

**Safeguarding**

**Policy statement**

The internet is a tool for children in our setting to investigate and learn more about the world. We have a duty to ensure that children are protected from potential harm when accessing the internet at pre-school. Every effort will be made to safeguard against all risks and children will never be allowed to access the internet without a member of staff, however it is likely that we will never be able to completely eliminate all risks. Any incidents that do arise will be dealt with quickly and according to policy to ensure that children and staff continue to be protected. The purpose of this policy is to be clear about how we use ICT and the measures we take to be E-Safe.

**Who is this policy for?**

This policy is for all staff, children, parents/carers, directors, visitors and contractors accessing the internet or using technological devices on the premises. This includes the use of personal devices by all of the above mentioned groups, such as mobile phones or iPads/tablets which are brought into our setting. This policy is also applicable where staff or individuals have been provided with devices for use off-site.

**E-Safety Lead Responsibilities**

The E-safety lead is a member of staff who takes overall responsibility for E-safety.

The E-Safety lead:

* Recognises the importance of E-Safety and understand the setting’s duty of care for the safety of children and staff.
* Has established and maintains a safe ICT learning environment.
* Ensures that all staff when accessing technology with children understand the need to supervise and provide safe internet access. This would normally entail a staff member checking the content before sharing with children.
* Ensures that filters and settings are set appropriately on all pre-school iPads and PC’s to a level that is safe for children to view i.e. no explicit language
* Reports issues immediately to the manager.
* Cascades/delivers staff training according to new and emerging technologies so that the correct E-Safety information is being shared.
* Keeps an E-Safety Incident Log to record any incidents and how they were dealt with.
* From time to time makes unannounced checks on staff when they are using IT equipment, to ensure it is being used appropriately.
* Offers guidance and resources to staff to ensure that they can provide a safe and secure online environment for all children in their care.
* Raises awareness amongst staff and parents of the potential risks associated with online technologies, whilst also highlighting the many educational and social benefits.
* Provides rules for staff on acceptable use (as detailed in our Acceptable Use Policy) to guide all users in their online experiences.
* Ensures that staff are clear about procedures for misuse of any technologies both within and beyond the early years setting.

**Management Responsibilities**

The Manager has overall responsibility for E-Safety as part of the wider remit of safeguarding and child protection. To meet these responsibilities the manager has designated an E-Safety Lead to implement policies, procedures, staff training and take the lead responsibility for ensuring E-Safety is addressed appropriately. All staff members, students, volunteers and visitors should be aware of who holds this post within the setting.

The manager:

* Provides a safe, secure and appropriately filtered internet connection for staff and children within the setting.
* Provide resources and time for the E-Safety lead and staff team to be trained and updated as appropriate.
* Ensures that any equipment which holds sensitive or confidential information and leaves the premises (e.g. iPads, back up device) are password protected.
* Ensures that E-safety is a standard agenda item on all staff and directors meeting agendas.
* Ensures that E-safety is embedded within all child protection training, guidance and practices.
* Elects an E-Safety Director to challenge the setting about E-Safety issues (this will always be the chair).
* Ensures that all staff, volunteers, students and directors have read, understood and signed to say that they will adhere to the Acceptable Use Policy as part of their induction.

**Staff (including volunteers) Responsibilities**

* All staff have a shared responsibility to ensure that children are able to use IT equipment safely, under constant supervision.
* Read and abide to our Acceptable Use Policy for Early Years Employees.

**Mobile Phones**

* Staff cannot carry or use their personal mobile phones whilst working in the setting. The phone must be on silent whilst in the setting.
* Setting telephone number should be given out to be used as an emergency contact for staff (01435 872523).
* Staff may not use any camera facility on their mobile during a session.
* Access to work email is prohibited on personal mobile phone.
* Reference should be taken of the Pre-School’s Safeguarding Policy.

**Broadband and Age Appropriate Filtering**

Broadband provision is essential to the running of an early years setting, not only for communication with parents and carers but also providing access to a wealth of resources and support. We use internet enabled devices - iPads, whiteboard and a PC to enhance the learning experience of children and to maintain our online observation and assessment tool called Tapestry. Great care is taken to ensure that safe and secure internet access, appropriate for both adults and children accessed.

* Parental controls are established on all internet enabled devices that children have access to, blocking or preventing access to any harmful, illegal or inappropriate content.
* The three iPads and office PC, are password protected and are only used by the children under adult supervision.
* The children’s ipad’s have no email access and will be used with an adult.
* For the purpose of running our setting we have an office email: [office@mayfieldpreschool.co.uk](mailto:office@mayfieldpreschool.co.uk) Emails from this address are sent and received on the office PC and our staff ipad, which are normally used by the manager, deputy, and admin manager. Our manager receives emails remotely when the preschool is closed – again, the system is password protected, and no passwords are saved to devices.
* When group emails to parents are sent the BCC option is selected so that emails are not shared and made public.
* All emails should be professional in tone and checked carefully before sending, just as an official letter would be.
* We do not use e-mail to provide information regarding specific children. However parents are welcome to contact us via e-mail in regard to absences, sessions etc.
* In conjunction with local Health Visitors, we use encrypted emailing when discussing children’s IPR.