Online safety (including mobile phones and 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 acceptable use of Information Communication Technology (ICT) equipment or exposure to inappropriate materials in the setting.

Procedures

Our Designated Safeguarding Lead Louise Trego and Deputy Designated Safeguarding Lead Nicola Coles are responsible for coordinating action to protect the children.

ICT equipment

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

Internet access

- Children will not normally have access to the internet and never have unsupervised access
- Staff will occasionally access the internet to help promote their child's learning. The child will never be left unattended during this activity.
- The designated person has overall responsibility for ensuring that children and young people ae 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

- 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.
- 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 the children use it.
- All computers for use by children are located 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 that may incite racism, bullying or discrimination to the Internet Watch Foundation at www.iwf.orf.uk
- Suspicions that an adult is attempting to make inappropriate contact with a child online will be 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 the internet safely.
- If staff become aware that a child is a victim of cyber bullying, they discuss this with the parents and refer them to sources of help such as NSPCC on 0800 5000 or www.nspcc.org.uk or Childline on 0800 1111 or www.childline.org.uk

Email

- Children are not permitted to use email in the setting. Parents and staff are not permitted to use setting equipment to access personal emails.
- Staff do not access personal or work email while supervising children
- Staff send personal information by encrypted email and share information securely at all times

Mobile phones - children

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

Mobile phones – staff and visitors

- Personal mobile phones that belong to staff and visitors must be placed in the filing cabinet drawer.
- In an emergency personal mobile phones may be used in an area where there are no children present, with the permission of the manager
- Our staff and volunteers 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 or volunteers take their mobile phones on outing for use in case of an emergency they must not make or receive personal calls or take photographs of the children
- Parents and carers are requested not to use their mobile phones whilst on the premises.
- These rules also apply to the use of work issued mobile phones and when visiting or supporting staff in other settings.

Cameras and videos

- Our staff and volunteers must not bring their personal cameras or video recording equipment into the setting
- Photographs and recordings of children are only taken for a valid reasons, such as to record their learning and development, or for displays within the setting. This is with written permission obtained on our registration forms. Such use will be monitored by the manager.
- Where parents request permission to photograph or record their own children at special events, general permission is gained from all parents for their children to be included. Parents are advised that they do not have the right to photograph anyone else's children.
- If photographs of children are used for publicity purposes, parental consent must be given and safeguarding risks minimised. For example that children can not be identified by name or logo on their clothing.

Social media

- Staff are advised to manage their personal security settings to ensure that their information is on available to people they choose to share information with.

- Staff should not accept service users, children and parents 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.
- Staff observe confidentiality and refrain from discussing any 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 designated person in their setting
- Staff avoid personal communication including 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 a child attending and a risk assessment and agreement in relation to boundaries is agreed.

Electronic learning journal for recording a child's progress

- Managers seek permission 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 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 reporting suspicions of abuse, is followed.
- Staff are aware that grooming children and young people online is an offence in its own right and concerns about a colleague's or other's behaviour are reported using the same procedure as above.

You can obtain further guidance and support from NSPCC or CEOP

Signed on behalf of Tiny Feet Preschool _____ date: _____

Name of Signatory _____

Role of Signatory _____

Policy updated on 03/08/2020