Online Safety
Child protection

The growth of Internet use brings advantages and disadvantages. Here, at Twinkle Toes Day Nursery, we are aware of the dangers this may bring and strive to support children, staff, and families in using the Internet safely. 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:*

1. *Content: being exposed to illegal, inappropriate, or harmful material*
2. *Contact: being subjected to harmful online interaction with other users*
3. *Conduct: personal online behaviour that increases the likelihood of, or causes, harm*

Our Designated Safeguarding person is ultimately responsible for online safety concerns. All concerns need to be raised as soon as possible to **Sumaya Ahmed (Nursery Manager).**

Within the nursery we aim to keep children (and staff) safe online by:

- 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, and any mobile devices.
- Keeping passwords safe and secure.
- Ensure management monitor all Internet activities in the setting.
- Locking away all nursery devices at the end of the day.
- No social media or messaging apps can be installed on nursery devices due to the security measures in place.
- 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).
- Ensuring children are supervised when using Internet devices.
- 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.
- Provide training for staff regularly about the importance of online safety and understanding how to keep children safe online.
- Ensuring staffs only use the work IT equipment for matters relating to the children and their education and care.
- Children do not have access to the Internet and never have unsupervised access.
- The designated person has overall responsibility for ensuring that children and young people are safeguarded and risk assessments in relation to online safety are completed.
- Children are taught the following stay safe principles in an age-appropriate way prior to using the Internet.
- Children aren't allowed access to social networking sites.
- Staff reports any suspicious or offensive material, including material that may incite racism, bullying or discrimination to the manager.
- The designated person ensures staffs have access to age-appropriate resources to enable them to assist children to use the Internet safely.
- If staff becomes aware that a child is the victim of cyber-bullying, they discuss the manager.

The Designated Safeguarding Person will make sure that:

- All staff knows how to report a problem and when to escalate a concern, including the process for external referral if they feel it is needed.
- All concerns are logged, assessed, and actioned upon using the nurseries safeguarding procedure.
- 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.

Policy reviewed by: Sumaya Ahmed (Manager)
Date: October 2023 Next review: October 2024