must not prompt AI models to generate illegal, offensive, or harmful content.

Digital Footprints: Pupils must understand that interactions with AI tools create a data trail, and they must protect their personal digital footprint.

Pupils must never attempt to 'jailbreak' or bypass the safety filters on our AI tools. Deliberately tricking an AI system into generating illegal, offensive, or harmful content is a breach of our Acceptable Use Policy

Emotional Attachment: Pupils must be mindful of forming inappropriate or overly deep emotional attachments to AI chatbots, which can create risks relating to manipulation or reliance. Some tools are designed in ways that actively encourage pupils to form emotional connections with them. This matters as it can substitute for human relationships and bypass the kind of trusted adult contact that sits at the heart of effective safeguarding.

We will provide a variety of methods for pupils to raise any concerns they have about any matter with a trusted adult. Pupils will only be able to access apps or online tools offering mental health interventions which claim to diagnose, treat, manage or intervene in a mental health condition via the schools internet systems which are regulated by the Medicines and Healthcare Products Regulatory Agency.

Cognitive Offloading. This occurs when pupils use AI to do the hard work and thinking for them. Note that this is now officially recognised as a safeguarding concern because it prevents pupils from developing their own skills, hides when they are struggling, and can reduce the chances of them seeking help from a trusted human adult.

Pedagogical Standards: AI tools designed for use in learning should avoid the anthropomorphisation of AI products (e.g., refraining from using "I-statements" or implying consciousness) to mitigate emotional harms.

12. AI Deepfakes as Child-on-Child Abuse

Deep Fakes are images, videos, or audio—created using artificial intelligence (AI) to convincingly replace a person's likeness, voice, or movements with someone else's.

In line with the KCSIE 2026 Draft (Part 1, para 34), the definition of child-on-child abuse now explicitly includes AI-generated images and/or videos (deepfakes).

Any incident involving the creation or circulation of self-generated intimate images or videos, including those created using AI, will be treated as

child-on-child abuse, reported to the police if illegal, and responded to in line with the safeguarding and behaviour for learning policy.

Under the **Crime and Policing Act 2026**, the creation, adaptation, or supply of "nudification" apps - tools that use AI to digitally remove clothing from images of real people - is now a criminal offence and will be reported to the Police.

At our school we will remain alert to this issue and deliver staff training and teach pupils through the computing and PSHE curriculum and assemblies. The use of AI tools will be included as part of our ongoing review of Online activity.

13. 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 Behaviour for Learning Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Code of Conduct and Disciplinary Policy. 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.

14. 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 throughout the year. 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.

The DSLs will undertake Level 3 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 annual safeguarding training.

15. Resources, guidance, and support

The Department for Education has published advice on how to teach online safety in schools, including around teaching about disinformation and misinformation. This includes ensuring that learners know how to measure and check authenticity online, and the potential consequences of sharing information that may not be true.

[Teaching online safety in schools](#)
[Online Media Literacy Resources](#)

Educate Against Hate has a number of resources that can help staff and parents understand more about fake news, misinformation, and disinformation, and how to effectively teach young people about media literacy, critical analysis, and how to manage news from online sources:

- [Be Internet Citizens – Educate Against Hate](#)
- [Be Internet Legends – Educate Against Hate](#)

- [Identifying the Difference Between Fact and Opinion – Educate Against Hate](#)
- [Trust Me – Educate Against Hate](#)
- [Reliable News – Educate Against Hate](#)
- [Managing Feelings About the News – Educate Against Hate](#)

Resources focusing on fact and opinion, the news and identifying reliable sources are used during PSHE and assemblies in order to facilitate discussions around what young people might encounter in the news and providing them with the opportunity to learn about how to sensitively and confidently navigate their feelings and emotions around content that may be factually inaccurate

Support and resources are also available from:

- the [CEOP Thinkuknow Programme](#)
- the [NCA's Click CEOP](#)
- [National Centre for Computing Education \(NCCE\)](#)
- [UK Council for Internet Safety](#)
- [Education for a Connected World](#)

Schools can also get advice from national organisations such as:

- [Anti-Bullying Alliance](#)
- [Association for Citizenship Teaching](#)
- [Childnet](#)
- [The Diana Award](#)
- [DotCom Charity](#)
- [Hopes and Streams](#)
- [Internet Matters](#)
- [Internet Watch Foundation](#)
- [NSPCC learning](#)
- [Parent Zone's school resources](#)
- [PSHE Association](#)
- [SWGfL](#)
- [UK Safer Internet Centre](#)

You can refer parents to the following national organisations for support:

- [Internet Matters](#)

- [NSPCC](#)
- [Parent Zone](#)

You can refer pupils to the following national organisations for support:

- [BBC Own It](#)
- [Childline](#)

Monitoring arrangements

The Safeguarding Team will log and monitor behaviour and safeguarding issues related to online safety on CPOMS.

This policy will be reviewed every year by the RLT Safeguarding Lead, RLT IT Director and School Governors.

16. Appendices

 **ARCHIVED Staff IT Acceptable Use Policy - review July 2026**

