Online Safety Policy

This policy applies to everyone - staff, children, parents/carers, visitors, and contractors accessing the internet or using technological devices on the premises. The policy is also applicable where staff or individuals have been provided with setting issued devices for use off-site.

We recognise the exciting opportunities technology offers to staff and children in our setting and have invested in age-appropriate resources to support this belief. While recognising the benefits we are also mindful that practitioners have a duty of care to ensure that children are protected from potential harmful online material and that appropriate filtering and monitoring systems are in place.

To reflect our belief that when used appropriately and safely, technology can support learning, we encourage adults and children to use a range of technological resources for a wide range of purposes. At the same time, we do all we can to ensure that technology is used appropriately and that children are safeguarded against all risks. While it is not possible to completely eliminate risk, any online safety concerns that do arise will be dealt with quickly to ensure that children and staff adhere to safe practices and continue to be protected. We will communicate our safe practice in the use of technologies with families and manage any concerns.

Our setting will refer to the 'Safeguarding children and protecting professionals in early years settings: online safety considerations' guidance as referenced in the Statutory Framework for the Early Years Foundation stage,2024, 3.6

We aim to:

- Raise awareness amongst staff and parents/carers of the potential risks associated with online technologies, whilst also highlighting the many learning and social benefits.
- Maintain a safe and secure online environment for all children in our care.
- Provide safeguarding protocols and rules for acceptable use to guide all users in their use of technology and online experiences
- Ensure all adults are clear about sanctions for misuse of any technologies both within and beyond the setting.

2. Hardware and provision use

Where staff have been issued with a device (e.g., setting laptop or tablet) for work purposes, personal use whilst off site is not permitted unless authorised by the provider/manager. The settings laptop/devices should be used by the authorised person only. Only technology owned by the setting will be used on the premises and on visits or outings. This includes mobile devices for everyday use, and, in case of emergency. Staff taking photographs or recording with technology not owned by our setting is specifically not allowed.

All staff have a shared responsibility to ensure that children are supervised when using the internet and related technologies to ensure appropriate and safe use as part of the wider duty of care and responding or reporting promptly issues of concern.

Setting issued devices only should be used for work purposes and, if containing sensitive information or photographs of children, should not leave the premises unless encrypted.

Online searching and installing/downloading of new programs and applications is restricted to authorised staff members only. Children should not be able to search or install anything on a setting device.

Setting issued devices should not leave the premises unless encrypted and this must be acknowledged in the policy. In the case of an outing, all data must be transferred/deleted from the setting's camera/device before leaving the setting.

3. Data Storage and Management

No electronic documents that include children's names or digital images will be transported out of the setting e.g., on Fobs, memory sticks.

Setting issued devices should not leave the premises unless encrypted. In the case of an outing, all data must be transferred/deleted from the setting's camera/device before leaving the setting.
Cybercriminals can damage a business, cause a temporary shutdown, expose confidential information, and access finances. The reputational damage could be huge and could lead to an investigation by the Information Commissioner's Office, resulting in hefty fines. Strong passwords that are reviewed regularly will be used to control access. The setting will ensure that all devices have protective software from viruses and malware and keep those up to date.

4. Email

The setting has access to a professional email account to use for all work-related business, including communication with parents/carers. This allows for email content to be monitored and protects staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.

Staff must not engage in any personal communications (i.e., via Hotmail or Yahoo accounts etc.) with children who they have a professional responsibility for. This also prohibits contact with children who previously attended the setting.

Staff should not participate in any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person or persons.

All emails should stay professional in tone and be checked carefully before sending, just as an official letter would be. Care should be taken when forwarding emails from others.

5. Social Networking

Employees must not access personal blogs/social networking sites on work premises or use the setting's internet systems or email address for their own use, without prior agreement or in accordance with the setting's policy.

The setting does not condone employees writing about their work on social networking sites or web pages. If employees choose to do so, they are expected to follow the following rules:

Staff must not:

- disclose any information that is confidential to the setting or any third party or disclose personal data or information about any individual child, colleague, or service user, which could be in breach of the UK General Data Protection Regulation (UKGDPR) and Data Protection Act 2018.
- disclose the name of the setting or allow it to be identified by any details at all. This includes posting photos of children and young people, the premises, or events with work colleagues.
- link their own blogs/personal web pages to the setting's website.
- make defamatory remarks about the setting, colleagues, or service users.
- misrepresent the setting by posting false or inaccurate statements.

Remember that anything posted online could end up in the public domain to be read by children, parents, or even future employers – so be careful what you post and who you post it to. For example, posting explicit pictures of yourself could damage your reputation and that of your profession and organisation. Parents and employers may also question your suitability to care for children.

Staff should not: send social networking site 'friend requests' to, or accept them from, children, young people or parents who use the setting. All communication with children and young people should always take place within clear and explicit professional boundaries. Staff should avoid any misinterpretation of their motives or any behaviour that could be construed as grooming. Failure to adhere to the rules and guidelines in this policy may be considered misconduct and could lead to disciplinary and/or criminal investigations.

Setting social media sites

Setting social networking sites containing information about children attending the setting must be "closed" i.e. the users of the site are accepted and monitored by the manager/administrator. No staff, families or children's personal information will be accessible by users of the site and the manager/administrator will ensure that users' profiles are kept private. The manager/administrator will moderate all postings to the site; they will review, and quality assure these before they appear, for example, to ensure they do not reveal personal information.

Safety Guidelines if using devices with children within the setting

Children will always be supervised when using devices and this will be used as a learning opportunity. All websites, apps and search results will be checked prior to children having access to them and safety and privacy settings are always kept at the highest level.
Staff will model the safe use of devices and online learning including activities away from devices that may support children's understanding of the risks online (further information on these activities can be found via Uk Safer Internet Centre)

Children will not use staff personal devices at any time. Any devices brought in from home will be securely stored for the duration of the child's attendance unless prior consent has been given by management. Any medical devices needed for the child's personal use will be risk assessed and managed with safety as a priority.

6. Sanctions

Misuse of technology or the internet may result in:

- the logging of an incident
- disciplinary action
- reporting of any illegal or incongruous activities to the appropriate authorities
- the allegations of harm process being followed using the relevant flowchart

7. Other relevant policies and guidance

- Model policy on the use of mobile phones and technological devices
- Guidance for settings on the use of images and technological devices
- Safeguarding Children and Protecting Professionals in Early Years Settings: Online Safety Considerations for Managers (UK Council for Internet Safety, 2019)
- Safeguarding Children and Protecting Professionals in Early Years Settings: Online Safety Guidance for Practitioners (UK Council for Internet Safety, Feb 2019)