**Online Safety Policy**

|  |
| --- |
| EYFS: 3.1-3.8 |

Providers are responsible for ensuring they follow the current version of the framework for their provider type.

This policy should be read in conjunction with the Data protection and confidentiality policy, Acceptable internet use policy and GDPR privacy notice.

Our nursery is aware of the growth of internet use and the advantages this can bring. However, it is also aware of the dangers it can pose and strives to support children, staff and families in using 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 **Kaneez Ur Rehman & Arooj Khan**

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.

Keeping Children Safe in Education states *“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. Keeping passwords safe and secure, not sharing or writing these down. Practitioners are reminded to use complex strong passwords so they are kept safe and secure. These will be changed at least every term to keep the devices secure and will not be written down anywhere and be kept safe with the practitioner.
* Ensure management monitor all internet activities in the setting
* Locking away all nursery devices at the beginning of the day, unless otherwise agreed upon i.e. Need to access the phone at all times for the purposes of staying in contact with children. If permission is not granted and the phone were to ring, the phone will not be picked up. However upon constant ringing, indicating an emergency, management will tell the staff members to access the phone, ensuring children ratio is not compromised upon. The phones can be accessed at the end of the day or during lunch time, away from the children.
* Ensuring no social media or messaging apps are installed on nursery devices apart from the nursery’s WhatsApp to be able to send broadcasted messages, and Instagram to make relevant posts and use it as a medium to engage the parents with Lote Tree Nursery Ltd.’s updates as well as a form of communication.
* Management reviewing all apps or games downloaded to tablets to ensure all are age appropriate for children and safeguard the children and staff
* Using approved devices to record/photograph 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 access to the nursery Wi-Fi
* Integrating online safety into nursery daily practice by discussing computer usage ‘rules’ deciding together what is safe and what is not safe to do online
* 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
* Provide 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](https://moodle.ndna.org.uk/course/index.php?categoryid=27)
* Staff model safe practise when using technology with children and we ensure that all staff abides by an acceptable use policy; instructing staff to only 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)
* 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
* Children’s screen time is monitored 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 and should be professional and takes place via the official nursery communication channels, e.g. the setting’s email addresses and telephones 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 upon using the Nursery’s Safeguarding procedures
* Parents are supported to develop their own knowledge of online safety issues concerning their children via Lote Tree Nursery Ltd. Sending articles on the topic of how to keep children and themselves safe online. Furthermore, the nursery mentions briefly during the gradual admission process how children are and can be safeguarded online. In addition, we ensure to let the parent know that it is their responsibility as well by also giving them a “Stay safe online” leaflet with their welcome pack.
* 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 or pornography material.
* The Professionals Online Safety Helpline (0344 381 4772 or [helpline@saferinternet.org.uk](mailto:helpline@saferinternet.org.uk)) is shared with all staff and used if any concerns arise
* Refer to <https://www.gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations-for-managers> to ensure all requirements are met in order to keep children and staff safe online
* Share <https://www.gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-guidance-for-practitioners> with the wider team to help them to keep themselves safe online, both personally and professionally

**Cyber Security**

***This policy should be read in conjunction with your 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’.

The management ensures that the topic of cyber security is covered during Training sessions, which take place termly so all staff is aware and updates regarding what to do. Articles and advice related to cyber security will also be sent to the parents via WhatsApp or email, or whatever form of communication is available to the parent.

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)

|  |  |  |
| --- | --- | --- |
| **This policy was adopted on** | **Signed on behalf of the nursery** | **Date for review** |
| *04/09/2024* | *KANEEZ UR REHMAN* | *04/09/2024* |