



Smalley Pre-school E-safety Policy

(Registered Charity No. 1033193)

Church Hall, Main Road, Smalley, Ilkeston, Derbyshire DE7 6EF
07903 129575

This policy relates to 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.

ICT equipment

- The setting manager ensures that all computers have up-to-date virus protection installed.
- Tablets are only used under direct supervision and are not connected to the internet.
- Tablets remain on the premises and are stored securely at all times when not in use.
- Staff follow the additional guidance provided with any equipment and systems.

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 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 safe.
 - 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 and not keeping secrets as part of social and emotional development in age-appropriate ways.
- Staff report any suspicious or offensive material, including material that 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.

Strategies to minimise risk include:

- Checking apps, websites and search results before using them with children.
- Children in early years should always be supervised when accessing the internet.
- Ensuring safety modes and filters are applied – default settings tend not to ensure a high level of privacy or security. However, children still need to be supervised closely.
- Role-modelling 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.
- Making use of home visits to inform understanding of how technology is used within the home and the context of the child with regard to technology.
- Checking privacy settings to make sure personal data is not being shared inadvertently or inappropriately.

Source: [Safeguarding Children and Protecting Professionals In Early Years Settings: Online Safety Guidance For Practitioners](#) (UK Council for Internet Safety, 2019)

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

- Personal mobile phones and 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. the kitchen). The setting manager completes a risk assessment for where they can be used safely.
- Personal mobile phones are switched off and stored in lockers or a locked office drawer.
- Wearable technology must be placed in airplane mode.
- In an emergency, personal mobile phones may be used in privacy 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.
- 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. Phones still should be stored away from any areas that children access and the setting phone number given to visitors so that they are still contactable. Visitors are advised of a private space where they can use their mobile phones.

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 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. Children are given the opportunity to consent to their photograph being taken, even if parent/carer permissions are in place.
- If photographs are used for publicity, parental consent is gained and safeguarding risks minimised (e.g. photos do not include children's faces).

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 the organisation is not negatively affected by their actions and do not name the setting;
- be aware that comments or photographs online may be accessible to anyone and should use their judgement before posting;
- be 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 screenshot of the image with a mobile phone;
- observe confidentiality and refrain from discussing any issues relating to work on social media;
- 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 new friends, as it is a breach of professional conduct;
- report any concerns or breaches to the designated safeguarding lead in the setting; and
- 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.

The only exception to the personal communication clause above is where a parent is a member of the committee and communication is required relating to the running of the pre-school.

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 safeguarding lead, who follows the procedure for allegations against staff, volunteers or agency staff.

This policy was adopted by Smalley Pre-school

On	23.12.25
Date to be reviewed	23.12.26
Signed on behalf of the provider	
Name of signatory	Joanne Rothwell
Role of signatory (e.g. chair, director or owner)	Chair of the Committee