Online safety

(incl. mobile phones, cameras, electronic devices, and online learning journals)

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:
  Michelle Tilley (Supervisor)

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 as part of our registration form process, and parents 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 online 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.

- 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 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 filing cabinet until the parent collects them at the end of the session.

Mobile phones – staff and visitors

- Personal mobile phones are not used by our staff on the premises during working hours. They will be packed away in their bags and stored in the kitchen area away from the main room/area used for childcare.
- In an emergency, personal mobile phones may be used in an area where there are no children present, with permission from the Playgroup Supervisor.
- 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. 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.

- 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.
- 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 Playgroup Supervisor.
- 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.

Tablet computers / iPads

- Staff may be provided with tablet computers / iPads ("devices") belonging to the setting to access the electronic learning journals for recording children's progress. This ensures that only technological devices belonging to the setting are used to take and record relevant images of children.
- Photos and / or videos of children will be removed from the devices at regular intervals.
- Staff must adhere to the following usage criteria. Failure to do so will result in disciplinary action.
- Staff will receive a unique email address solely for use on the devices. Staff are not permitted to set up their own personal email address on the device.
- Staff must either set up fingerprint access to the device or set a passcode which must be changed at least once per term. The passcode must be unique and must not be recorded.
- If any member of staff suspects that their login details have been compromised in any way, they must inform the Playgroup Supervisor as a matter of urgency, who will reset access to the device and all relevant applications.
- The device is not to be used for personal use.
- Staff are not permitted to allow others (e.g. family members, friends) to use the device.
- Staff are not permitted to download third party software onto the devices, nor link to personal third-party apps or services such as Dropbox or other storage; on-demand TV; other media streaming services.
- The devices must not be used to sign into personal social media accounts, e.g. Twitter; WhatsApp, Facebook, Instagram, LinkedIn.
- Staff are not permitted to download any materials from the device onto their personal devices or mobile phones.
- Devices must only be used to access the internet via a secure network.

- If staff wish to access the internet to find resources to share with children for the purposes of promoting their learning, staff must ensure that they have fully checked search results in advance before sharing with children. Staff attempting to access websites on these devices without permission of the Playgroup Supervisor or Deputy Supervisor could be subject to disciplinary action for gross misconduct.
- Staff are not permitted to jailbreak their devices, or otherwise hack, or tamper with it.
- The device must be in a protective case at all times.
- The device must be handled with care and respect. Do not throw, damage, place heavy items on, or intentionally drop your device.
- Only approved cleaning materials can be used to clean the device, such as laptop or tablet sprays and cloths.
- Do not keep or leave the device unattended in vehicles.
- Keep the device safe and secure at all times. Each staff member should know where their device is at all times.
- Staff are permitted to take the device back to their home address solely for work-related use only. It may not be used whilst out and about, or at other locations. Whilst using the device at home staff must be aware of other people around them and make sure that they are not overlooked.
- Staff must logout of applications as soon as they have finished working.
- Staff are required to ensure the device is charged and ready for use each and every day.
- If a device becomes lost or stolen, report it to the Playgroup Supervisor and Committee Chair as a matter of urgency.
- If a device becomes damaged, report it to the Playgroup Supervisor and Committee Chair as a matter of urgency, and hand over the device to them.
- Staff must not carry out repairs on any setting-owned device or solicit any individual or company to repair a setting-owned device on your behalf.

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 Playgroup Supervisor prior to a child attending and an agreement in relation to boundaries is agreed.

Tapestry Online Learning journal for recording children's progress

- The Playgroup Supervisor will seek permission from the senior management team prior to using any online learning journal (e.g. Tapestry). Details of how the online learning journal manage their 'application' to ensure children are safeguarded will be obtained and considered by the Playgroup Supervisor and the senior management team prior to using it.
- Staff must adhere to the guidance provided with the online learning journal system at all times.
- In the event of a breach of policy it is possible to disable a user's access to Tapestry.
- Staff must set up a secure login which is password protected (PIN number protected in the case of the Tapestry app). All passwords / PIN codes should be changed at least termly. All passwords / PIN codes must be unique and must not be recorded.
- Staff must maintain confidentiality and professionalism at all times, ensuring that all entries into Tapestry are appropriate.
- Staff must not share information stored with anyone other than the Playgroup Supervisor and Staff at Tansor Playgroup.
- All data held on our Tapestry account is owned by Tansor Playgroup; we are the Data Controller registered with the Information Commissioner's Office and are bound by the terms of the Data Protection Act 2018.
- Information on how Tapestry process and store data can be found on their website: https://www.tapestry.info/
- When a child leaves our setting we will transfer the Tapestry account to the new setting if they also use this system. If they do not, we will email a PDF of the account to the new setting.
- Parents/carers can download a copy of their child's learning journey from Tapestry at any time by requesting access from the Playgroup Supervisor.
- All accounts of children who leave Tansor Playgroup are made inactive, and details of children and their parents/carers are deleted from Tapestry before the start of the new academic year.

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

- 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 at a meeting of	Tansor Playgroup Committee
Held on	3rd April 2019
Signed on behalf of Tansor Playgroup Committee	Keri Blunston
Role of signatory	Co-Chair of Playgroup Committee

This policy was reviewed and updated on	23rd October 2019
Reviewed on behalf of Tansor Playgroup Committee	Wendy Ross
Role of reviewer	Co-Chair of Playgroup Committee