e-Safety Policy
(Including mobile phones & cameras)

Policy Statement

At Chudleigh Knighton Pre-school we believe that children flourish best when they are offered the opportunity to experience using different forms of Information Communication Technology (ICT) We ensure that access to this technology is safe and protected.

Aim

We aim to teach children to use technology in a safe manner. We ensure the programmes that the children have access to are suitable for their development level and that we support their learning in this area.

Procedures

We will appoint an e-Safety coordinator. This will be the designated Safeguarding Coordinator as it is considered that the roles overlap. This is not a technical role.
The e-Safety coordinator is Mandy Davey with technical support from the Office manager.

This e-Safety policy has been written by the pre-school, building on guidance from the government & Early Years Alliance. It has been agreed by the management team and will be reviewed annually, or earlier if changes to legislation so require.
This policy is drawn up to protect all parties – the children, the staff and the pre-school, and aims to provide clear advice and guidance on how to minimise risks and how to deal with infringements.

Equipment

- Only ICT equipment belonging to the setting is used by staff & children.
- The e-safety coordinator is responsible for ensuring all ICT equipment is safe & fit for purpose.
- All computers have virus protection installed/windows defender**.**
- **S**afety settings are activated to ensure inappropriate material cannot be accessed.
- If a second-hand computer is purchased or donated to the setting, the designated person will ensure that no inappropriate material is stored on it before children use it.

Internet Access

- Children do not normally have access to the internet and never have unsupervised access.
- The designated person has overall responsibility for ensuring that children and young people are safeguarded and risk assessments in relation to online safety are completed.
- Children are taught the following stay safe principles in an age-appropriate way prior to using the internet.
- Only go online with a grown up
- Be kind online.
- 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
- All computers for use by children are located in an area clearly visible to staff.
- Children are not allowed to access social networking sites.

- 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.
- Suspicions that an adult is attempting to make inappropriate contact with a child on-line is reported to the National Crime Agency's Child Exploitation and Online Protection Centre at www.ceop.police.uk**.**
- The designated person ensures staff have access to age-appropriate resources to enable them to assist children to use the internet safely.
- If staff become aware that a child is the victim of cyber-bullying, they discuss this with their parents and refer them to sources of help, such as the NSPCC on 0808 800 5000 or www.nspcc.org.uk, or Childline on 0800 1111 or www.childline.org.uk.

E-mails

- Children are not permitted to use email in the setting. Parents and staff are not normally permitted to use setting equipment to access personal emails.
- Staff do not access personal or work email whilst supervising children.
- Staff send personal information by encrypted email and always share information securely.

Mobile Phones/Devices – Children.

- Children do not bring mobile phones or other ICT/gaming devices with them to the setting. If a child is found to have a mobile phone or device with them, this is removed and stored in the office until the parent collects them at the end of the session.

Mobile phones – staff and visitors

- Personal mobile phones are not used by staff on the premises during working hours. They will be stored in the kitchen.
- In an emergency, personal mobile phones may be used in an area where there are no children present, with permission from the manager.
- Our staff and volunteers ensure that the setting telephone number is known to family and other people who may need to contact them in an emergency.
- The pre-school mobile phone is taken on outings, for use in case of an emergency, it is never used to make or receive personal calls or take photographs of children.
- Parents and visitors are requested not to use their mobile phones whilst on the premises and to leave them in the foyer. We make an exception if a visitor's company or organisation operates a lone working policy that requires contact with their office periodically throughout the day. Visitors will be advised of a quiet space where they can use their mobile phone, where no children are present.
- These rules also apply to the use of work-issued mobiles, and when visiting or supporting staff in other settings.

Cameras and videos

- Our staff and volunteers must not bring their personal cameras or video recording equipment into the setting.
- Photographs and recordings of children are only taken for valid reasons i.e., to record their learning and development, or for displays within the setting, with written permission received by parents (see the Registration form). Such use is monitored by the manager.
- Where parents request permission to photograph or record their own children at special events, general permission is gained from all parents for their children to be included. Parents are advised that they do not have a right to photograph anyone else's child or to upload photos of anyone else's children.
- If photographs of children are used for publicity purposes, parental consent must be given and safeguarding risks minimised.
  Photographs that include pupils will be selected carefully so that individual children cannot be identified or their image mis-used. Where possible we will use group photos rather than full face photos of individual children.

Social media

- 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 or parents as friends due to it being a breach of expected professional conduct.
- If staff name the organisation or workplace 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 designated person in their setting.
- Staff avoid personal communication, including on social networking sites, with the children and parents with whom they act in a professional capacity. If a practitioner and family are friendly prior to the child coming into the setting, this information is shared with the manager prior to a child attending and a risk assessment and agreement in relation to boundaries is agreed.

Use and/or distribution of inappropriate images

- Staff are aware that it is an offence to distribute indecent images. In the event of a concern that a colleague or other person is behaving inappropriately, the Safeguarding Children and Child Protection policy, in relation to allegations against staff and/or responding to suspicions of abuse, is followed.
- Staff are aware that grooming children and young people online is an offence in its own right and concerns about a colleague's or others' behaviour are reported (as above).

Further guidance

- NSPCC and CEOP *Keeping Children Safe Online* training: www.nspcc.org.uk/what-you-can-do/get-expert-training/keeping-children-safe-online-course/

Protecting personal data

Personal data will be recorded, processed, stored and made available in accordance to the Data Protection Act 1998

Assessing risk

The pre-school will take reasonable precautions to ensure e-Safety. However, due to the scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The pre-school cannot accept liability for material accessed, or any consequences of internet access.
The pre-school will regularly check ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate and effective.

Handling e-Safety complaints

Staff are given information about infringements in use and possible sanctions.
Complaints of ICT misuse will be dealt with by the e-Safety Co-ordinator and Directors.
Any complaint about staff mis-use will be referred to the Manager, Mandy Davey and in her absence the Deputy Manager, Karen Gwillam

Staff and the e-Safety policy

All staff will be given the Pre-School e-Safety Policy and its importance explained.
Staff will always use a child friendly safe search engine when accessing the web.
Staff use of the lap top will be monitored and regularly reviewed by the e-Safety coordinator.
This policy and the importance of its content will be discussed with staff during regular supervisions and yearly appraisals.

Parents' and carers' support
Parents' and carers' attention will be drawn to the pre-school e-Safety Policy in newsletters, the pre-school information pack and the pre-school website.
Staff, parents and volunteers are also requested to read the Safeguarding Children's policy in conjunction with this e-Safety Policy.
Children in our care do not use the internet without adult supervision.

This policy was adopted at a meeting of the pre-school committee held on (date)

Signed on behalf of the Pre-school Management Committee

Please print name and title

Signed by Pre-school Manager/ deputy manager

Please print name and title
