6 Safeguarding children, young people and vulnerable adults procedures

6.9 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 (Includes all equipment, devices and equipment even if not expressly mentioned)

- The setting managers ensures that all computers / laptops / tablets / devices and equipment have up-to-date virus protection installed.
- Tablets / computers / laptops / devices and equipment are only used for the purposes of observation, assessment and planning and to take photographs for individual children's learning journeys and for legitimate education and business purposes.
- Tablets / computers / laptops/ devices and equipment are stored securely at all times when not in use.
- Tablets / computers / laptops / devices and equipment can be removed from the premises with specific permission from the settings managers but only to be used by employees for authorised for business purposes.
- Staff follow the additional guidance provided with the system.
- Regular checks and monitor is completed on all equipment.
- All staff complete yearly E safety training.

Internet access

- Children never have unsupervised access to the internet.
- The setting managers 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 due to the risk of inappropriate content.
- 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.

Personal mobile phones, Smart watches and all other internet enabled devices. – staff and visitors

- Personal mobile phones smart watches and all other internet enabled devices are not used by staff during working hours. This does not include breaks where personal mobiles may be used off the premises or in a safe place e,g, staff room / office. The setting managers completes a risk assessment for where they can be used safely.
- Personal mobile phones, smart watches and all other internet enabled devices are ideally switched off and stored in the office or in staff's lockers in the staff room. No devices are worn during working hours.
- In an emergency, personal mobile phones may be used in the privacy of the office / staff room 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.
- Staff do not take their mobile phones on outings, unless the device is required for their personal medical needs (eg diabetes monitoring device). On outings a personal device needed for medical needs are stored in a separate designated bag
- Members of staff do not use personal equipment to take photographs of children, store details or any records or data about children, or the setting.
- Parents and visitors do not use their mobile phones or other internet enabled or recording devices on the premises, unless in a designated area ie office or staff room. There is an exception if a visitor's company/organisation operates a policy that requires contact with their office periodically throughout the day, where phones etc can be left in the office switched on. Visitors are advised of a private space where they can use their mobile.

Cameras and videos

- Members of staff do not bring their own cameras or video recorders to the setting. Hired devices are checked and where possible storage devices / SD cards owned by Acorn Pre-School & The Mighty Oaks are used.
- Photographs/recordings of children are only taken for valid reasons, e.g. to record learning and development, or for displays, school photos and are only taken on equipment belonging to the setting or hired from a reputable company with appropriate policies.
- 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. Permissions are obtained as part of the registration process.

- If photographs are used for publicity, social media, marketing specific 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.

Social Media

- Staff must not access their personal social media/messaging accounts on computers/tablets or devices that are property of Acorn Pre-School & The Mighty Oaks.
- 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 Acorn Pre-School & The Mighty Oaks 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 Manager.
- Staff are advised to avoid personal communication, including on social networking sites, with the children and parents with whom they act in a professional capacity.
- If a staff member and / or family are friendly prior to the child coming into Acorn Pre-School & The Mighty Oaks, this information is shared with the Manager prior to a child attending and an agreement in relation to boundaries can be agreed.

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/ photo editing apps/ screen recording apps 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 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

Access to the Internet

- Hardware owned, leased, rented or otherwise provided by staff may be connected to the internet only by arrangement with, and the explicit approval of the Managers/Committee.
- Limited use of email and internet facilities for personal purposes is permitted, ie during breaks and in emergencies.

- Personal use and downloads, permission must be gained before downloading apps or files and they must not be from inappropriate or illegal sources i.e. films.

Random periodic checks will take place to ensure compliance with this policy and procedure.

Breaches of our Online Safety policy

- Any breach of this Online E-Safety policy will be dealt with promptly and may result in disciplinary action being taken as set out in our Discipline and Dismissal Policy.

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/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 **6.2** Allegations against staff, volunteers or agency staff.