



## **Online Safety Policy**

**Pre-school Manager: Nicky Benson-Dare**

**This policy will be reviewed annually. It will also be revised following any concerns and/or updates to national and local guidance and procedures.**

## Statement

St Peter's Busy Bees Pre-school has a commitment to keeping children safe and healthy. The Online Safety Policy is the implementation of the Safeguarding Policy in relation to electronic communications of all types. The internet is now regarded as an essential resource to support teaching and learning. Computer skills are vital to accessing life-long learning and employment. It is important for children to learn to be e-safe from an early age and we can play a vital part in starting this process. Unmediated internet access brings with it the possibility of placing children in embarrassing, inappropriate and even dangerous situations.

## Aim

In line with our safeguarding policies, our aim is to provide children with as safe an internet environment as possible, as well as starting to teach them to be aware of and respond responsibly to possible risks. We want to highlight and endorse best practice for managing the risks associated with online technologies.

## Procedures

- Staff support children to use technology for guided educational use. Staff will guide pupils in online activities that will support their learning and development. Internet use should be carefully planned and targeted within a regulated and managed environment. Pre-school internet access is tailored expressly for educational use and will include appropriate filtering.
- Risk assessment: We have a duty to ensure children in the pre-school are not exposed to inappropriate information or materials. We also need to ensure that children know how to ask for help if they come across material that makes them feel uncomfortable.
- Responsibility: Internet safety in the pre-school depends on staff, parents, carers and visitors taking responsibility for the use of internet and other communication technologies such as mobile phones. It is the pre-school's responsibility to use solutions to limit internet access and to monitor their effectiveness.
- The internet is also used in the pre-school to support the professional work of staff, to allow effective planning and to enhance the nursery's management information and business administration systems.
- Staff or children's home information will not be published.
- Website photographs that include children will be selected carefully and will not allow individual children to be clearly identified.
- Pupils' full names will not be used anywhere on the pre-school website, particularly in association with photographs. Written permission from parents or carers for featuring

their child on the website is requested when each child starts at the pre-school and parents/carers' wishes are followed at all times.

#### Communication

- Children will not have access to e-mail.
- Staff using e-mail will use a pre-school e-mail address. This address must not be used for personal e-mail.
- Staff will use personal e-mail outside of work hours, off the premises.

#### Use of Personal Devices and Mobile Phones

- St Peter's Busy Bees Pre-school recognises that personal communication through mobile technologies is an accepted part of everyday life for staff and parents/carers, but technologies need to be used safely and appropriately within the setting.
- All use of personal devices (including but not limited to tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as staff behaviour and safeguarding.
- Electronic devices of any kind that are brought onto our site are the responsibility of the user.
  - All members of St Peter's Busy Bees Pre-school community are advised to take steps to protect their mobile phones or devices from loss, theft or damage. We accept no responsibility for the loss, theft or damage of such items on our premises.
  - All members of St Peter's Busy Bees Pre-school community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices. Passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used outside of the kitchen area.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden; any breaches will be dealt with as part of our behaviour policy.
- All members of St Peter's Busy Bees Pre-school community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our staff behaviour or safeguarding policies.

## Staff use of personal devices and mobile phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures
- Staff will be advised to:
  - Keep mobile phones and personal devices in a safe and secure place - the phone box in the kitchen
  - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled.
  - Ensure that any content brought onto the site via mobile phones and personal devices is compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting parents/carers.
  - Any pre-existing relationships, which could undermine this, will be discussed with the DSL and manager.
- Staff will not use personal devices:
  - To take photos or videos in the setting and will only use work-provided equipment for this purpose.
  - Directly with the children and will only use work-provided equipment
- If a member of staff breaches our policy, action will be taken in line with our staff behaviour and allegations against staff policies.
  - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.
- Any member of staff using their own laptop must adhere to the Online Safety Policy in all matters relating to the pre-school.

## Visitors' use of personal devices and mobile phones

- Parents/carers and visitors (including volunteers) should ensure that they follow the expected procedures outlined in this policy
- We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of our expectations of their use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL or manager of any breaches our policy.

## Social Media

- The expectations regarding safe and responsible use of social media apply to all members of St Peter's Busy Bees Pre-school community.
- The term "social media" may include (but is not limited to) blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chat rooms and instant messenger.
- All members of St Peter's Busy Bees Pre-school community are expected to engage in social media in a positive, safe and responsible manner.
  - All members of St Peter's Busy Bees Pre-school community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The use of social media during setting hours for personal use is not permitted.
  - Inappropriate or excessive use of social media during setting hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the conduct of any member of St Peter's Busy Bees Pre-school community on social media, should be reported to the DSL and will be managed in accordance with our allegations against staff, staff behaviour and safeguarding policies.

## Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our Staff Behaviour Policy.
- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.
  - Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
  - Setting the privacy levels of their personal sites.
  - Being aware of location sharing services.
  - Opting out of public listings on social networking sites.
  - Logging out of accounts after use.
  - Keeping passwords safe and confidential.
  - Ensuring staff do not represent their personal views as those of the setting.
  
- Members of staff are encouraged not to identify themselves as employees of St Peter's Busy Bees Pre-school on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.
  
- All members of staff are encouraged to consider carefully the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with our policies and the wider professional and legal framework.
  
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues, will not be shared or discussed on social media sites.
  
- Members of staff will notify the designated safeguarding lead immediately if they consider that any content shared on social media sites conflicts with their role.

#### Communicating with parents/carers through social media

- All members of staff are advised not to communicate with or add as 'friends' any relatives of children attending the pre-school.
  
- Staff will not use personal social media accounts to contact parent/carers, nor should any contact be accepted, except in circumstances where prior approval has been given by the manager.
  
- Any communication from parents/carers received on personal social media accounts will be reported to the DSL (or deputy).

## Staff Misuse

- Any complaint about staff misuse will be referred to the manager in accordance with the complaints policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with our staff behaviour policy

## Management of Applications (apps) used to Record Children's Progress

- We use Tapestry to track learners' progress and share appropriate information with parents and carers.
- The Manager and DSL is ultimately responsible for the security of any data or images of children that we hold. They will ensure that the use of tracking systems is appropriately risk-assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard children's data:
  - Only staff-issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
  - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.
  - Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
  - All users are advised of safety measures, such as using strong passwords and logging out of systems.
  - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access, for example, not sharing passwords or images.

## Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- St Peter's Busy Bees Pre-school will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

- St Peter's Busy Bees Pre-school recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL.
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.

#### Online Radicalisation and Extremism

- We will take all reasonable precautions to ensure that children and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our safeguarding policy.
- If we are concerned that member of staff may be at risk of radicalisation online, the manager will be informed immediately, and action will be taken in line with the safeguarding and allegations against staff policies.

#### Staff Responsibilities

It is the responsibility of all staff to:

- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the setting's safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.



- Welcome professional development within this area.

#### Parents/carers and online safety

- Parents/carers' attention will be drawn to the pre-school's Online Safety Policy

#### Useful Contacts and Links for Settings

- **Education Safeguarding Service**
  - **Area Safeguarding Advisor - Maidstone** - 03301 651 440
  - **Online Safety in the Education Safeguarding Service**
    - 03301 651 500
    - [onlinesafety@theeducationpeople.org](mailto:onlinesafety@theeducationpeople.org) (**non-urgent issues only**)
- **LADO Service**
  - **Telephone: 03000 410 888**
  - Email: [kentchildrenslado@kent.gov.uk](mailto:kentchildrenslado@kent.gov.uk)
- **Integrated Children's Services/ Children's Social Work Services**
  - Front Door: 03000 411 111
  - Out of Hours Number: 03000 419 191
- **Early Help**
  - [Maidstone](http://Maidstone) - 03000 42 23 40 - [MaidstoneEarlyHelp@kent.gov.uk](mailto:MaidstoneEarlyHelp@kent.gov.uk)
- **Kent Police**
  - 101 or 999 if there is an immediate risk of harm
- **Kent Safeguarding Children Multi-Agency Partnership (KSCMP)**
  - [kscmp@kent.gov.uk](mailto:kscmp@kent.gov.uk)
  - [www.kscmp.org.uk](http://www.kscmp.org.uk)
  - 03000 421 126
- **Adult Safeguarding**
  - Adult Social Care via 03000 41 61 61 (text relay 18001 03000 41 61 61) or email [social.services@kent.gov.uk](mailto:social.services@kent.gov.uk)
  - [www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding](http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding)
  - [www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials](http://www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials)
  - [www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links](http://www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links)
  - [www.theeducationpeople.org/blog/?tags=Online+Safety&page=1](http://www.theeducationpeople.org/blog/?tags=Online+Safety&page=1)

#### KSCB:

- [www.kscb.org.uk](http://www.kscb.org.uk)

Kent Police:

- [www.kent.police.uk](http://www.kent.police.uk) or [www.kent.police.uk/internetsafety](http://www.kent.police.uk/internetsafety)

In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

Other:

- Kent Public Service Network (KPSN): [www.kpsn.net](http://www.kpsn.net)
- EiS - ICT Support for Schools and Kent Schools Broadband Service Desk: [www.eiskent.co.uk](http://www.eiskent.co.uk)

National Links and Resources for Educational Settings

- CEOP:
  - [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)
  - [www.ceop.police.uk](http://www.ceop.police.uk)
- Childnet: [www.childnet.com](http://www.childnet.com)
- Internet Matters: [www.internetmatters.org](http://www.internetmatters.org)
- Internet Watch Foundation (IWF): [www.iwf.org.uk](http://www.iwf.org.uk)
- Lucy Faithfull Foundation: [www.lucyfaithfull.org](http://www.lucyfaithfull.org)
- NSPCC: [www.nspcc.org.uk/onlinesafety](http://www.nspcc.org.uk/onlinesafety)
  - ChildLine: [www.childline.org.uk](http://www.childline.org.uk)
  - Net Aware: [www.net-aware.org.uk](http://www.net-aware.org.uk)
- The Marie Collins Foundation: [www.mariecollinsfoundation.org.uk](http://www.mariecollinsfoundation.org.uk)
- UK Safer Internet Centre: [www.saferinternet.org.uk](http://www.saferinternet.org.uk)
  - Professional Online Safety Helpline: [www.saferinternet.org.uk/about/helpline](http://www.saferinternet.org.uk/about/helpline)
- 360 Safe Self-Review tool for schools: [www.360safe.org.uk](http://www.360safe.org.uk)

National Links and Resources for Parents/Carers

- Action Fraud: [www.actionfraud.police.uk](http://www.actionfraud.police.uk)
- CEOP:
  - [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)
  - [www.ceop.police.uk](http://www.ceop.police.uk)
- Childnet: [www.childnet.com](http://www.childnet.com)
- Get Safe Online: [www.getsafeonline.org](http://www.getsafeonline.org)
- Internet Matters: [www.internetmatters.org](http://www.internetmatters.org)
- Internet Watch Foundation (IWF): [www.iwf.org.uk](http://www.iwf.org.uk)
- Lucy Faithfull Foundation: [www.lucyfaithfull.org](http://www.lucyfaithfull.org)
- NSPCC: [www.nspcc.org.uk/onlinesafety](http://www.nspcc.org.uk/onlinesafety)
  - ChildLine: [www.childline.org.uk](http://www.childline.org.uk)
  - Net Aware: [www.net-aware.org.uk](http://www.net-aware.org.uk)
- The Marie Collins Foundation: [www.mariecollinsfoundation.org.uk](http://www.mariecollinsfoundation.org.uk)
- UK Safer Internet Centre: [www.saferinternet.org.uk](http://www.saferinternet.org.uk)