The Parkside School
E-Safety Policy

Approved by:	Mr Paul Stanley Chair of Governors	**Date:**	January 2026
Signed:			
Next review due: **by:**	January 2027 Kirsty Lofty		

Rationale

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk, especially those with special educational needs, within and outside the school. Our approach is to identify and support pupils who are potentially at greater risk of harm online than others. It is impossible to eliminate those risks completely; therefore, it is essential, through good educational provision, to build our pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Risks faced by young people online include:

- Access to illegal, harmful or inappropriate images or other content. This includes, but is not limited to, misinformation, disinformation (including fake news), racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
- Unauthorised access to / loss of / sharing of personal information
    - The risk of being subject to grooming by those with whom they make contact on the internet, including adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
    - The risk posed by Artificial Intelligence (AI), including deepfakes (videos and photos created to look real) and AI chatbots that may create fake intimacy or offer harmful advice.
    - The sharing / distribution of personal images without an individual's consent or knowledge. This includes the severe risks and potential criminal consequences of acquiring, generating, keeping, or forwarding indecent or sexual images of someone under 18, even if the photo is of themselves or was AI-generated.
- Inappropriate communication / contact with others, including strangers.
- Risk of Criminal exploitation e.g. county lines/Incel culture/radicalisation

- Cyber-bullying/ peer on peer abuse / inappropriate social development, which can escalate conflicts and utilize technology and social media for harassment and stalking.
- Access to unsuitable video / internet games, including risks related to online gambling, video game monetisation, and scams.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this policy is used in conjunction with and supported by other school policies (e.g. RSHE, behaviour, anti-bullying).The breadth of issues classified within online safety is considerable, but aligns with the four areas of risk identified in statutory safeguarding guidance 'Keeping Children Safe in Education':

1. Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
2. Contact: being subjected to harmful online interaction with other users; for example: 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'.
3. Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying: and
4. Commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams, including sextortion

(DfE Keeping Children Safe in Education 2025)

Development and Monitoring

This E-safety policy has been developed by the-RSHE, E-safety and Pupil Wellbeing lead and the Designated Safeguarding Lead in conjunction with the School Leadership team. As part of this policy, records will be maintained of E-Safety related incidents involving staff and pupils and any incidents recorded will be

treated in accordance with our safeguarding procedures. This policy will be reviewed at least annually.

Roles and Responsibilities

The key roles involved in the E-Safety Policy are:

Designated Safeguarding Lead : John Habershon:

The DSL takes lead responsibility for online safety in school. Responsibilities include:

•The DSL/RSHE lead takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.
• The DSL ensures that the filtering and monitoring systems are understood, working effectively, and reviewed regularly, reporting to the Governing Body for assurance.
• They receive reports of e-safety incidents and maintain a log of incidents to inform future e-safety developments (see Appendix 5 in the model policy).
• They undertake annual risk assessments that consider and reflect the risks pupils face, given that technology and related harms evolve rapidly.
• They manage all online safety issues and incidents in line with the school's child protection policy.
• They provide training and advice for staff and liaise with the Local Authority where necessary

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing its effectiveness. They will ensure all staff undergo online safety training as part of child protection and safeguarding training. They must also ensure that the school has appropriate filtering and monitoring systems in place on school devices and networks, and will regularly review their effectiveness, discussing with IT staff and service providers what is needed to meet DfE standards. Governors will monitor online safety logs as provided by the DSL.

The Computing Co-ordinator, RSHE, E-safety and Pupil Wellbeing lead and Designated Safeguarding Leads:

- Are responsible for the implementation and effectiveness of this policy. They are also responsible for reporting to the Governing Body on the effectiveness of the policy and, if necessary, make any necessary recommendations for further improvement.
- Take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies / documents

- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Report any serious breaches of the E-Safety Policies
- Provide training and advice for staff
- Liaise with the Local Authority where necessary
- Receive reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Are trained in and share with staff awareness and understanding of e-safety issues and the potential for serious child protection issues that can arise.

Teaching and Support Staff

- Teaching and Support Staff are responsible for ensuring that:
- They have an up to date awareness of e-safety matters and of the current school e-safety policy.
- They have read and understood the E—Safety policy, Mobile policy and Use of AI Policy
- They report any suspected misuse or problem to a designated Safeguarding Lead for investigation. (CPOMS)
- Digital communications with pupils and parents / carers (email are on a professional level)
    - Acting as good role models in their use of ICT, the internet and mobile devices.
    - Working with the DSL to ensure any online safety incidents are logged and dealt with appropriately.
    - Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline.
    - Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes

Pupils

- Pupils understand and follow the Parkside computer use rules and, where possible, school e-safety policy
- Pupils know how they can report abuse, misuse or inappropriate materials
- Understand that the school's E-Safety Policy covers their actions out of school, if related to another pupil, where appropriate for age and ability.

Education - Pupils

E-Safety education is provided in a comprehensive, differentiated, and inclusive manner, appropriate to pupils' age, ability, and developmental stage (Year 3 to Year 13). Given that our pupils have SEND, teaching is adapted for vulnerable children to ensure a more personalised or contextualised approach.

- The school's e-safety curriculum is integrated as part of Computing/ RSHE as well as other lessons.
- Key e-safety messages are continually reinforced throughout the school.
- Staff act as good role models in their use of ICT, the internet and mobile devices
- Pupils are allowed to search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites that are visited. Filters are in place to ensure pupils can only access appropriate content.

The curriculum is structured using the PSHE Association Education Planning Framework for Pupils with SEND (Key Stages 1–4), which allows staff to map content and differentiate learning using progressive stages (Encountering, Foundation, Core, Development, Enrichment, Enhancement). Online safety is explicitly covered in the *Self-Care, Support and Safety* and *The World I Live In* sections of the framework. The curriculum draws on high-quality, evidence-based resources:

1. Life Lessons Curriculum: Used to provide coverage for all statutory content, emphasizing an evidence-based, peer-led, and relational approach. These resources are designed to be inclusive, employing dual coding, scaffolding activities, word banks, and emotions characters to support pupils with SEND.

2. POL-ED: Resources are utilised across Key Stages (Year 3–13) to cover themes such as Relationships, Keeping Safe, Understanding the Law, and Well-being. This includes specific lessons relevant to online behaviour, such as:

- ◦ "How can I keep safe online?" (Year 2 content, adaptable for foundational needs)
- ◦ "What can and can't I do on the internet?" (Year 5)
- ◦ "Are we responsible with social media?" (Year 8)
- ◦ "What are deep fakes?" (Year 8)
- ◦ "What is phishing and hacking?" (Year 8)
- ◦ "How do we manage cyber security?" (Post-16)

3. NSPCC Keeping Children Safe Online: Used to access advice and activities tailored for families and children with SEND, focusing on helping young people make friends and stay safe online.

4. Common sense Media: addresses critical issues facing children in a fast-changing world of media and technology. The innovative lessons teach students to think critically and develop the habits of mind to navigate digital dilemmas in their everyday lives. They use six core topics; Media balance and wellbeing; privacy and security; digital footprint and identity; relationships and communication, cyberbullying, digital drama and hate speech, News and media literacy

5. Natterhub: Natterhub provides fun and interactive online safety learning for children
6. Childnet: Childnet works directly with children and young people from the ages of 3-18, as well as parents, carers, teachers and professionals, finding out about their real experiences online and the positive things they are doing. Working directly with these audiences is important in helping us to equip them to stay safe online and informs the resources that we develop for them

Content Coverage (Aligning with 2025 RSHE Statutory Guidance for Y3–13):
The school's e-safety curriculum is integrated into RSHE, Computing, and other relevant lessons, ensuring pupils cover both primary (KS2) and secondary (KS3/4) statutory expectations by the time they leave school.
Key areas covered by the end of primary (Year 6) must include:

- Using technology safely and respectfully, keeping personal information private.
- Identifying where to go for help and support when concerns arise about content or contact.
- Understanding the risks associated with people they have never met online and recognizing harmful content or contact.

- Knowing that there is a minimum age for joining social media sites (currently 13).
- Recognizing that any material shared online might be circulated permanently.

Key areas covered by the end of secondary (Year 13) must be progressive and include:

- Understanding rights and responsibilities online, and that the same expectations of behaviour apply as offline.
- Using privacy and location settings appropriately.
- Recognising characteristics of social media, including that accounts may be fake or created with AI.
- Understanding the law regarding sharing explicit images (including AI-generated imagery) of someone under 18 being a crime, even if consented to, and knowing how to seek support without fear of blame.
- Learning about the prevalence of deepfakes and how to identify them.
- Identifying online risks such as inappropriate content (misogyny, violence), online scams (phishing, sextortion), and the risks associated with AI chatbots.

Education - Parents

The school will continue to provide information and awareness to parents and carers, recognising their essential role in monitoring and regulating children's online experiences.

- Information is provided through letters, emails, the school website, and online learning opportunities.
- The school ensures transparency by letting parents know what systems the school uses to filter and monitor online use, and what sites their children access.
- Parents and carers will be signposted to key external resources for advice, including:

Common Sense Media: For age-based media reviews, guidance on digital parenting, social media, and parental controls and information on AI Companions and Generative AI.

2. **NSPCC Keeping Children Safe Online for Families and Children with SEND:** Provides specific online safety tips, advice, and activities, developed in partnership with Ambitious about Autism, tailored for parents and carers of children with SEND. This includes activities focusing on sharing personal details, online friendships, and cyberbullying.

Acceptable use of the internet in school

- 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.
- If necessary the school can monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.
- Parkside uses securely, a cloud-based web-filtering system, across the school to provide a safe internet environment for staff and students alike. This system provides appropriate filtering and produces activity logs for designated staff for serious activity that requires investigation. Filtering and monitoring systems are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content.

Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are **not** permitted to use them during:

- Lessons
- Clubs before or after school, or any other activities organised by the school, unless explicitly permitted by staff for an educational activity

Staff may ask to see a pupil's mobile device to support any ongoing e-safety issues. Staff have the right to retain or confiscate mobile phones, or other online technologies, if there is deemed to be a justifiable safeguarding risk, in line with statutory guidance on searching, screening, and confiscation.

Misuse and Consequences
Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour and safeguarding policies. If inappropriate material is found, the DSL/Headteacher will decide on a suitable response. If the material relates to an indecent image of a child, staff must not view the image and must report it immediately to the DSL in line with statutory guidance

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
- 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 promptly installing the latest updates
    - Read and follow the schools mobile device policy for more information

Training and Monitoring
Staff Training
All new staff members receive training on safe internet use and online safeguarding issues as part of their induction. All staff receive refresher training and updates at least once each academic year as part of safeguarding training. This training ensures staff are aware of:
• The significant component technology plays in safeguarding issues.
• How children can abuse peers online (e.g., sharing abusive or indecent images).
• How to spot the signs and symptoms of online abuse.
• The procedure for logging incidents

The DSL and deputies undertake child protection and safeguarding training, including online safety, at least every 2 years, and update their online safety knowledge annually.

Monitoring Arrangements The DSL logs behaviour and safeguarding issues related to online safety, using the internal incident log. This policy is reviewed annually by the RSHE, E-safety and pupil wellbeing lead, supported by an annual risk assessment that considers and reflects the rapidly evolving risks pupils face online.
Links with other policies
This online safety policy is linked to our:
• Child protection and safeguarding policy
• Behaviour policy
• Staff disciplinary procedures
• Data protection policy and privacy notices

- Complaints procedure
- Parkside Relationship and Sex Education Policy
- ICT and internet acceptable use policy
    - Mobile phone Policy
    - Use of AI policy