CODICOTE PRE-SCHOOL

ST. GILES PARISH CENTRE, BURY LANE, CODICOTE SG4 8XX +44 (0)7542 285 412

E-Safety Policy

This policy refers to all electronic devices with internet capability.

Online Safety

It is important that children and young people receive consistent messages about the safe use of technology and can 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 used for the purposes of observation, assessment and planning and to take photographs for individual children's learning journeys.
- If the children use tablets, it is under the supervision of staff in an adult-led activity.
- Staff check beforehand any content to be used on the tablets with the children before the children are given access.
- Tablets remain on the premises and are stored securely at all times when not in use.
- Staff follow the additional guidance provided by each website.

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, not keeping secrets as part of social and emotional development in age-appropriate ways.
- All computers for use by children are situated in an area clearly visible to staff.
- Staff report to the Designated Safeguarding Lead(s) (DSL) 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 and Devices – Staff and Visitors (including internet enabled devices and smart watches).

- Personal mobile phones 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. The setting manager completes a risk assessment for where they can be used safely.
- Smart watches are not to be worn during working hours
- Personal mobile phones are stored in kitchen on silent in your bag or box
- In an emergency, personal mobile phones may be used in the privacy of the office with permission.
- Staff are to ensure that the contact details of the setting are known to family and people who may need to contact them in an emergency. The contact phone number is: **07542 285412**.
- Staff may take their mobile phones on outings for necessary communication only with permission.
- Members of staff do not use personal equipment to take photographs of children.
- Parents and visitors do not use their mobile devices 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.

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.
- If photographs are used for publicity, parental consent is gained and safeguarding risks minimised, e.g. children's names are not used.

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

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.

- 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 access it.

  not accept service users/children/parents as friends, as it is a breach of professional conduct unless prior acquaintances.

  In the case of prior acquaintances, information needs to be shared with the manager and a risk assessment and agreement in relation to boundaries are agreed.

- report any concerns or breaches to the DSL(s) 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 needs to be 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 06.2 Allegations against staff, volunteers or agency staff.

Date policy was written	March 2024
Policy last reviewed/amended	February 2025
The date the policy is due for review	February 2026