



Online Safeguarding Policy (incl. mobile phones, cameras and social networking)

Policy Statement

Ditton Church Pre-School take steps to ensure that there are effective procedures in place to protect children, young people and vulnerable adults from the unacceptable use of Information Communication Technology (ICT) equipment or exposure to inappropriate materials in the setting.

Procedures

- Our designated person responsible for co-ordinating action taken to protect children is: Wendy Caldicott
- Our second named designated person responsible for co-ordinating action taken to protect children is: Alison Pestell
- Our named committee representative responsible for safeguarding children is: Caroline Gibbons

Information Communication Technology (ICT) Equipment

- Only ICT equipment belonging to the setting is used by staff and children within the setting. This includes tablet computers which are kept on airplane mode to prevent access to the internet. The designated person is responsible for ensuring all ICT equipment is safe and fit for purpose.
- If staff are completing report writing on home computers, they must be encrypted as well as password protected and must only be transferred to the setting via an encrypted memory stick
- All computers have virus protection installed.
- The designated person ensures that safety settings are set to ensure that inappropriate material cannot be accessed.



Internet Access

- Children do not have access to the internet and never have unsupervised access to computers.
- If staff access the internet for the purposes of promoting children's learning, they will ensure content is age appropriate.
- The designated people have 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
 - children are taught about online safety through age-appropriate books, such as 'Penguin Pig', 'Smartie the Penguin', 'It's a Book', 'Chicken Clickin' and 'Dot'
 - information is shared with parents on how to keep their children safe online, via our website, noticeboard and secret Facebook page
- If a secondhand computer or tablet is purchased or donated to the setting, the designated person will ensure that no inappropriate material is stored on it before children use it
- All computers or tablets for use by children are located 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
- 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. (Although children are not allowed access to the internet in Pre-School staff are alert to comments children may make about something that has happened at home or to an older sibling)



Email

- 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 via a secure email address and share information securely at all times.

Only leadership staff and administrators will have access to passwords and only these staff will contact parents via email.

Mobile Phones, Smartphones and Smart Devices – Staff and Visitors

- Personal mobile phones, smartphones and all other smart devices with cameras, are not used by our staff whilst supervising children. They will be stored in the designated place (basket in kitchen) and must only be used away from children.
- 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.
- If our members of staff or volunteers take their mobile phones/smartphones on outings, for use in case of an emergency, they must not make or receive personal calls, or take photographs of children.
- Parents and visitors are requested not to use their mobile phones/smartphones whilst on the premises. Visitors will be advised of a quiet space, i.e. lounge, where they can use their mobile phone, where no children are present

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
- 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, for example, ensuring children cannot be identified by name.



- Occasionally children may be allowed to use cameras to record things of interest to them, but this would always be under staff supervision.

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 and parents as friends due to it being a breach of expected professional conduct.
- In the event that 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.
- Our Pre-School Facebook group will be set as a Secret Group and controlled by two administrators: Wendy Caldicott, Pre-School Supervisor and DSL and Sandie Thomas, Childcare Development Practitioner. Only current Pre-School children's parents or guardians, committee members and staff will be part of this group.

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/
- Useful links
- Childnet
- www.getsafeonline.org
- Internetmatters.org
- NSPCC – Be Share Aware video

Useful Contacts: Rebecca Avery (Safeguarding Advisor Online Protection) Tel: 03000 415797 or 07789968705

This policy was adopted by the: Ditton Church Pre-School Management Committee

Date: April 2022

Signed on behalf of the Management Committee:

Role of signatory: Chair of Management Committee

Next review date: April 2023