Online Safety Policy

EYFS: 3.1-3.8

Little Learners Nursery is aware of the significance of the internet in our society and the advantages this can bring. However, it is also aware of the dangers it can pose and we strive to support children, staff and families to use the internet safely.

We refer to the UK Council for Internet Safety's 2019 document Safeguarding Children and Protecting Professionals in Early Years Settings: Online Safety Guidance for Practitioners to support this policy.

The Designated Safeguarding Lead, Joanne Spalding, is ultimately responsible for online safety concerns. All concerns need to be raised as soon as possible to her.

The use of technology has become a significant component of many safeguarding issues. It provides the platform that facilitates harm in the areas of child sexual exploitation; radicalisation; sexual predation and more.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material, for example, pornography, fake news, racist or radical and extremist views
- Contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults
- Conduct: personal online behaviour that increases the likelihood of, or causes, Harm, for example making, sending and receiving explicit images, or online bullying.

Within the nursery we aim to keep children, staff and parents safe online. Our safety measures are:

- Ensuring we have appropriate antivirus and anti-spyware software on all devices and update them regularly
- Ensuring content blockers and filters are on all our devices, e.g. computers, laptops, tablets and any mobile devices
- Ensuring all devices are password protected and have screen locks. Practitioners are reminded to use complex strong passwords and they are kept secure and are not written down
- Monitoring all internet usage across the setting
- Providing secure storage of all nursery devices at the end of each day
- Ensuring no social media or messaging apps are installed on nursery devices
- Reviewing all apps or games downloaded onto devices to ensure they are age and content appropriate
- Using only nursery devices to record/photograph children in the setting
- Never emailing personal or financial information

- Reporting emails with inappropriate content to the internet watch foundation (IWF www.iwf.org.uk)
- Teaching children how to stay safe online and reporting any concerns they have
- Ensuring children are supervised when using internet connected devices
- Not permitting staff or visitors access to the nursery Wi-Fi for any use unrelated to the daily operation of the nursery
- When using face to face platforms (e.g. Skype or FaceTime), discussing with the children what they would do if someone they did not know tried to contact them
- Providing training for staff, at regular intervals, in online safety and understanding how to keep children safe online.
- Modelling safe practice when using technology with children
- Ensuring all staff abide by an acceptable use policy
- Instructing staff to use the work IT equipment for matters relating to the children and their education and care. No personal use will be tolerated (see acceptable IT use policy)
- Monitoring children's screen time to ensure they remain safe online and have access to material that promotes their development. Ensuring that their screen time is within an acceptable level and is integrated within their programme of learning
- Being aware of the need to manage our digital reputation, including the appropriateness of information and content that we post online, both professionally and personally. This is continually monitored by the setting's management
- Ensuring all electronic communications between staff and parents is professional and takes place via the official nursery communication channels, e.g. the setting's email addresses and telephone numbers. This is to protect staff, children and parents
- Signposting parents to appropriate sources of support regarding online safety at home

If any concerns arise relating to online safety, then we will follow our safeguarding policy and report all online safety concerns to the DSL.

The DSL will make sure that:

- All staff know how to report a problem and when to escalate a concern, including the process for external referral
- All concerns are logged, assessed and actioned in accordance with the nursery's safeguarding procedures
- Parents are offered support to help them talk about online safety with their children using appropriate resources
- Parents are signposted to appropriate sources of support regarding online safety at home and are fully supported to understand how to report an online safety concern.
- Staff have access to information and guidance for supporting online safety, both personally and professionally
- Under no circumstances any member of staff, either at work or in any other place, makes, deliberately downloads, possesses, or distributes material they know to be illegal or harmful.

Cyber Security

This policy should be read in conjunction with our Data Protection and Confidentiality Policy, Acceptable IT Use Policy and GDPR Privacy Statement.

Good cyber security means protecting the personal or sensitive information we hold on children and their families in line with the Data Protection Act. We are aware that cyber criminals will target any type of business including childcare and we ensure all staff are aware of the value of the information we hold in terms of criminal activity e.g. scam emails. All staff are reminded to follow all of the procedures above including backing up sensitive data, using strong passwords and protecting devices to ensure we are cyber secure.

To prevent any attempts of a data breach (which is when information held by a business is stolen or accessed without authorisation) which could cause temporary shutdown of our setting as well as our reputational damage with the families we engage with, we inform staff not to open any suspicious messages including official-sounding messages about 'resetting passwords', 'receiving compensation', 'scanning devices' or 'missed deliveries'.

Staff are asked to report these to the manager as soon as possible and these will be reported through the National Cyber Security Centre (NCSC) Suspicious Email Reporting Service at report@phishing.gov.uk

This policy was adopted on	Signed on behalf of the nursery	Date for review
19th April 2024		*19th April 2025*