1.6 Online safety (inc. mobile phones, wearable technology and cameras)

Policy statement

At The Learning Meadow, 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:
  Dawn Pirie (Owner/Manager)

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 and are encrypted.
- 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.
- Occasionally staff may access the internet with children for the purposes of promoting their learning,
- 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 safe
  - 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 a locked drawer 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 are stored in a box in the office which is locked when left unattended. Only the manager and deputy have access to the office. If staff need to check their phones they must get permission from either manager who will unlock the office for them. Staff can then check their phones in a space where there are no children and return them to the box in the locked office.
- In an emergency, personal mobile phones may be used in an area where there are no children present, with permission from 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.
- When we visit the garden centre and the manager or deputy stay behind they will not take the setting mobile phone. We access the office using our radio's For example if there is an emergency we radio through to the office and follow guidance. We have all emergency contact details with us and can access the garden centre phone if required.
- Parents and visitors are requested not to enter the setting with their mobile phones as per signs outside. 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 that their phones must be stored in the box in the office and seek permission from the manager or deputy to use it. Then it must be used in an areas where there are no children.

- 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 who are working with the children full time must not bring their personal cameras or video recording equipment into the setting. This includes wearable technology that has recording and camera triggering functions.
- 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.

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.
- The setting facebook page is public and staff should not use it for inappropriate or unprofessional comments.
- The setting facebook page will not contain any photo's that easily identify children.
- Our closed face book parents group will be monitored by tow staff members and will be used to share activities, messages and only show photo's of children whose parents have signed a permission form.
- Staff should NEVER post any photographs of children or staff on any social media sites.
- 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 a risk assessment and agreement in relation to boundaries is agreed.

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	The Learning Meadow	*(name of provider)*
On	October 2018	*(date)*
Date to be reviewed	October 2019	*(date)*
Signed on behalf of the provider		
Name of signatory	Dawn Pirie	
Role of signatory (e.g. chair, director or owner)	Owner/Manager	

Other useful Pre-school Learning Alliance publications

Safeguarding Children (2013)

Employee Handbook (2012)

Review record.

Date reviewed	comments	Sign	Next review
Oct 2019	No Changes	DP 2019	Oct 2020
Oct 2020	No Changes	DP 2020	Oct 2021
Nov 2021	Changed mobile phone storage rules	DP 2021	Nov 2022