SAFEGUARDING & WELFARE REQUIREMENT: CHILD PROTECTION

1.7 Online Safety and the use of Mobile Phones, Cameras and other Electronic Devices

Policy Statement

St John's Playtime Pre-school takes 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, and from the unacceptable use of mobile phones, cameras and other electronic devices.

It is important that children and young people receive consistent messages about the safe use of technology and can recognise and manage the risks posed in both the real and the virtual world.

Terms such as 'e-safety', 'online', 'communication technologies' and 'digital technologies' refer to fixed and mobile technologies that adults and children may encounter, now and in the future, which allow them access to content and communications that could raise issues or pose risks; the issues are:

Content – being exposed to illegal, inappropriate or harmful material

Contact – being subjected to harmful online interaction with other users

Conduct – personal online behaviour that increases the likelihood of, or causes, harm

Procedures

- Our designated persons responsible for co-ordinating action taken to protect children are:
  Natalie Bailey (Manager and Safeguarding Designated Lead) Sarah Gosling (Deputy Designated Safeguarding Lead) Megan Blanchard (Deputy Designated Safeguarding Lead)

Information Communication Technology (ICT) equipment

- Only ICT equipment belonging to the setting is used by staff and children.
- The designated persons are responsible for ensuring all ICT equipment is safe and fit for purpose.
- All computers have virus protection installed.
- The designated persons ensure 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.

- Our designated persons 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 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
- Our 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 persons 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**.**
- Our designated persons ensure 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.

The setting manager ensures staff have access to age-appropriate resources to enable them to assist children to use the internet safely.

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

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 emails whilst supervising children.
- Staff send personal information by encrypted email and share information securely at all times.

Pre-school Social Networking and Websites

Social networking is the use of sites such as Facebook, Bebo, My Space, Twitter etc. St John's Playtime Pre-school has a Facebook page and a website and their content is closely monitored by our Administration staff and our Manager.

- The objective of our Facebook page is to provide parents with updated information about our setting.
- Any photos that are uploaded are with full parental consent.
- Any offensive remarks or comments will be removed and further action will be taken if necessary.

Personal Social Networking

- All staff should bear in mind that information they share through personal social networking applications, even though they are on private spaces, are still subject to copyright, data protection and freedom of information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation.
- 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 St John's Playtime Pre-school 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. **Refer to policy 1.8 Social Media and Professional Partnerships for further guidance.**

Electronic learning journals for recording children's progress

- St John's Playtime Pre-school uses the Tapestry electronic learning journals for recording children's progress in our setting.
- Families are informed of the use of Tapestry in the setting and provided with information regarding its privacy policy.
- Families are able to opt out of e-mail communications regarding Tapestry if they wish.
- 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 to ensure all children are safeguarded.

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).

Personal Mobile Phones – children

- Children do not bring mobile phones or other ICT devices with them to our 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 in the office until the parent collects them at their time of collection.

Personal Mobile Phones – staff, parents and visitors

- Personal mobile phones belonging to members of staff are not used whilst staff are working.
- At the beginning of each individual's shift, personal mobile phones are stored in the lockable office.

- In the event of an emergency, personal mobile phones may be used in the privacy of the office, with permission from our Manager.
- Members of staff ensure that the telephone number of the setting is known to immediate family and other people who need to contact them in an emergency.
- If members of staff take their own mobile phones on outings, for use in the case of an emergency, they must not make or receive personal calls or take photographs of the children.
- Parents and visitors are requested not to use their mobile phones whilst on the premises. There is 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 there are no children present.
- These rules also apply to the use of work-issued mobiles, and when visiting or supporting staff in other settings.

Cameras, Videos and other Electronic Devices

- Members of staff must not bring their own cameras or video recording equipment into the setting. This includes wearable devices such as 'smart' watches (which have camera settings accessible or are linked to personal phones) or personal smart phones. If it is necessary that a smart watch (which ***is*** connected to a personal phone) must be worn for medical safety reasons only, the reasons for this must be documented and recorded in writing. To clarify, members of staff are able to wear smart watches but they ***must not*** be linked to their personal phones (unless for the reasons stated above).
- Photographs and recordings of children are only taken of children if there is written permission to do so (found on the individual child's Registration Form).
- 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. We seek parental consent before any photographs are used on our website or on any social media sites.
- Photographs or recordings of children are only taken on equipment belonging to the setting.
- Camera and video use is monitored by our Manager.
- Where parents request permission to photograph or record their own children at special events, permission will first be 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.

Computers & Data Storage

- No information containing personal details or photographs of children and families at the setting will be stored on a home computer.

- If staff use their own computers for planning, observations etc. containing children's names they should transfer the data to a memory stick and erase it from their computer as soon as this is done.
- Memory sticks & external disk drive/back up are held in a secure place at home or at the setting.
- The settings cameras and computers are stored safely whilst the pre-school is closed.

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/

Other useful Pre-school Learning Alliance publications

Safeguarding Children (2025)

Employee Handbook (2025)

This policy was adopted at a meeting held by St John's Playtime Pre-school committee on 17th June 2009.

This policy was reviewed & updated on: June 2026

This policy will be reviewed again on: June 2027

Signed on behalf of the Management committee and provider:

Name of Signatory: Polly Fyfe

Role of Signatory: Committee Chairperson