**E-Safety Policy**

Written by: Alice Mcpherson Date: 16.07.2021

The use of technology is growing, and children are exposed to technology from an incredibly young age. I recognise the benefit of using electronic devices to support children’s learning in my provision and to help me comply with the record keeping and learning and development aspects of the Early Years Foundation Stage (EYFS, 2017).

E-safety covers all electronic devices including cameras, computers, videos and DVD recorders, mobile phones, and other devices capable of taking photographs or linking to the internet. It also includes the use of social media, software, emails, chat rooms, blogs, laptops, games consoles and new technology as I am aware that internet and technology is constantly evolving.

For more information about how I use mobile phones and cameras, please see my **Safeguarding and Child Protection Policy and Procedures**.

**How the internet is used**

The internet is used in different ways in the setting:

* The Early Years Foundation Stage (EYFS, 2017) requires providers to teach children about technology which is generally accepted to include learning about the internet. I aim to take a common-sense approach to how long children spend using ICT during the day and the suitability of ICT resources for various ages of children. Parents are consulted about time spent on the internet and, for example, watching television and their wishes are followed. Parents, please do not allow your child to bring electronic games rated over the age of the child.
* Staff use the internet to *input learning and development information about children; share learning and development information with children’s parents; store personal data bout children and their families*
* Management use the internet to *complete payroll; send messages including email to parents and children; share information with families and staff.*

**The risks of using the internet**

I am aware of the risks of allowing staff and children to go online on computers, tablets, mobile phones, watches, gaming etc and:

* I aim to supervise use to protect children and staff when using the internet.
* I share safe internet messages with parents so they can support their children’s internet use and keep them safer at home.
* I teach children about how to use the internet safely and monitor their use.
* I train staff to keep online information secure and to raise awareness of the risks of radicalisation and extremism on the internet and online bullying.
* Staff including volunteers and students are only given access to children’s online data when training has been provided and a **Data Sharing Agreement** signed.
* Staff and children are made aware of the risks of being online and know how to report any concerns.

**Keeping data safe**

I understand that while technology is useful for learning it can also present safety problems when misused and this policy has been written to clarify appropriate technology use within the provision and by parents of children who attend my provision when related to childminding and childminded children and –

* The broadband is secured by a password which is changed regularly.
* Virus protection software is automatically updated.
* *Online learning journey systems are secured with a password which is changed regularly.*
* Passwords are used for all online systems – passwords are changed regularly, and the password is stored in a password protected document on the main computer and shared via Dropbox;
Note – Dropbox is cloud storage owned by a US company and not covered by GDPR.
* Laptops, tablets, and other ICT equipment which contain sensitive data about children, families and staff are secure and do not leave the premises.
* Tablets and laptops ‘time out’ to a password protected page when unused.
* Memory sticks, when used, are encrypted, and locked away.
* The password to any secure documents is shared with my partner to ensure it remains secure should I be injured or fall ill.

**Online communications**

All internet enabled devices are monitored to ensure safe internet use. Any technology used by children has internet safety controls in place so children cannot access inappropriate sites. Every effort will be made to keep internet security updated and online usage by children will be monitored.Any uploading of personal information onto websites must be carried out in compliance with the Data Protection Act 1998 and will not be done without prior written permission from the parent involved.

* The *website, Facebook group - blog* … *does / does not* contain photos of children and staff.
Note – if photos of children or staff are used online consent (parent or staff member permission) must be sought in writing in advance and can be withdrawn at any time.
* When emails are sent to parents, BCC is used to protect private email addresses.
* Use of work-related ICT equipment will be monitored and work-related equipment must not be used for private or social networking purposes.
* Staff are trained to recognise the importance of ensuring all communications between staff, parents and children are professional respectful. If concerning comments are made by other staff members or parents etc on social media, staff will not respond they will report the comment to the *Designated Safeguarding Lead / Manager* on the next working day.
* Staff are trained to understand that information about children and families will not be shared online, including on social media – this is a disciplinary offence.

I am registered with the Information Commissioner’s Office - ICO - [www.ico.gov.uk](http://www.ico.gov.uk): please see my ICO registration certificate.

If there is a concern about e-safety, I will act on the concern to comply with the requirements of the EYFS, Childcare Registers, Ofsted and the ICO.

If you have any questions about my Policy / Procedures or would like to make any comments, please ask.

Signed: Review date:

