

06 – Safeguarding Children, Young People & Vulnerable Adults

06.9 – E-Safety And Devices

Children today use technology everywhere — at home, in the community, and sometimes in early years settings. It's important that they learn safe habits early and that adults around them use technology safely too.

This policy covers ALL electronic devices with internet access or cameras (phones, tablets, laptops, cameras, smart watches etc.).

What Does “Online Safety” Mean?

Children and adults can face three types of online risk:


1. Content

Material that is harmful, inappropriate or illegal.

 *Examples:* violent videos, unsuitable websites, extremist content, sexual content.

2. Contact

Being contacted by someone online in a harmful way.

 *Examples:* strangers messaging, bullying, grooming.

3. Conduct

Behaviour online that could hurt themselves or others.

 *Examples:* sharing private information, sending unkind messages.

ICT Equipment in Our Setting

We keep all technology safe, secure and well-managed:

- ✓ All setting computers have updated virus protection
- ✓ Tablets are only used for:
 - Observations and assessment
 - Planning

- Taking photos for Family to share with parents
- ✓ Tablets are:
- Kept on-site only
 - Stored securely
 - Used following strict internal guidance





Internet Use

Children never go online without an adult next to them.

We make sure:

- ✓ Only safe, reputable early-years websites are used (e.g. *CBeebies*)
- ✓ YouTube or video sites are checked fully by staff first
- ✓ Devices children access are always in full view of staff
- ✓ Risk assessments for online safety are completed

Children learn simple online safety rules:

-  “Only go online with a grown-up”
-  “Be kind online and keep information about me safe”
-  “Only click on things I understand”
-  “Tell a grown-up if anything makes me sad or worried”

We also help children build resilience — including friendships, staying safe, asking for help, and not keeping unsafe secrets.

If staff spot inappropriate or dangerous online content, they report it to:

👉 Internet Watch Foundation – www.iwf.org.uk

We also send out termly tips to families on the importance of E-safety

How We Reduce Online Risks

We always:

- ✓ Check apps, websites, videos and search results BEFORE using them
- ✓ Apply safety filters
- ✓ Supervise children closely
- ✓ Teach safe behaviour (e.g. asking permission before taking photos)
- ✓ Use home visits or all about me questionnaires to understand a child’s digital

world

- ✓ Check privacy settings on all devices

Personal Mobile Phones & Internet-Enabled Devices including smart watches and any devices with camera access

To keep children safe:

For Staff:

- Personal mobiles/devices are not used in working hours
- Must be switched off and stored in the office
- Allowed only off-site or in staff room during breaks
- Can be used in the office during an emergency with permission
- Staff give family the setting phone number for emergencies
- Staff do not bring personal phones on outings
- No personal equipment is used to take photos
- Smart watches may be worn but must be disconnected from other devices and have no camera or internet access.

For Parents & Visitors:

- No mobile phone use in any childcare area
- If work requires contact, their phone stays stored safely and they use a private space
- The setting's phone number is given for urgent contact

For the Setting:

- We use a work mobile device for setting business only

Cameras and Videos

- ✓ Only setting-owned equipment is used
- ✓ Photos/videos are taken only for valid reasons:
 - Learning observations
 - Displays
- ✓ Children are asked for their own consent, even if parents have already given permission

- ✓ Photo use is monitored by the manager
- ✓ Parents can photograph their child at events only if:
 - ALL parents give permission
 - They do not upload images of other children
- ✓ For publicity photos:
 - We always ask parent permission
 - We avoid risks (e.g. not showing setting names on clothing)

Cyberbullying

If we learn that a child is affected by cyberbullying at home or elsewhere, we:

- Talk to parents
- Offer support and guidance
- Signpost to help:

 NSPCC: 0808 800 5000

 Childline: 0800 1111

Staff Use of Social Media

All staff must:

- ✓ Set strong privacy settings
- ✓ Protect confidentiality
- ✓ Never name the setting online
- ✓ Think carefully before posting anything
- ✓ Never discuss work or children online
- ✓ Never post images relating to the setting
- ✓ Never accept parents or children as “friends”
- ✓ Report concerns about online conduct immediately
- ✓ Follow safer-use agreements if they knew the family socially beforehand

Inappropriate or Illegal Images

Staff understand that:

- Sharing or possessing indecent images is a criminal offence
- Grooming online is a criminal offence



- Any concerns must be reported to the Designated Safeguarding Lead immediately
- Procedure 06.2 (Allegations against Staff) will then be followed