

Safeguarding and Welfare Requirement: Child Protection

The safeguarding policy and procedures must include an explanation of the action to be taken in the event of an allegation being made against a member of staff and cover the use of mobile phones and cameras in the setting.



1.6 Online safety (inc. mobile phones and cameras)

Policy statement

We recognise that online safety is a safeguarding issue not an ICT issue and includes safety at home as well as nursery. The internet is used at Jolly Tots to promote children's' achievements and support the professional work of staff, including training. It is essential in modern 21st century life to enhance education and practice and it is our responsibility to 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 our setting.

Procedures

- Our designated person responsible for co-ordinating action taken to protect children is:

Amy Jowett, Ginny Jowett and Lee Davison

- The internet is now regarded as an essential resource to support teaching and learning, and for communication purposes.

Information Communication Technology (ICT) equipment

- Only ICT equipment belonging to the setting is used by staff and children.
- The designated person 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.

Internet access

- Children do not normally have access to the internet and never have unsupervised access.
- If staff access the internet with children for the purposes of promoting their learning, written permission is gained from parents who are shown this policy.

- 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 on line with a grown up
 - be kind on line
 - 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
- Designated persons will also seek to build children's resilience in relation to issues they may face in the online world, and will address issues such as staying safe, having appropriate friendships, asking for help if unsure, not keeping secrets as part of social and emotional development in age-appropriate ways.
- 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.
- All computers for use by children are 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

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 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 our staff in the rooms or around the children during working hours. They will be stored in lockers. Staff may use their mobile phones at lunchtime in the designated staff room.
- In an emergency, personal mobile phones may be used in an area where there are no children present, with permission from the Person in Charge.
- 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 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 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.

Cameras and videos

- Our staff and volunteers must not bring their personal cameras or video recording equipment into our 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 owner.
- 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.
- Photographs download to the nursery computers/laptop are deleted yearly.

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, unless their friendships were established prior to starting at our setting.
- 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 owner prior to a child attending and a risk assessment and agreement in relation to boundaries is agreed.

Electronic learning journals for recording children’s progress

- A risk assessment is completed with details on how the learning journal is managed to ensure children are safeguarded.
- Staff adhere to the guidance provided with the system at all times.

Website

- Permission is obtained from parents regarding using their child’s photograph on our website.
- Photographs are never accompanied by the child’s name unless permission is given by the parents.
- Named photographs of staff are used with permission from each member of staff and no personal information is disclosed.

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 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/

This policy was adopted by	Jolly Tots Preschool Nursery	<i>(provider)</i>
On	1 st September 2025	<i>(date)</i>
Date to be reviewed	September 2026	<i>(date)</i>
Signed on behalf of the provider	<hr/>	
Name of signatory	Lee Davison	
Role of signatory (e.g., Chair, director or owner)	Manager	
	<hr/>	

Other useful Pre-school Learning Alliance publications

Safeguarding Children (2018)

New Early Years Employee Handbook (2019)

Other guidance

UK council for internet safety – Safeguarding children and protecting professionals in early years settings: online considerations for managers (4th February 2019)