Online Safety

December 2025 **Review: December 2025 (or when required)**

Link to Every Child Matters: Feeling Safe

Links to Safeguarding and Welfare Requirements: 3.4-3.7

Kidzproof Ltd is aware of the growth of internet use and the advantages this can bring. However, it is also aware of the dangers and strives 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:

- 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"

Our Designated Safeguarding person is ultimately responsible for online safety concerns. All concerns need to be raised as soon as possible to **Nichola O'Regan (Kidzproof 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, not sharing or writing these down. These are stored in a Password Management programme.

• 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 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.

• We abide by an acceptable use policy; ensuring staff only use the work IT equipment for matters relating to the children and their education and care. No personal use will be tolerated

Computers

The children's computers are located in an area clearly visible to staff. If a second-hand computer is purchased or donated to the nursery, the designated person will ensure that no inappropriate material is stored on it before children use it.

Internet Access

• 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;

• Only go online with a grown up

• Be kind online

• Keep information about me safely

• Only press buttons on the internet to things I understand

• Tell a grown up if something makes me unhappy on the internet

• Children aren't allowed access to social networking sites.

• Staff report any suspicious or offensive material, including material which may incite racism, bullying or discrimination to the internet watch foundation at www.iwf.org.uk.

• Suspicions that an adult is attempting to make inappropriate contact with a child on-line is reported to the national crime Agency's Child Exploitation and Online Protection Centre at www.ceop.police.uk.

• The designated person ensures staff have access to age-appropriate resources to enable them to assist children to use the internet safely.

• If staff become aware that a child is the victim of cyber-bullying, they discuss this with their parents and refer them to sources of help, such as the NSPCC on 0808 800 5000 or www.nspcc.org.uk, or Childline on 0800 111 or www.childline.org.uk.

• The designated person will seek to build children's reliance in relation to issues they may face in the online world, and will address issues such as staying safe, having appropriate friendships, asking for help if unsure, not keeping secrets as part of social and emotional development in age appropriate ways.

Email

• Children are not permitted to use email in the nursery. Parents and staff are not normally permitted to use setting equipment to access personal emails.

• Staff do not access personal or work emails whilst supervising children.

Use of Online Systems

The nursery has a secure network that the computers and tablets link to that is password protected.

Famly App- the nursery is registered with Famly App to provide an online learning journey that can be accessed by the nursery and families. Security is of key concern in a nursery environment and Famly App takes its security measures very seriously. Famly App offers fully locked-down secure tablet devices to ensure they are not misused in any manner - Facebook, e-mails, etc., are all disabled on these specially configured high-security tablets. Each user has a separate user-ID and password and using a role-based access mechanism, a user is permitted to see only the information that is relevant for them. Famly App uses the Secure Sockets Layer (SSL) to encrypt all communication between the server and the tablets. All data is stored on secure Cloud-based servers in data centres located here in UK. All data is regularly backed-up onto redundant systems.

Transfer of data

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.

Social Media

• Staff are advised to manage their personal security settings to ensure their information is only available to people they chose to share with.

• Staff should not accept parents/carers as friends due to it being a breach of expected professional conduct.

• In the event that staff name the organisation or workplace in any social media they do so in a way that is not detrimental to the organisation or it's children or parents/carers.

• Staff observe confidentiality and refrain from discussing an issues relating to work

• Staff should not share information they would not want children, parents or colleagues to view.

• Staff should report any concerns or breaches to the nursery's designated person.

• Staff avoid personal communication, including on social networking sites, with the children and parents with whom they act in a professional capacity. If a practitioner and family are friendly prior to the child coming to the nursery, this information must be shared with the manager prior to a child attending and a risk assessment and agreement in relation to boundaries is agreed.

Parents and visitors' use of social networking

We promote the safety and welfare of all staff and children and therefore ask parents and visitors not to post, publically or privately, information about any child on social media sites such as Facebook, Instagram and Twitter. We ask all parents and visitors to follow this policy to ensure that information about children, images and information do not fall into the wrong hands.

We ask parents not to:

• Send friend requests to any member of nursery staff

• Screen shot or share any posts or pictures from the nursery on social media platforms (these may contain other children in the pictures)

• Post any photographs to social media that have been supplied by the nursery with other children in them (e.g. Christmas concert photographs or photographs from an activity at nursery)

We ask parents to share any concerns regarding inappropriate use of social media through the official procedures (please refer to the partnership with parents policy, complaints procedures and grievance policy).

Use and/or distribution of inappropriate images

• Staff are aware that it is an offence to distribute indecent images. In the event of a concern that a colleague or person is behaving inappropriately, the Safeguarding Children and Child Protection Policy, in relation to allegations against staff and/or responding to suspicions of abuse, is followed.

• Staff are aware that grooming children and young people online is an offence in it's own right and concerns about a colleague's behaviour are reported.

The Designated Safeguarding Person will make sure that:

• All staff know 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 Nursery's 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.

• The Professionals Online Safety Helpline (0344 381 4772 or 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-protectingprofessionals-in-early-years-settings-online-safety-considerations/safeguarding-childrenand-protecting-professionals-in-early-years-settings-online-safety-considerations-formanagers 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-protectingprofessionals-in-early-years-settings-online-safety-considerations/safeguarding-childrenand-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

Reporting concerns of misuse

If any concerns arise relating to online safety or disregard for any of the policy then we will follow our safeguarding policy and report all online safety concerns to the Designated Safeguarding Person.

Further Guidance

NSPCC and CEOP Keeping Children Safe Online training: www.nspcc.org.uk/what-you-cando/get-expert-training/keeping-children-safe-online-course/