Online Safety Policy

Policy statement

At South Milford Preschool, 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 coordinating action taken to protect children is:

Mel Riches

*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.
* The designated person ensures that safety settings are set to ensure that inappropriate material cannot be accessed.

*Internet access*

* We do not have access to the internet on our ICT equipment. Children never have access to the internet in our setting.
* Staff must not access the internet with the children using their own devices.
* 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 taught the following stay safe principles in an age appropriate way regarding using the internet at home;
* only go on line 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.
* Parent’s will be given information and links to websites in regard to keeping their children safe online at home.
* 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.
* 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](http://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](http://www.ceop.police.uk/).
* If staff become aware that a child is the victim of cyberbullying, 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 have no access to setting equipment to access personal emails.
* 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 the locked paper cupboard until the parent collects them at the end of the session.

*Mobile phones – staff and visitors*

* Personal mobile phones are not used by staff whilst working with and supervising the children. Staff mobile phones will be stored in the staff drawers in the kitchen area.
* In an emergency, personal mobile phones may be used in an area where there are no children present, with permission from the manager.
* 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.
* The manager may give permission for members of staff or volunteers to 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. If necessary, 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 smart devices such as watches.

*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 photograph anyone else’s child or to upload photos of anyone else’s children. Parents are also required not to post any photos on social media platforms.
* 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.

*Cyber Bullying*

* If staff become aware that a child is the victim of cyberbullying 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](http://www.nspcc.org.uk) or ChildLine Tel: 0800 1111 [www.childline.org.uk](http://www.childline.org.uk)

*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 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 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 and a risk assessment and agreement in relation to boundaries is agreed.

*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

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

[Online safety at home](https://www.childnet.com/parents-and-carers/hot-topics/keeping-young-children-safe-online/?tempid=1326955)

| This policy was adopted by | South Milford Pre-school |  |
| --- | --- | --- |
| On | July 2023 |  |
| Date to be reviewed | July 2024 |  |
| Signed on behalf of the provider | M Riches |
| Name of signatory | Mel Riches |

Links to other policies:

Safeguarding children and child Protection Policy

Mobile Phone and Camera Policy

Social Media Policy

Staff Code of Conduct Policy

Visitors Policy