

Safeguarding children, young people and vulnerable adults procedure

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

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

- The setting manager ensures that all computers have up-to-date virus protection installed.
- Tablets are only used for the purposes of observation, assessment and planning and to take photographs for individual children's learning journeys.
- Staff follow the additional guidance provided with the system

Work mobile phone

Staff have access to this at all times this can be used when going on outings, during fire drills and where internet access is unavailable to access the Family app. This number is shared on the safeguarding policy to ensure that the manager is contactable in case of any immediate safeguarding concerns.

Internet access

- Children never have unsupervised access to the internet.
- The setting manager ensures that risk assessments in relation to e-safety are completed.
- Only reputable sites with a focus on early learning are used (e.g. CBeebies).
- YouTube Kids can be used with supervised access.
- 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.
- 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.

The setting manager ensures staff have access to age-appropriate resources to enable them to assist children to use the internet safely.

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

- Personal mobile phones/smart phones and internet enabled devices are not used by staff during working hours. This does not include breaks where personal mobiles may be used off the premises or in a safe place e.g, staff room or when authorised by the setting manager to use their device.
- Personal mobile phones are stored securely in the office or locked cupboard.
- In an emergency, personal mobile phones may be used in the privacy of the office with permission of the manager or the deputy manager.
- Staff ensure that contact details of the setting are known to family and people who may need to contact them in an emergency.
- Staff to ensure that they take the pre-school/manager's work mobile phone when going on outing or for school pick-ups. Pre-school mobile to be used only in emergencies and for pre-school use only.
- Members of staff do not use personal equipment to take photographs of children.
- Parents and visitors do not use their mobile phones on the premises. There is an exception if a visitor's company/organisation operates a policy that requires contact with their office periodically throughout the day. Visitors are advised of a private space where they can use their mobile.

Smartwatch and fitness trackers

We recognise there are many health benefits for the use of smartwatches such as counting steps and heart rate. To ensure the safe wearing of Smart Watches staff must ensure that:

- The watch has to be worn in 'flight mode' or Bluetooth is disconnected, this will ensure there is no internet connectivity to access notifications or Wi-Fi.
- They agree to random spot checks by the manager and deputy to confirm the above.
- Staff understand they may not use their watch to receive calls or check messages during working hours and whilst on pre-school premises as this creates distraction and potential dangers.
- Staff have to be vigilant of others checking their watches and remind them of the Pre-school and nursery policy and procedures of the safe wearing of a smart watch.

- Photographs can only be processed from a Smart Watch with a mobile device in close proximity; staff are reminded that the safe storage of a mobile phone is in their bag stored in a locked cupboard or kept in the office.
- Staff should not use their Smart Watch to access photos or images whilst on nursery premises (indoors or outdoors) and whilst on local trips/outings.
- Where ongoing technology advances the pre-school reserves the rights to request the removal of a Smart Watch if the safety of a child[ren] is at risk.

Cameras and videos

- Members of staff do not bring their own cameras or video recorders to the setting.
- Photographs/recordings of children are only taken for valid reasons, e.g. to record learning and development, or for displays, and are only taken on equipment belonging to the setting.
- Camera and video use is monitored by the setting manager.
- Where parents take photographs or record their own children at special events, parents are told they do not have a right to upload photos or videos on any social media platforms. If the setting becomes aware of a breach of this nature by a parent, a meeting will be held with the parent to remove any offending media and reinforce the setting's procedure.
- Photographs/recordings of children are only made if relevant permissions are in place.
- If photographs are used for publicity, parental consent is gained and safeguarding risks minimised, e.g. children may be identified if photographed in a sweatshirt with the name of their setting on it.

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 settings 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 setting
- 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 settings 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 setting
- 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 setting. In this case information is shared with the manager and a risk assessment and agreement in relation to boundaries are agreed

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 follows procedure 06.2 Allegations against staff, volunteers or agency staff.

•

This policy was adopted by

Tilehouse Street Pre-school and Nursery

On

04/10/2023

Date to be reviewed

October 2024 or as and when required

Signed on behalf of the provider

Name of Signatory

Role of Signatory (e.g. chair, director or owner)

Employee agreement to wear Smartwatch or fitness tracker

We recognise that there are many health benefits for the use of smart watches such as counting steps and heart rate. To ensure the safe wearing of SmartWatches and fitness trackers we have put in place following procedures. Please read and sign to acknowledge that you understand and agree to the following procedures:

- The watch has to be worn in 'flight mode' or Bluetooth is disconnected, this will ensure there is no internet connectivity to access notifications or Wi-Fi.
- Staff agree to random spot checks by the manager and deputy to confirm the above.
- Staff understand they may not use their watch to receive calls or check messages during working hours and whilst on pre-school premises as this creates distraction and potential dangers.
- Staff have to be vigilant of others checking their watches and remind them of the nursery policy and procedures of the safe wearing of a smart watch.
- Photographs can only be processed from a Smart Watch with a mobile device in close proximity; staff are reminded of the safe storage of a mobile phone in the locked cupboard or stored in the office.
- Staff should not use their Smart Watch to access photos or images whilst on nursery premises (indoors or outdoors) and whilst on local trips/outings.
- Where ongoing technology advances the pre-school reserves the rights to request the removal of a Smart Watch if the safety of a child[ren] is at risk.
- The pre-school reserves the right to request removal of Smart watch or fitness tracker should a staff member fail to adhere to the above procedures.

I

Name of staff:

Signature:

Date: