Online Safety Policy

Little Explorers is aware of the rapid growth of the internet and the advantages this brings to education and communication. However, we are also aware of the dangers it can pose. We are committed to supporting children, staff, and families to use the internet safely and responsibly.

This policy is underpinned by current legislation and safeguarding guidance, including Safeguarding children and protecting professionals in early years settings: online safety considerations, the Statutory Framework for the Early Years Foundation Stage, Keeping Children Safe in Education, and Working Together to Safeguard Children, ensuring our approach reflects the latest expectations for keeping children safe.

The Designated Safeguarding Lead (DSL) is ultimately responsible for online safety. Any concerns must be raised with the DSL or Deputy Designated Safeguarding Lead (DDSL) as soon as possible.

The use of technology is a significant component in many safeguarding issues including child sexual exploitation, radicalisation, and sexual predation. Technology often provides the platform that facilitates harm.

This policy applies to:

- Staff
- Children
- Parents
- Visitors
- Contractors

Online Safety Risk Areas

Online safety risks are commonly grouped into the following four categories:

- **Content:** Being exposed to illegal, inappropriate, or harmful material (e.g., pornography, fake news, racist or extremist views).
- **Contact:** Harmful online interaction with other users (e.g., commercial advertising, grooming, impersonation).
- **Conduct:** Personal online behaviour that increases the likelihood of harm (e.g., cyberbullying, sharing explicit content).
- **Commerce:** Exposure to scams, in-app purchases, phishing attempts, or fraudulent advertising.

Measures in Place

To keep children, staff, and families safe online, we:

- Install and regularly update appropriate antivirus and anti-spyware software on all devices.
- Use content blockers and filters on all internet-connected nursery devices.
- Ensure all devices are password protected with complex passwords that are changed regularly and stored securely.
- Monitor all internet usage across the setting.
- Securely store all nursery devices at the end of each day.
- Prohibit installation of social media or messaging apps on nursery devices.
- Review all apps and games to ensure age-appropriate content.
- Use only nursery devices for photographing or recording children.
- Report inappropriate emails to the Internet Watch Foundation (www.iwf.org.uk).
- Teach children how to stay safe online and how to report concerns.
- Supervise children when using internet-connected devices.
- Use tracking software to monitor suitability of internet usage (where age-appropriate).
- Restrict staff and visitor access to nursery Wi-Fi.
- Discuss online 'stranger danger' with children and compare online friends to real-life acquaintances.
- When using video calls (e.g., Team, Zoom or FaceTime), discuss safe contact practices with children. Only approved platforms used, Parental consent required, No 1:1 unsupervised video interactions, Calls must be recorded or logged where appropriate.
- Ensure staff model safe technology use and adhere to our Acceptable IT Use Policy.
- Monitor children's screen time to ensure it remains age-appropriate, purposeful, and supports learning.
- Consider physical safety including posture when using devices.
- Manage our digital reputation and ensure staff understand their responsibilities online.
- Require all communication with families to occur via nursery channels (official email and phone).
- Signpost parents to appropriate online safety support and resources.

- Promote national online safety initiatives such as Safer Internet Day.
- Prohibit the use of personal mobile phones or smart devices by staff in areas where children are present.

Staff behaviour outside work (professional conduct)

Staff must not:

- Accept parents on social media
- Discuss nursery children online
- Share identifiable information

Use of Images and Digital Media

- Parental consent must be obtained before taking or using images
- No staff personal devices used for photos
- Images must never be shared on personal social media
- Secure storage and deletion procedures
- Clear rules around apps (e.g. Ovivio) - please see our Ovivio Use Policy.

Responding to Online Safety Concerns

If concerns arise:

- The safeguarding policy will be followed.
- All concerns must be reported to the DSL (Designated Safeguarding Lead).

The DSL (Designated Safeguarding Lead) will ensure:

- All staff know how to report and escalate concerns, including external referrals.
- All concerns are logged, assessed, and acted upon in line with safeguarding procedures.
- Parents are supported to develop awareness and confidence in managing online safety at home.
- Staff have access to up-to-date information and guidance to support online safety personally and professionally.
- Under no circumstances should any staff member access, download, possess, or distribute illegal materials, including child sexual abuse material.

Concerns may be reported to:

- DSL
- Local Authority
- NSPCC whistleblowing helpline

Illegal content must be reported to:

- Police
- Internet Watch Foundation

Online safety is included in:

- Induction
- Safeguarding training updates
- DSL training

Artificial Intelligence (AI) & emerging tech

- Staff must not input personal/confidential data into AI tools
- AI-generated content must be checked for accuracy and appropriateness
- Children must not access AI tools unsupervised

Please see our AI Policy for more information.

Cyber Security

This policy should be read in conjunction with our:

- Data Protection and Confidentiality Policy
- Acceptable IT Use Policy
- GDPR Privacy Statement
- UK GDPR and Data Protection Act 2018
- Personal data must be:
    - Processed lawfully
    - Stored securely
    - Accessed only when necessary
-

To ensure robust cyber security, we:

- Recognise that childcare settings are targets for cybercrime.
- Remind staff of the value and sensitivity of the information we hold.
- Encourage regular backups of sensitive data.
- Use strong, secure passwords.
- Maintain device protections.
- Warn staff not to open suspicious messages (e.g., those about resetting passwords, compensation offers, or missed deliveries).
- Instruct staff to report suspicious messages to management.

- Report phishing attempts via the NCSC Suspicious Email Reporting Service (report@phishing.gov.uk).

Appropriate filtering and monitoring systems

- Named responsibility (Manager/DSL oversees filtering systems)
- Regular review of filtering effectiveness
- Immediate action if safeguarding breach detected

Online safety is embedded across our safeguarding culture and is considered in all aspects of teaching, learning, and daily practice.

This policy is reviewed annually or sooner if new guidance is issued.

This policy was adopted on	**Revised**
24/01/2022	*4th May 2026*