11 Safeguarding

# 11.03 E-safety (including all electronic devices with internet capacity)

**Online Safety**

It is important that children and young people receive consistent messages about the safe use of technology and are able to recognise and manage the risks posed in both the real and the virtual world.

Terms such as ‘e-safety’, ‘online’, ‘communication technologies’ and ‘digital technologies’ refer to fixed and mobile technologies that adults and children may encounter, now and in the future, which allow them access to content and communications that could raise issues or pose risks.The issues are:

*Content* – being exposed to illegal, inappropriate or harmful material

*Contact* – being subjected to harmful online interaction with other users

*Conduct* – personal online behaviour that increases the likelihood of, or causes, harm

**I.C.T Equipment**

* The setting manager ensures that all computers have up-to-date virus protection installed.
* Tablets are only used 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 stored securely at all times when not in use.
* Children only have access to the children’s ‘Safe’ area on the interactive tablet.

**Internet access**

* Children never have unsupervised access to the internet.
* The setting 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).
* Video sharing sites such as YouTube are not accessed unless with adult supervision for learning purpose.
* 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 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.
* 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/).

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

**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](http://www.nspcc.org.uk) or ChildLine Tel: 0800 1111 [www.childline.org.uk](http://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 the organisation 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
* not accept service users/children/parents as friends, as it is a breach of professional conduct
* report any concerns or breaches to the designated person in their setting
* not engage in personal communication, including on social networking sites, with children and parents with whom they act in a professional capacity. There may be occasions when the educator and family are friendly prior to the child coming to the setting. In this case information is shared with the manager and a risk assessment and agreement in relation to boundaries are agreed

**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 is behaving inappropriately, staff advise the designated person who follow procedure Allegations against staff, volunteers or agency staff.