



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

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(s) responsible for co-ordinating action taken to protect children are:

Karen Roberts and Karen Illsley

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 do not normally have access to the internet and never have unsupervised access.
- 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.
- 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 prior to using the internet;
 - only go on line with a grown up.
 - be kind on line.
 - 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.
- All computers for use by children are located in an area clearly visible to staff.
- 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. 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 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 office in a lockable cabinet until the parent collects them at the end of the session.

Mobile phones – staff ,visitors and contractors

- We allow staff to bring in personal mobile telephones for their own use.
- Users bringing personal mobile telephones into the setting must ensure there is no inappropriate or illegal content on the device.

- All staff must ensure that their mobile telephones are left inside their bag in the office or locked cleaners cupboard.
- Mobile phone calls may be taken during staff breaks during non child contact time. If staff have a personal emergency they are free to use the setting's phone and are encouraged to give this number to immediate family in case of emergencies.
- All helpers will be requested to place their bag containing their phone in the mobile friendly area (cleaners cupboard or office).
- All visitors will be informed that no mobile phones are to be used during their time at the setting, unless in a mobile friendly zone as agreed by the Manager.
- It is the responsibility of all members of staff to be vigilant and report any concerns to the Manager.
- Concerns will be taken seriously, logged and investigated appropriately in line with our safeguarding policy.
- If it is necessary for visitors/Contractors to have their mobile phones to implement their role effectively then they are to be supervised at all times. Any photographs taken need to be vetted by the Manager or Assistant Manager.

Cameras and videos

- Our staff and volunteers must not bring their personal cameras or video recording equipment into the setting.
- Photographs are taken for the purpose of recording a child or group of children participating in activities or celebrating their achievements and are an effective form of recording their progression in the Early Years Foundation Stage. They may also be used on our website and/or by the local press, social media with permission from the parents.
- However, it is essential that photographs are taken and stored appropriately to safeguard the children in our care.
- 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 informed that they do have the right to upload photos of any photographs with other children in or display on social media. If the setting is providing care for a looked after child and/or a child at risk no photographs can be taken at all.
- 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.
- Only the designated Pre-school cameras, or tablets are to be used to take any photos within the setting or on outings.

- Images taken on these cameras, and tablets must be deemed suitable without putting the child/children in any compromising positions that could cause embarrassment or distress.
- All staff are responsible for the location of the cameras, and tablets which are locked away at the end of the session.
- Images taken and stored on the cameras and tablets must be downloaded on site as soon as possible, and then deleted.
- Under no circumstances must cameras of any kind be taken into the toilet area.

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.
- We take a professional approach to confidentiality and the privacy of family life. Our policy is that staff do not make or accept invitation to become online friends with parents or other family carers on any social networking site. This policy also applies to all students and bank staff .
- Facebook, Twitter and other networking sites or personal blogs are all public forms of communication. In their non work time, staff, students or helpers remain responsible for not posting anything online that breaks confidentiality about children, families or colleagues, or information that could damage the reputation of the pre-school.
- To keep staff safe, we advise that any social media pages are kept secure and can only be viewed by close friends. We also advice staff to not disclose where they work on any social media sites.
- 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 an agreement in relation to boundaries is made.

Learning journals for recording children's progress

- Staff do not take the children's learning journey's home with them without prior agreement by the manager and parents.

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).

Working in partnership with parents

- We share any relevant advice regarding online safety with our parents through our newsletter, posters, and information evenings.

All staff are required to agree to and sign an 'Acceptable Use Agreement' regarding all ICT and electronic devices. This agreement is then kept in individual staff personnel files.

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/

<i>This policy was adopted at a meeting of Pirton Pre-School Committee.</i>	
Held on (date)	
Signed on behalf of the Management Committee / Proprietor	
Role of signatory (e.g. chairperson)	