



1.6 Online safety (inc. all devices/technology with imaging and sharing capability)

Policy statement

We 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 Safeguarding Leads (DSL) responsible for coordinating action taken to protect children are:

Alice Clark & Sharron Sheppard

Information Communication Technology (ICT) equipment

- Only ICT equipment belonging to the setting is used by staff and children.
- The DSL is responsible for ensuring all ICT equipment is safe and fit for purpose.
- All computers have virus protection installed.
- The designated person ensures that safety settings are set to ensure that inappropriate material cannot be accessed in line with KCSIE guidance on Filtering & Monitoring.

Internet access

- Children DO NOT have unsupervised access to the internet
- If staff access the internet with children for the purposes of promoting their learning, written permission is gained from parents via their Childcare Agreement.
- The DSL have overall responsibility for ensuring that children and young people are safeguarded and risk assessments in relation to online 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 safely

- 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.

On rare occasions where fully supervised access to the internet is granted the following strategies will be applied to minimise the risks:

Strategies to minimise risk include:

- Check apps, websites and search results before using them with children.
- Children in Early Years should always be supervised when accessing the internet.
- Ensure safety modes and filters are applied - default settings tend not to ensure a high level of privacy or security. But remember you still need to supervise children closely.
- Role model 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.
- Make use of home visits to inform your understanding of how technology is used within the home and the context of the child with regards to technology.
- Check privacy settings to make sure personal data is not being shared inadvertently or inappropriately. (source: <https://www.gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-guidance-for-practitioners>)

Online safety information is available for parents via our website Safeguarding page and our Parent Handbook.

If a second-hand computer is purchased or donated to the setting, the designated leads will ensure that no inappropriate material is stored on it before children use it, with assistance from Wired4Tech IT.

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

Suspicious 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

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 0800 800 5000 or www.nspcc.org.uk, or Childline on 0800 1111 or www.childline.org.uk.

Email

- 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 share information securely at all times.

Mobile phones – children

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

Mobile phones , smart watches and other devices capable of imaging/sharing – staff and visitors

Personal mobile phones are not used by our staff on the premises during working hours. They will be stored in the nursery office. 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.

We have two nursery owned mobile phones for use in Forest School and on outings. Staff are also recommended to take a personal mobile phone on Tractor Trailer, Forest School, Farm Walk or other outings as a back-up for emergency use. In our rural setting there can be issues with mobile phone signals – a wider choice of phone networks being available will increase the chance of being able to contact the emergency services when needed.

Parents and visitors are requested not to use their mobile phones whilst on the premises. 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.

Smart watches & other devices may be worn by staff, but must not be used to answer calls, messages, or emails whilst in the classroom. They may be used in the Office whilst staff are on breaks. Whilst many smart watches are capable of taking pictures, they photograph what is seen by the connected phone rather than the watch itself – As staff phones are always safely stored in their bags in the office this is not deemed to be a risk.

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. Parents inform us via the Childcare Agreement how they are happy for us to use their child's image. Permission is requested for use of images on our Instagram page, website and in our Newsletter. [Children are given the opportunity to consent to their photograph being taken, even if parent/carers permissions are in place.](#)

At events parents are advised that they can take pictures, but must not upload them to social media without the permission of the parents of the children in the image.

If photographs of children are used for publicity purposes, parental consent must be given, via the Childcare Agreement, and safeguarding risks minimised, for example, ensuring children cannot be identified by name or through being photographed in their smock with a name on.

Social media

See Employee Handbook

Electronic learning journals for recording children's progress

Our learning journals and data for child progression are held online via a password protected application. Each device is registered as an app user and so if the app is accessed outside of this device our software provider My Montessori Child will notify us. Access to the app is removed if a member of staff leaves the setting.

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/
- [CEOP Education \(thinkuknow.co.uk\)](http://thinkuknow.co.uk)

This policy was adopted by	The Willow On The Farm Nursery	
On	15 th July 2019	
Review Frequency	Annually or sooner if required	
Drawn up on behalf of the provider by	Dawn Wilson-Fry	

Deputy Manager

Reviewed

25/08/2021 DWF

27/06/2022 DWF

16/12/2022 NJR

23/01/2024 NJR

10/08/2025 NJR