6. Safeguarding Children, Young People and Vulnerable Adults Procedures

6.9 Online 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
Commerce – risk of gambling and inappropriate advertising, phishing and/or scams

Information and guidance regarding online safety is shared with parents via newsletters and individual cases for concern are dealt with in line with our safeguarding procedures.

I.C.T Equipment

- The setting manager ensures that all computers have up-to-date virus protection installed.
- All staff sign an Electronic Device User Agreement which includes ALL electronic devices with imaging and sharing capabilities,
- Staff Tablets are used for the purposes of observation, assessment and planning and to take photographs for individual children's learning journeys.
- Childrens Tablets are used to support children's learning. This is only done on a 'child' profile meaning no access to the internet is possible and the education apps are age appropriate and relevant.

- Tablets remain on the premises and are stored securely at all times when not in use, unless permission is sought from the Manager
- The interactive whiteboard has access to the internet. The whiteboard is used under adult supervision. Any content shared is age appropriate.

Internet access

- Children never have unsupervised access to the internet.
- 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 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.
- 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.

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

Electronic Devices – staff and visitors (includes internet enabled devices and devices with imaging and sharing capabilities)

- Tablets are used by staff during working hours, and in accordance with the Electronic Device User Agreement.
- Smart watches can be worn but need to be disabled i.e. airplane mode. This does not include breaks where personal mobiles may be used off the premises or in a safe place e.g. The Den (when children are not present)
- Personal mobile phones are stored in the office or in a lockable cupboard with the staff members' belongings.
- 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.
- Parents and visitors do not use their mobile phones on the premises. There is an exception if a visitor's company/organisation operates a policy that requires contact with their office periodically throughout the day. Visitors are advised of a private space where they can use their mobile.

- Any photos taken by a contractor in order to support maintenance work will be checked by the Manager or Assistant Manager before leaving the premises.
- 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 setting manager.
- Where parents request permission to photograph or record their own children at special events, general permission is first gained from all parents for their children to be included. Parents are told they do not have a right to photograph or upload photos of anyone else's children.
- Photographs/recordings of children are only made if relevant permissions are in place.
- Parents are required to sign a 'Tapestry User Agreement' prior to any accounts being made.
- If photographs are used for publicity, parental consent is gained and safeguarding risks minimised.

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
- not make or accept an invitation to become online friends with parents or other family carers on any social networking site. This applies to all students and bank staff. There may be occasions when the practitioner 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. This also applies to service users and children due to the breach in professional conduct
- 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 Snapchat 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 gain access
- 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.

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 in '6.2 Allegations Against Staff, Volunteers or Agency Staff'.