Online Safety Policy (example)

EYFS: 3.4-3.7

Our nursery is aware of the growth of internet 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.

Keeping Children Safe in Education categorises online safety into three areas of risk:

- ✓ *Content: being exposed to illegal, inappropriate or harmful material*
- ✓ *Contact: being subjected to harmful online interaction with other users; and*
- ✓ *Conduct: personal online behaviour that increases the likelihood of, or causes, harm."*

The Designated Safeguarding Lead is ultimately responsible for online safety concerns. All concerns need to be raised as soon as possible to **[insert DSL name].**

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm.

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; and
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 include:

- Ensuring we have appropriate antivirus and anti-spyware software on all devices and update them regularly
- Ensure content blockers and filters are on all our devices, e.g. computers, laptops, tablets and any mobile devices
- Ensuring all devices are password protected. Passwords should be kept safe and secure, changed regularly 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 ensuring 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 report any concerns they have
- Ensuring children are supervised when using internet connected devices
- Using tracking software to monitor suitability of internet usage (for older children)
- Not permitting staff or visitors to access to the nursery Wi-Fi
- Talking to children about 'stranger danger' and deciding who is a stranger and who is not; comparing people in real life situations to online 'friends'
- When using Skype and FaceTime (where applicable) discussing with the children what they would do if someone they did not know tried to contact them
- Providing training for staff, at least annually, in online safety and understanding how to keep children safe online. We encourage staff and families to complete an online safety briefing, which can be found at https://moodle.ndna.org.uk
- 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)
- Children's screen time is monitored to ensure they remain safe online and have access to material that promotes their development. We will ensure that their screen time is within an acceptable level and is integrated within their programme of learning
- The nursery is 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
- All electronic communications between staff and parents should be professional and take 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.

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 supported to develop their knowledge of online safety issues concerning their children via **[insert examples from own nursery]**
- 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 should any member of staff, either at work or in any other place, make, deliberately download, possess, or distribute material they know to be illegal, for example child sexual abuse material

This policy was adopted on	**Signed on behalf of the nursery**	**Date for review**
[Insert date]		*[Insert date]*