**Online safety (Inc. mobile phones, smart watches 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. All employees including supply, agency, cover and other individuals from partner organisations will be expected to comply with this policy. If staff are found to be in breach of this policy they may be subject to disciplinary action, in accordance with the Pre-school’s Disciplinary Policy and Procedures.

**Procedures**

* Our designated person (Manager/Deputy Manager) is responsible for co-ordinating action taken to protect children

***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 with internet access 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.
* We have an e-safety board displayed for parents/carers to help them understand how to keep their children and devices safe for use.( Action)
* 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.
* 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](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/)**.**
* 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, use the secure server or via anycomms and share information securely at all times.

***Mobile phones – staff and visitors***

* Personal mobile phones are not used by our staff on the premises during working hours. They will be turned on silent/off and stored safely and securely and returned on lunch break and then on leaving the setting.
* In an emergency, personal mobile phones may be used in an area where there are no children present, with permission from the manager.
* Staff may give the pre-schools landline number as a personal emergency contact number.
* If a staff member needs to make an urgent personal call during working hours they may use the pre-schools landline at the discretion of the Manager or Deputy.
* 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 children.
* Parents and visitors are requested not to use their mobile phones whilst on the premises, and are stored in the office until they leave the setting
* These rules also apply to the use of work-issued mobiles, and when visiting or supporting staff in other settings.
* We reserve the right to refuse admittance to anyone who does not agree to this policy.

***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.
* 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.

***Smart watches***

We recognise there are many health benefits for the use of smart watches such as counting steps and heart rate.

Smart watches that do not have a camera device in them can be worn in the setting. Staff need to ensure that phones are stored in the mobile phone drawers and Bluetooth is turned off. Staff can be asked to removed this by management.

To ensure the safe wearing of smart watches staff and visitors must;

* Understand they are prohibited from using their watch to receive calls or check messages whilst in the playrooms as this creates distraction and potential dangers.
* be vigilant of others checking their watches and remind them of the Pre-school policy and procedures of the safe wearing of a smart watch.

***Social media***

Social media websites such as Facebook and Twitter are all useful technologies that are now a part of everyday life. Every employee has an opportunity to express and communicate on-line in many ways, and as an employer we do not wish to discourage an on-line presence. However, everyone needs to use good judgement on what material makes its way on-line.

The pre-school respects employees’ rights to a private life. However, the pre-school must ensure that confidentiality and its reputation are protected. Whilst the pre-school does not wish staff to discourage staff from using such sites on the internet in their personal time it does expect certain standards of conduct to be observed in order to protect the pre-school and its reputation and also to protect staff from danger of inappropriate use.

* 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.
* All employees who use social networking applications are required to take care not to allow their interactions on these sites to damage working relationships with colleagues and service users of the pre-school and the wider community. On no account must photographs of the children in the setting be placed on these sites.
* That no staff member should be “friends” with current parents of children in our setting and we ask that you delete them before they join our pre-schools. If you feel there is special circumstances that you remain friends with a parent on facebook then you will need to write the reasons down and the Directors will discuss at their meetings.

* In addition we would discourage the immediate 'friending' of parents when children leave our preschools, as the relationship at this point is a professional one and it could damage the preschool reputation if it is seen to be otherwise.
* Remember that no information sent over the web is totally secure and as such if you do not wish the information to be made public refrain from sending it over a social network site.
* Even though you may think you are anonymous or use an alias you may be recognised. Maintain professionalism, honesty, and respect. Could you be guilty of leaking information, discussing confidential information?
* Further, if any employee becomes aware of social networking activity that would be deemed distasteful, please contact your Manager.
* 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.

**Company resources**

The use of Company computers, Internet access, email, social networking, etc is intended for the benefit of the organisation and service users and should be not be used for personal activity.

**Company sensitive matters**

Any on-line communication regarding information such as employment issues and management decisions should not be discussed online.

**Enforcement:**

* Any breach of this policy could result in Staff member being disciplined in accordance with the pre-school disciplinary procedures
* The management/Directors reserve the right to require the closure of any applications or removal of content published by Staff which may adversely affect the reputation of the Pre-School or put it at risk of legal action.
* Any communications or content which is published that causes damage to the pre-school, any of its employees or any third party’s reputation may amount to misconduct or gross misconduct to which the pre-school Disciplinary procedures apply. Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct.

***Electronic learning journals for recording children’s progress (see our Tapestry Policy)***

* Managers seek permission from parents prior to using any online learning journal. A risk assessment is completed with details on how the learning journal is managed to ensure children are safeguarded.
* Staff adhere 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](http://www.nspcc.org.uk/what-you-can-do/get-expert-training/keeping-children-safe-online-course)

|  |  |  |
| --- | --- | --- |
| Document ID- | Policy adopted at meeting – Sept 2012 | Reviewed by : Ladybirds Directors |
| Date reviewed | 20/03/2024 | ZMH & JP |
|  |  |  |
|  |  |  |