



## Online Safety and Social Networking Policy, 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:  
**Marie Winnett & Janna McDonald (to attend EY Internet Safety Course March 2017)**  
With support from Louise Symonds and Sally Legg, Early Years Internet Safety Advisors

### Information Communication Technology (ICT) equipment

- Only ICT equipment belonging to the setting is used by staff and children.
- The designated persons are responsible for ensuring all ICT equipment are 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.
- 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](http://www.nspcc.org.uk), or Childline on 0800 1111 or [www.childline.org.uk](http://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, except in support parents in the setting up or maintenance of their Tapestry account. In this scenario, access will be fully supervised by a staff member.
- Staff do not access personal or work email whilst supervising children.

### **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. The Leader would discuss this with parents/carers to ensure device is not brought into setting again.

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

- Personal mobile phones are not used by staff on the premises during working hours. They will be stored in the mobile phone box in the office or a locked drawer.
- In an emergency, personal mobile phones may be used in an area where there are no children present, with permission from the manager.
- 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.
- When on an outing, the pre-schools own mobile telephone will be used. If members of staff or volunteers take their mobile phones on outings, it will be with the permission of the Leader/Manager, They must not make or receive personal calls unless emergency, or take photographs of children.
- 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. This will be outside of the building or in the office. All visitors are made aware of our policy.
- These rules also apply to the use of work-issued mobiles, and when visiting or supporting staff in other settings.
- Under no circumstances must phones or cameras of any kind be taken into the toilet or intimate care areas.
- Only the pre-school mobile telephone may be to hand during working hours. This phone does not have a camera.

### **Cameras and videos**

- 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 consent received by parents (see the Registration form). Such use is monitored by the Leader.
- 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.
- All cameras in the pre-school, including mobile telephones, can be subject to scrutiny at any time by the Safeguarding Lead or Pre-School Leader.

### **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 are reminded they represent the setting and have a responsibility to uphold the settings reputation and good name, and must not engage in activities on the internet which might bring the setting or colleagues into disrepute.
- It is not acceptable or appropriate to share work related information whether written or pictorial in this way. Sharing of information and ideas of a non-sensitive nature, may be shared through the dedicated closed Facebook groups; Pre-School Chit Chat restricted to staff and committee, and Pre-School Brainstorming for staff only. These groups are not suitable for sharing information about children or families.
- Staff respect the privacy and feelings of others.
- 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 will be completed as necessary.

### **Using Social Media to promote the Pre-School**

- The aim of our setting Facebook page is for advertisement showing what we do (using appropriate reference/pictures) and for appropriate information sharing with parents, for example fundraising activities and term dates. Content is planned and information will always remain professional. The effectiveness of this page will be continually monitored in relation to these aims.
- Parents will provide or decline permission for their child to be photographed and for photographs to be used on the pre-school website and Facebook/social media page. Children's photographs will not appear on the website or Facebook page without parental permission.
- Children's names will not be used on the settings Facebook page.
- Our Facebook page is an open group and therefore may be viewed by persons unknown to the pre-school. All parents are fully informed of this before permission is sought.
- Events such as sports day will be photographed for use in learning journeys etc., however photographs can only be used on pre-schools own Facebook page with parental permission. Parents are again reminded to photograph their own children, and children can only be photographed by others i.e. parents taking group photographs, if all parents have given permission. We insist that these photos are not used on social networking sites.

- A minimum two staff have attended the Early Years Internet Safety Course at any given time.

### **Electronic learning journals for recording children’s progress**

- Managers seek permission from the management committee 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).
- Our Whistleblowing Policy will also apply.

### **ICT and storing data**

- No information containing personal details of children and families at the setting will be stored on a home computer.
- Staff will not, under any circumstances, store photos of children and their families at the setting on a home computer.
- Memory sticks, if used, will be held in a secure place if at home or at the setting, and only with permission from the Manager or Leader.
- Photos of children will not be stored on the settings camera/iPod once printed off or downloaded for storage.
- The cameras/iPod/iPad will be stored safely whilst the pre-school is closed, in a locked drawer or locked space.
- The setting computer has ‘parental controls’ set to prevent children accessing inappropriate websites. All children are supervised while using the computer to access the web or websites.
- Our WIFI connection is locked and encrypted preventing inappropriate access.

*Any staff member, volunteer or student found to be non compliant with this policy will be subject to disciplinary action.*

### **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 is reviewed annually, or as deemed necessary.

Policy reviewed and updated.....(date)

Signed.....