Safeguarding and Welfare Requirement: **Child Protection** Providers must have and implement a policy, and procedures, to safeguard children.

1.6 Online safety (inc. mobile phones 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.

Procedures

- Our designated person is responsible for co-ordinating action taken to protect children is:
  EYFS **Designated Safeguarding Officer** (Manager) – Katarina Turbe
  1st Additional Safeguarding Lead (Deputy/Business Manager) – Anna Cranidge
  2nd Additional Safeguarding Lead (Senior Lead Practitioner) – Sam Eilertsen
  3rd Additional Safeguarding Lead (EYFS Leader/Director) – Jennifer Walker

---

Information Communication Technology (ICT) equipment

- Only ICT equipment belonging to the setting is used by staff and children.
- The **Designated Safeguarding Officer** is responsible for ensuring all ICT equipment is safe and fit for purpose.
- All computers have virus protection installed.
- The **Designated Safeguarding Officer** 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 **at the time of registration.**

- The **Designated Safeguarding Officer** 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
- All staff (directed by the Management & Leadership team) 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 Safeguarding Officer with the Directors** will ensure that no inappropriate material is stored on it before children use it.
- All IT devices for use by children are located in an area clearly visible to staff.
- Children and staff 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 Safeguarding Officer** 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 in ratio for supervising children.

- Staff send personal information by encrypted email and share information securely at all times – all email correspondence from the team must go through the management & Leadership team or the business manager via the office email address for security.

Mobile phones – children

- Children **do not bring mobile phones or other wearable 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 and other wearable ICT devices** are not used where children are present and must be kept in our secure area. They can be used during lunch or rest breaks (in our separate staff room). Calls may be made/taken outside of the building during these breaks (staff are required to use an agreed area, away from the building and children at play to take calls at this time). **Staff are expected to give the setting's telephone number as an emergency contact for urgent messages during working hours.**
- In an emergency, personal mobile phones may be used in an area where there are no children present, with permission from the management and leadership team.
- 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.
- Visitors will be asked to leave their mobile phones in reception for the duration of their visit. Trades people will be onsite for emergency (and minimal) periods while children are also in the building. In these circumstances all staff are made aware of their presence and keep children from the area requiring attention. Necessary trade calls will be made in the car park area away from all 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 must not bring their personal cameras or video recording equipment into the setting.
- Setting ipads should be used in an appropriate and safe manner at all times for EyLog & EyMan purposes and always linked to learning (see below). Photographs/videos should only ever be recorded in base rooms or in the outdoor learning areas. Ipads should not be taken into the toilet area under any circumstances.

- 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 & separate EyLog/EyMan consent forms). Such use is monitored by the management and Leadership team.
- 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.
- 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 Safeguarding Officer** 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 an educator 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.

Electronic learning journals for recording children's progress

- Staff seek permission from the Management team prior to accessing any online learning journal in its full capacity (eg for report collation or parent meetings). This would only be accessed while on the nursery premises. Training is completed with details on how the learning journal is managed to ensure children are safeguarded. Lead educators oversee daily additions from staff within base rooms and a member of Management & Leadership check observations before they are 'released to parents' via the direct App.

- Only Management & Leadership may use secure access to check the learning journals while working from home.
- 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/
- Safeguarding Children (Pre-school Learning Alliance 2013)
- The New Early Years Employee Handbook (Pre-school Learning Alliance 2019)

This policy was adopted by	Sparkling Minds Pre-school & Day Nursery
On	2nd January 2021
Record of review dates:	Dates electronically saved securely & also on hard copy on site