E-safety

(including all electronic devices with imaging and sharing capabilities)

Online Safety

It is important that children and young people attending Stepping Stones Pre-school receive consistent messages about the safe use of technology and can recognise and manage the risks posed in both the real and the virtual world.

I.C.T Equipment

- The managers at Stepping Stones Pre-school ensures that all computers have up-to-date virus protection installed.
- Tablets are only used by practitioners at Stepping Stones Pre-school for the purposes of observation, assessment, and planning and to take photographs for individual children's learning journeys.
- Tablets remain on the premises and are always password protected.
- Staff follow the additional guidance provided with the system

Internet access

- Children never have unsupervised access to the internet.
- The centre manager and business manager ensures that risk assessments in relation to e-safety are completed.
- Only reputable sites with a focus on early learning are used (e.g. CBeebies).
- Children are taught the following stay safe principles in an age-appropriate way:
  - only go online with a grown up
  - be kind online **and** 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
- Staff at Stepping Stones Pre-school support children's resilience in relation to issues they may face online, and address issues such as staying safe, appropriate friendships, asking for help if unsure, not keeping secrets as part of social and emotional development in age-appropriate ways.

- All computers for use by children are sited in an area clearly visible to staff.

The setting manager ensures staff have access to age-appropriate resources to enable them to assist children to use the internet safely.

Strategies to minimise risk include:

- Check apps, websites and search results before using them with children.
- Children in Early Years are always supervised when accessing the internet.
- Ensure safety modes and filters are applied - default settings tend not to ensure a high level of privacy or security. But remember you still need to supervise children closely.
- Role model safe behaviour and privacy awareness. Talk to children about safe use, for example ask permission before taking a child's picture even if parental consent has been given.
- Check privacy settings to make sure personal data is not being shared inadvertently or inappropriately. (source: https://www.gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-guidance-for-practitioners

Personal mobile phones – staff and visitors (includes internet enabled devices)

- Personal mobile phones have to be kept in the staff room or the office during working hours. No mobile phones can be taken into any of the children's rooms while children are in attendance. Visitors are always asked to leave their phones in a cupboard in the entrance area.
- In an emergency, personal mobile phones may be used in the privacy of the office with permission.
- Staff ensure that contact details of the setting are known to family and people who may need to contact them in an emergency.
- Members of staff do not use personal equipment to take photographs of children.

Cameras and videos

- Members of staff do not bring their own cameras or video recorders to the setting.

- Photographs/recordings of children are only taken for valid reasons, e.g. to record learning and development, or for displays, and are only taken on equipment belonging to the setting.
- Camera and video use is monitored by the centre manager.
- Parents/carers are allowed to take photographs/videos as special events but the centre manager, business manager or room leader will always confirm this at the beginning of the event and Parents are told they do not have a right to upload photos of anyone else's children.
- Photographs/recordings of children are only made if relevant permissions are in place.
- If photographs are used for publicity, parental consent is gained and safeguarding risks minimised, e.g. children may be identified if photographed in a sweatshirt with the name of their setting on it.

Cyber Bullying

If staff become aware that a child is the victim of cyber-bullying at home or elsewhere, they discuss this with the parents and refer them to help, such as: NSPCC Tel: 0808 800 5000 www.nspcc.org.uk or ChildLine Tel: 0800 1111 www.childline.org.uk

Use of social media

Staff are expected to:

- understand how to manage their security settings to ensure that their information is only available to people they choose to share information with
- ensure Stepping Stones pre-school is not negatively affected by their actions and do not name the setting
- are aware that comments or photographs online may be accessible to anyone and should use their judgement before posting
- are aware that images, such as those on Snapshot may still be accessed by others and a permanent record of them made, for example, by taking a screen shot of the image with a mobile phone
- observe confidentiality and refrain from discussing any issues relating to work
- not share information they would not want children, parents or colleagues to view
- set privacy settings to personal social networking and restrict those who are able to access

- report any concerns or breaches to the designated safeguarding lead in their setting

Use/distribution of inappropriate images

- Staff are aware that it is an offence to distribute indecent images and that it is an offence to groom children online. In the event of a concern that a colleague at Stepping Stones Pre-school is behaving inappropriately, staff advise the designated safeguarding lead.