|  |  |
| --- | --- |
|  | **Online safety, including mobile phones and cameras** |

**Safeguarding and Welfare Requirement: Child Protection**

The safeguarding policy and procedures must include an explanation of the action to be taken in the event of an allegation being made against a member of staff, and cover the use of mobile phones and cameras in the setting.

**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**

* Our designated person responsible for co-ordinating action taken to protect children is:

**Paula Maxted**

*Information Communication Technology (ICT) 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.
* 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 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. 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 children use it.
* 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](http://www.iwf.org.uk/).
* Suspicions that an adult is attempting to make inappropriate contact with a child online is reported to the National Crime Agency’s Child Exploitation and Online Protection Centre at [www.ceop.police.uk](http://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 1111 or www.childline.org.uk.

*Email*

* Children are not permitted to use email in the setting.
* Staff do not access personal or work email whilst 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 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 collects them at the end of the session.

*Mobile phones – staff and visitors*

* Personal mobile phones belonging to staff and volunteers are only used during lunch breaks in the office where there are no children present.
* At the beginning of each individual’s shift, personal mobile phones are stored in a locked cupboard in the office.
* 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 outings, for use in case of an emergency, they must not make or receive personal calls or take photographs of the children.
* Staff and volunteers will not use their personal mobile phones for taking photographs of children on outings.
* Parents and visitors are requested not to use their mobile phones whilst on the premises. We make an exception for parents during the registration visit who are required to provide contact telephone numbers on the Registration Form which may be stored on their mobile phones. This activity will be supervised by the key person conducting the registration visit. We also 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 to go into the office where they can use their mobile phone.

*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 valid reasons i.e. to record their learning and development, or for displays within the setting, with written permission received by parents (see the Registration form). Such use is 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 a right to upload photographs of anyone else’s child to social media websites.
* If photographs of children are used for publicity purposes, parental consent must be given (see Registration form) and safeguarding risks minimised, for example, ensuring children cannot be identified by name.

*Fitbits and Smart Watches*

* Smart watches may only be worn into the room in the presence of children if their Bluetooth and internet connectivity is restricted, via airplane mode or turning the functions off manually. Staff understand they may not use their watch to receive calls or check messages as this creates a distraction with the potential to be dangerous.
* Staff are also vigilant of others checking their watches and are expected to report any personal use of smart watches during the day to management.
* Staff must not use their watch to access photographs or content as children may be exposed to inappropriate images.
* Staff are also aware that they must not use their smart watches to take photos or voice recordings on their phone using the watch to operate this and are aware that the rules of GDPR prevent voice recordings or photographs being taken without the person’s express consent.
* Where ongoing technological advances with smart watches occur, the Pre-school reserves the right to request the member of staff to remove their smart watch completely, for instance if it were to become capable of taking photographs.
* Wherever possible the Pre-school advise staff to avoid wearing a smart watch at work as there is a chance of it being lost or damaged and the Pre-school take no responsibility for this occurrence.

*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 be aware of their responsibilities with regard to professional conduct when accepting service users, parents and carers as friends.

* 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 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 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.

*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 online 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/](http://www.nspcc.org.uk/what-you-can-do/get-expert-training/keeping-children-safe-online-course/)

This policy was adopted at a meeting of Thames Pre-school

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |