**Online Safety Policy and Procedure**

**Statement of Intent**

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 e-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.

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.

**Aim**

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 early years setting.

**Procedure**

*Hardware and provision use*

Where staff have been issued with a device (e.g. setting laptop or iPad) for work purposes, personal use whilst off site is not permitted unless authorised by the supervisor/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 setting visit or outings. This includes mobile devices for everyday use and, in case of emergency, a mobile phone is provided.

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.

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.

All photographs from the setting’s camera are downloaded the same day and put onto the settings laptop for use within the setting only. The laptop does not leave the building and is stored in a locked office overnight.

*Data Storage and Management*

No electronic documents that include children’s names or digital images will be transported out of the setting.

In the case of an outing, all data must be transferred/deleted from the setting’s camera/device before leaving the setting.

*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 via email with parent/carers of children who they have a professional responsibility for.

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 checked carefully before sending. Care should be taken when forwarding emails from others.

*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 rules below:

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 General Data Protection Regulation (GDPR) 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.

Communication with children and young people, by whatever method, 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.

Staff should not send social networking site ‘friend requests’ to, or accept them from, children, young people or parents/carers who use the setting. Failure to adhere to the rules and guidelines in this policy may be considered misconduct and could lead to disciplinary and /or criminal investigations. Remember that anything posted online could end up in the public domain to be read by children, parents/carers and others.

Staff must not engage in any personal communications via text message or any social media account with parent/carers of children who they have a professional responsibility for.

*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 office manager. No staff, families or children’s personal information will be accessible by users of the site and the office manager will ensure that user’s profiles are kept private. The office manager will moderate all postings to the site; they will view and quality assure these before they appear, for example, to ensure they do not reveal personal information.

*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

• allegations process being followed

Updated and implemented Autumn Term 2023 – reviewed regularly and the procedure monitored and evaluated