



Registered Charity No. 1022409

1 Safeguarding children, young people and vulnerable adults policy and procedures

Designated person/lead for safeguarding is: Flora Lau

Back up Designated person is: Caz Schmull

Designed officer is: Emma George

1.12 E-safety procedures (including all electronic devices with internet capacity)

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.

Online Safety

It is important that children and young people receive consistent messages about the safe use of technology and are able to recognise and manage the risks posed in both the real and the virtual world.

Terms such as 'e-safety', 'online', 'communication technologies' and 'digital technologies' refer to fixed and mobile technologies that adults and children may encounter, now and in the future, which allow them access to content and communications that could raise issues or pose risks. The issues are:

Content – being exposed to illegal, inappropriate or harmful material

Contact – being subjected to harmful online interaction with other users

Conduct – personal online behaviour that increases the likelihood of, or causes, harm

I.C.T Equipment

- Only ICT equipment belonging to the setting is used by staff and children.
- The designated person is responsible for ensuring all ICT equipment is safe and fit for purpose.
- The preschool manager ensures that all computers have up-to-date virus protection installed.
- The designated person ensures that safety settings are set to ensure that inappropriate material cannot be accessed.

- Tablets are only used for the purposes of observation, assessment and planning and to take photographs for individual children's learning journeys.
- Tablets are password protected and are stored securely at all times when not in use.
- Staff follow the additional guidance provided with the system

Internet access

- Children do not normally have access to the internet and never have unsupervised access to the internet.
- If staff access the internet with children for the purposes of promoting their learning, written permission is gained from parents who are shown 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.
- Only reputable sites with a focus on early learning are used (e.g. CBeebies).
- Video sharing sites such as YouTube are not accessed due to the risk of inappropriate content.
- Children are taught the following stay safe principles in an age appropriate way:
 - only go online with a grown up
 - be kind online **and** 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
- Staff support children's resilience in relation to issues they may face online, and address issues such as staying safe, appropriate friendships, asking for help if unsure, not keeping secrets as part of social and emotional development in age-appropriate ways.
- If a second-hand computer is purchased or donated to the setting, the designated person will ensure that no inappropriate material is stored on it before children use it.
- All computers for use by children are sited in an area clearly visible to staff.
- Children are not allowed to access 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.

Email

- Children are not permitted to use email in the setting. Parents 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.
- Staff always send personal information by encrypted email and share information securely.

Personal mobile phones – children (includes internet enabled devices)

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 out of children's reach until the parent collects them at the end of the session.

Personal mobile phones – staff and visitors (includes internet enabled devices)

- Personal mobile phones and internet enabled devices are not used by staff during working hours; unless there is an emergency. They will be stored on the window sill in the main room.
- The designated person completes a risk assessment for where they can be used safely.
- In an emergency, personal mobile phones may be used in an area where there are no children present, with permission from the preschool manager.
- Our staff and volunteers ensure that the contact details of the preschool telephone number is known to family and other people who may need to contact them in an emergency.
- If our members of staff or volunteers 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 and visitors are requested not to use their mobile phones whilst on 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.

Cameras and videos

- Members of staff do not bring their own cameras or video recorders to the preschool.
- Photographs/recordings of children are only taken for valid reasons, e.g. to record learning and development, or for displays, with written permission received by parents, and are only taken on equipment belonging to the preschool.
- Camera and video use is monitored by the preschool manager.
- Where parents request permission to photograph or record their own children at special events, general permission is first gained from all parents for their children to be included. Parents are told they do not have a right to photograph or upload photos of anyone else's children.
- Photographs/recordings of children are only made if relevant permissions are in place.
- If photographs of children are used for publicity purposes, parental consent must be given and safeguarding risks minimised, for example, ensuring children cannot be identified by name or through being photographed in a sweatshirt with the name of their setting on it.
- Children may on occasion be given the opportunity to photograph each other and their surroundings. This practice may occur during off-site activities and for most children it will be normal practice to take photographs to record a trip or event. Children also have access to cameras within the setting environment to support

their learning and development needs. These activities will be encouraged in a safe and enabling environment

Cyber Bullying

If staff become aware that a child is the victim of cyber-bullying at home or elsewhere, they discuss this with the parents and refer them to help, such as: NSPCC Tel: 0808 800 5000 www.nspcc.org.uk or ChildLine Tel: 0800 1111 www.childline.org.uk

Use of social media

Staff are expected to:

- understand how to manage their security preschools to ensure that their information is only available to people they choose to share information with
- ensure the organisation is not negatively affected by their actions and do not name the preschool
- are aware that comments or photographs online may be accessible to anyone and should use their judgement before posting
- are aware that images, such as those on Snapshot may still be accessed by others and a permanent record of them made, for example, by taking a screen shot of the image with a mobile phone
- observe confidentiality and refrain from discussing any issues relating to work
- not share information they would not want children, parents or colleagues to view
- set privacy preschools to personal social networking and restrict those who are able to access
- not accept service users/children/parents as friends, as it is a breach of professional conduct
- report any concerns or breaches to the designated person in their preschool
- not engage in personal communication, including on social networking sites, with children and parents with whom they act in a professional capacity. There may be occasions when the practitioner and family are friendly prior to the child coming to the preschool. In this case information is shared with the manager and a risk assessment and agreement in relation to boundaries are agreed

Electronic learning journals for recording children's progress

- Preschool leader will seek permission from the committee prior to using any online learning journal. A risk assessment is completed with details on how the learning journal is managed to ensure children are safeguarded.
- Staff always adhere to the guidance provided with the system.

Use/distribution of inappropriate images

- Staff are aware that it is an offence to distribute indecent images and that it is an offence to groom children online. In the event of a concern that a colleague is behaving inappropriately, staff advise the designated person who follow procedure 1.4 Allegations against staff, volunteers or agency staff.
- Staff are aware that grooming children and young people on line is an offence 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 on 6th September 2023

Date to be reviewed 6th September 2024

Signed by committee chairperson

Signed by preschool manager
