

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.

1.6 Online safety (Inc. 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 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:
Tracey Pritchard

Information Communication Technology (ICT) equipment

- Only ICT equipment belonging to the setting is used by 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, and I Pads are password protected.

Internet access

- Children do not normally have access to the internet and never have unsupervised access.
- 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 to stay safe in an age appropriate way when using the internet e.g. only go on line with a grown up.
- 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.
- 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 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 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. 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 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 until the parent collects them at the end of the session.

Mobile phones – staff and visitors

- Personal mobile phones belonging to our staff and volunteers are not used on the premises during working hours. Personal mobile phones must be left in bags in the kitchen.
- In an emergency, personal mobile phones may be used in an area where there are no children present, with permission from the manager i.e. outside the front door. 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 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 whilst supervising children.
- Staff or volunteers must not take photographs of children on personal devices.
- 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 i.e. outside.
- These rules also apply to the use of work-issued mobiles, 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 where children are present.

- 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 from the parents (see the photo consent 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 photos of anyone else's children.
- If photographs of children are used for publicity purposes, parental consent must be given, and safeguarding risks minimised.

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 are advised not to accept service users (i.e children and parents) as friends, and staff are advised not to discuss information of a personal nature with parents on social media.
- The Manager and Deputy will monitor the Pre-school face book page on a regular basis to ensure there are no posts of an inappropriate/personal nature.
- 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.

Electronic learning journals for recording children's progress

- Managers seek permission from the committee prior to using any online learning journal.
- Parental permission is obtained for any child with an online learning journal. If consent is withheld the pre-school will continue with the paper learning journal.
- I Pads are used by staff to record children's learning, these are locked away at the end of a session.
- The I Pads are pin protected, any staff member whose suspects their log in details have been compromised in anyway must inform the manager.
- Staff must log out as soon as they finish at the end of the session.
- Staff can access tapestry using their own devices at home using a secure pin protection. Staff are aware of confidentiality and do not share information with anyone else.
- Staff adheres 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 responding to suspicions of abuse, is followed.
- Staff are aware that grooming children and young people on line 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/

This policy was adopted by

St Nicholas and St Faith Pre-

school

On _____ (date)

Date to be reviewed _____ (date)

Signed on behalf of the provider

Name of signatory

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

