

# ONLINE SAFETY AND CYBER SECURITY POLICY



Stepping Stones

Updated: June 2022

Our nursery is aware of the growth of the 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.

We refer to 'Safeguarding children and protecting professionals in early years settings: online safety considerations' to support this policy.

The Designated Safeguarding Lead is ultimately responsible for online safety concerns. All concerns need to be raised as soon as possible to Tania Sandhu or Nisha Gaj.

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
- 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 screen locks. Practitioners are reminded to use complex strong passwords and they are 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 by ensuring the property is locked at the end of each day
- Ensuring no social media or messaging apps are installed on nursery devices, unless used for communication purposes with parents only.
- 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](http://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 private 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'
- Providing training for staff, at least every two years, 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/>
- Staff model safe practice when using technology with children and 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. We ensure that their screen time is within an acceptable level and is integrated within their programme of learning
- Making sure physical safety of users is considered including the posture of staff and children when using devices
- 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 supported to develop their knowledge of online safety issues concerning their children via **online briefings (link shared within this policy)**.
- Parents can approach us for support to help them talk about online safety with their children using appropriate resources
- Parents can request appropriate sources of support regarding online safety at home and guidance on 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.

## **Cyber Security**

This should be read in conjunction with the 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 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 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) that could cause temporary shutdown of our setting and reputational damage with the families we engage with we inform staff not to open any suspicious messages such as 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 NCSC Suspicious Email Reporting Service at [report@phishing.gov.uk](mailto:report@phishing.gov.uk)