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

Stowey Bears Preschool takes steps to ensure that effective procedures are in place to protect children from online and digital risks, including unacceptable use of Information Communication Technology (ICT), mobile phones, cameras, online learning platforms, social media, connected devices and exposure to inappropriate or harmful materials. This policy supports compliance with the Early Years Foundation Stage (EYFS) statutory framework, Keeping Children Safe in Education where relevant to good safeguarding practice, Working Together to Safeguard Children, local safeguarding partner procedures, the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Children Act 1989 and 2004.

Procedures

- Our designated persons responsible for co-ordinating action taken to protect children are:

  Rachel Penny and Sarah Grubb

  - The designated safeguarding lead and deputy designated safeguarding lead are responsible for ensuring online safety concerns are recorded, risk assessed and escalated in line with the Safeguarding Children and Child Protection policy, including referral to Somerset safeguarding partners, children's social care, the Local Authority Designated Officer (LADO), Ofsted, the police or CEOP where appropriate.

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.

- Filtering, monitoring and security arrangements are reviewed at least annually, and whenever new devices, applications or online services are introduced, to ensure they remain suitable for children's age, stage of development and safeguarding needs.

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.
- Any use of screens, tablets or online content is planned, purposeful, age appropriate, supervised and balanced with children's wider learning, play, physical activity, rest and wellbeing needs.
- 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.
- Staff are alert to the four main areas of online risk: content, contact, conduct and commerce, including harmful content, grooming, bullying, exploitation, misinformation, scams and pressure to share personal information or images.
- 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 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.

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 only send personal or sensitive information by secure, setting-approved systems and only where there is a lawful basis to do so. Passwords must not be shared, accounts must be protected, and any suspected data breach must be reported immediately to the manager or designated person.

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 on the premises during working hours. They will be stored in the office and used on lunch breaks out of the main room and away from the children.
- 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.
- 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. If a parent is staying with their child to help settle them when first transitioning to the preschool, mobile phones must be kept in the office. 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.

- Staff, students, volunteers, contractors and visitors must not use personal devices to take, store or share photographs, videos or information about children. Any breach is treated as a safeguarding concern and may also be managed under disciplinary, whistleblowing, data protection or allegations procedures.

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 i.e. Christmas Nativity, 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 or through being photographed in a sweatshirt with the name of their setting on it.
- Images and recordings are processed in line with UK GDPR and the Data Protection Act 2018. Consent is specific, informed and capable of being withdrawn, and images are stored securely, retained only for as long as necessary, and deleted safely when no longer required.

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.
- 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.

Electronic learning journals for recording children's progress

- Managers seek permission from the senior management team prior to using any online learning journal. 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.
- Before using any online learning journal, app or digital platform, the manager checks privacy, access permissions, data storage, parental access, image-sharing controls and provider terms, and records the decision as part of the setting's data protection and safeguarding arrangements.

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 on line is an offence in its own right and concerns about a colleague's or others' behaviour are reported (as above).
- Concerns involving online grooming, sexual communication with a child, child sexual abuse material, image-based abuse, upskirting, voyeurism or the creation, possession or sharing of indecent images are reported immediately through safeguarding procedures and, where appropriate, to the police, CEOP, the Internet Watch Foundation, Ofsted and the LADO.

Training, monitoring and review

- All staff, students and regular volunteers receive induction and refresher safeguarding training that includes online safety, professional boundaries, use of devices, image handling, data protection, reporting routes and whistleblowing.
- The manager and designated safeguarding lead review this policy annually, and sooner if legislation, statutory guidance, local safeguarding procedures, technology, incidents or setting practice change.

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/
- Voyeurism (offence) Act 2019

- Early Years Foundation Stage statutory framework for group and school-based providers, Department for Education, current version
- Working Together to Safeguard Children, Department for Education, current version
- UK General Data Protection Regulation and Data Protection Act 2018
- ICO guidance on children's information and data protection for early years settings

This policy was adopted by	Stowey Bears Preschool	*(name of provider)*
On	15th July 2026	*(date)*
Date to be reviewed	Reviewed annually	*(date)*
Signed on behalf of the provider	Rachel Penny	
Name of signatory	Julia Jameson	
Role of signatory (e.g. chair, director or owner)	Chairperson	

Other useful Pre-school Learning Alliance publications

Safeguarding Children (2013)

Employee Handbook (2012)