Online safety (inc. mobile phones & cameras)

Policy statement

We take steps to ensure that there are effective procedures in place to protect children, young people and vulnerable adults from the unacceptable use of Information Communication Technology (ICT) equipment or exposure to inappropriate materials in the setting.

Procedures

As safeguarding lead, Tahmina Haque is the person designated to manage online safety.

Information Communication Technology (ICT) equipment

- Staff and children only use ICT equipment belonging to the setting.
- The designated person is responsible for ensuring all ICT equipment is safe and fit for purpose.
- Second hand equipment is not used in the setting.
- All computers have virus protection installed.
- All devices are password protected.
- All ICT equipment for use by children is located in an area clearly visible to staff.
- All ICT equipment must be kept safe and secure. Staff must report loss or damage to the Manager immediately.
- All ICT equipment is PAT tested annually.
- USB devices are not used to store personal data.

Internet access

- Parental permission is obtained for children to have supervised access to the internet for learning activities when children join Pre-School and parents are made aware of this policy.
- 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 not allowed to access social networking sites.
- The designated person ensures that safety settings are in place to ensure that inappropriate material cannot be accessed. Our computers and laptops are protected by FortiGate web filtering and our tablets are set to block inappropriate content.
- If staff discover an unsuitable site, it must be reported immediately to the designated person responsible for online safety.
- Senior staff, alongside Simply IT, will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- Staff must not access personal accounts whilst in Pre-School or change any of the settings.
- We will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content it is not possible to guarantee that unsuitable material will never appear on a Pre-School computer, laptop or tablets.
- The Pre-School cannot accept liability for the material accessed, or any consequences of internet access, however any incidents will be reported to the designated person responsible for online safety. The person responsible for online safety in conjunction with the person responsible for managing the network will decide upon the appropriate action to be taken to prevent the situation arising again.
- Children are taught the following stay safe principles in an age appropriate way prior to using the internet;
    - only go on line with a grown up
    - be kind on line
    - keep information about me safe
    - only press buttons on the internet to things I understand
    - tell a grown up if something makes me unhappy on the internet
- Designated persons will also seek to build children's resilience 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.
- 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 and to the designated person for online safety.
- 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 follow safeguarding procedures and discuss this with their parent/carer and refer them to sources of help, such as the NSPCC on 0808 800 5000 or www.nspcc.org.uk, or Childline on 0800 1111 or www.childline.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.

Email

- Children are not permitted to use email in the setting. Parents/carers and staff are not normally permitted to use setting equipment to access personal emails.
- Staff do not access personal or work email whilst supervising children.

Mobile phones – children

- Children do not bring mobile phones or other ICT devices with them to the setting. If a child is found to have a mobile phone or ICT device with them, this is removed and stored in a locked drawer until the parent/carer collects them at the end of the session.

Mobile phones – staff, volunteers, students and visitors

- During working hours personal mobile phones are not to be used in any areas where children are likely to be present; this includes classrooms, cloakrooms, toilets and outdoor play areas. They will be stored in the office or in the staff member's locker.
- In an emergency, personal mobile phones may be used in an area where there are no children present, with permission from the manager.
- Our staff, volunteers and students ensure that the setting telephone number is known to family and other people who may need to contact them in an emergency.
- If our members of staff, volunteers or students take their mobile phones on outings, for use in case of an emergency, they must not make or receive personal calls, or take photographs of children.
- Parents/carers and visitors are requested not to bring their mobile phones in to setting. Mobile phones are placed in a secure box during visits and returned when they leave. Mobile phones are not to be used outside the premises. We make an exception if a visitor's company or organisation operates a lone working policy that requires contact with their office periodically throughout the day. Visitors will be advised of a quiet space where they can use their mobile phone, where no children are present.
- These rules also apply to the use of work-issued mobiles, and when visiting or supporting staff in other settings.
- Smart watches are not allowed in setting.

Cameras and videos

- Photographs & videos are taken with the consent of parents/carers and images are used, stored and protected in accordance with our Privacy Notice.
- Our staff and volunteers must not bring their personal cameras, watches with cameras e.g. Apple watches or video recording equipment into the setting.
- Only photos taken by staff with a setting camera, tablet or video camera will be used in the setting. Staff, students and volunteers will never take photos on their own personal cameras, wrist cameras or mobile phones either within the setting or during outings.
- Memory cards remain on the premises when they are not in use.
- Pre-School cameras and tablets are locked away in the designated area at the end of the day.
- Photos will never be taken in the changing or toileting areas.
- If there are outside photographers attending the setting for any reason other than that of school photos, we will notify parents/carers and ask for their permission separately for their child to be photographed.

- At events and fundraising activities where parents/carers may take photographs, parents/carers are requested not to publish images on social media or the internet.

Social media

- Staff are advised to manage their personal security settings to ensure that their information is only available to people they choose to share information with.
- Staff should not accept service users, children and 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 its service users.
- Staff observe confidentiality and refrain from discussing any issues relating to work.
- Staff should not share information they would not want children, parents/carers or colleagues to view.
- Staff should report any concerns or breaches to the designated person in their setting.
- Staff avoid personal communication, including on social networking sites, with the children and parents/carers with whom they act in a professional capacity. If a practitioner and family are friendly prior to the child coming into the setting, this information is shared with the manager prior to a child attending and a risk assessment and agreement in relation to boundaries is agreed.

Electronic learning journals for recording children's progress

- A risk assessment is completed with details on how the learning journal is managed to ensure children are safeguarded.
- Staff adhere to the guidance provided with the system at all times.

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 other 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 on line is an offence in its own right and concerns about a colleague's or others' behaviour are reported (as above).

Further guidance

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

This policy was adopted by	**Silsoe Pre-School**
Date	**September 2022**