# Online Safety Policy

This policy should be read in conjunction with the Data protection and confidentiality policy, Acceptable internet use policy and General Data Protection Regulation (GDPR) privacy notice. 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 Heather Black.

The use of technology has become a significant component of many safeguarding issues such as child sexual exploitation, radicalisation and sexual predation with technology often providing the platform that facilitates harm. The breadth of issues included 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 have screen locks. We use complex strong passwords, keep them safe and secure, change them regularly and not to write them 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 and /or 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

• Ensuring that staff do not to use personal electronic devices with imaging and sharing capabilities, including mobile phones, smart watches and cameras

• Not permitting staff or visitors 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 annually, in online safety and understanding how to keep children safe online. We encourage staff and families to complete a free online safety briefing, which can be found at https://moodle.ndna.org.uk/

• Staff modelling safe practice when using technology with children and ensuring all staff abide by an acceptable use policy such as instructing staff to use the nursery IT equipment for matters relating to the children and their education and care only. No personal use will be tolerated (see Acceptable internet 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 the 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 is posted online, both professionally and personally. This is continually monitored by the setting's management

• Staff must not friend or communicate with parents on personal devices or social media accounts

• 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 children and child protection 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 regular information sharing.

• 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.

Cyber Security

This policy should be read in conjunction with the Data protection and confidentiality policy, Acceptable internet use policy and GDPR privacy notice. 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 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 |
|---|---|---|
| 01/03/2026 | Heather Black | 01/03/2027 |