

**ONLINE SAFETY AND ACCEPTABLE USE POLICY**

Cheryl Knight: SDL - Manager

Leander Trunks: SDP - Deputy Manager

Jo Walton: SDP - Deputy Manager

Date of last review: 19/12/2023 Next Review Date: Dec 2024

This policy will be reviewed every 12 months, but we will regularly monitor and evaluate our online safety and mobile phone approach, reflecting on any concerns and updating our policy and practice as required.

Links with other policies: Child Protection and Safeguarding Children –– mobile phone, recordable device & wearable technology policy, Staff Code of Practice, whistleblowing policy

**Rationale:**

At the Mulberry Bush keeping children safe is our priority and online safety is a crucial part of that. We recognise that technology is part of the ever changing, digital world we live and work in and is an important aspect of the children’s learning. Technology forms part of the Statutory Framework for the Early Years Foundation stage*:* There is an expectation that children can access technology and use it safely. Computer skills are key to accessing learning. However, we are very aware of the possible dangers of the misuse of technology and the importance to help children to learn to use technology safely and appropriately. We aim to encourage responsible and appropriate use of technology within the setting and by sharing information and ideas with parents and carers. This policy aims to give guidance to staff, parents and children at the setting, to ensure children’s safety and privacy is protected and online safety is preserved.

**Aims of this policy:**

To help our children to begin to learn how to use technology safely, to stay safe online and enable them at a level appropriate for their age and ability and to share any online concerns. We engage with parents/carers about how technology is used within the family home, and offer online safety advice (and sign posting) to support them in keeping their children safe when using technology at home and help them talk about online safety with their children in an age appropriate way.

* Promote safe and responsible use of technology devices
* Set clear guidelines on acceptable use of devises
* Support policies relating to Child Protection and the Safeguarding of children
* Address challenges posed such as: Risks to children, Data Protection and Privacy breeches.

**Policy statement**

**Who is responsible:** On-line safety is recognised as vital part of our settings safeguarding responsibility. The nursery Designated Safeguarding Lead Practitioner(s) and staff have accessed training to ensure they have a clear understanding of the unique risks associated with online safety for children of all ages and are competent in ensuring they understand their responsibility with required to keeping children safe. The nursery DSL takes responsibility for the appropriate use of technology within the setting including the use of mobile phones and wearable technology devices and ensuring all staff are familiar with and comply with the nursery policies and procedures surrounding Child Protection and online safety. and will take appropriate action by addressing any concerns raised. (*Also See Child Protection and Mobile phone, camera and wearable technology devices and acceptable use policy*)

The setting DSL ensures staff undertake online safety training and that it forms part of our robust induction process. All staff are aware of the risks to children online and understand that any child is vulnerable and that their vulnerability can vary depending on their age, development stage and personal circumstances. *UKCIS framework (Education for a Connected World provides information about skills young children need regarding online safety from the age of 4yrs).*

Staff model safe practice when using technology with the children and are fully aware of their personal responsibility with regards to online safety and know how to follow the procedures for reporting any concerns to the setting DSL immediately which will be recorded and actioned. The setting DSL will make decisions about how and when to escalate a concern. If the setting DSL has concerns about a child’s safety or welfare, they will notify the appropriate safeguarding agency with statutory responsibility without delay. All staff understand they may escalate their concerns via a direct referral to the local safeguarding hub if they feel their concerns have not been recognised or actioned appropriately in line with our Child protection policy.

**Staff:**

* Staff have a responsibility to maintain the good name of the setting and to promote online safety for the children and their families. Staff are aware of their personal responsibility with regards to using social media, both professionally and in their personal lives. They must manage their digital reputation, including appropriateness of information and content that they post online, both professionally and personally. Staff should discuss their online expectations and permissions with family and friends for example; what photographs of them can and cannot be shared on social media.
* Staff are aware that no matter what privacy settings are used, anything posted online can become public and permanent and could be misinterpreted and or used without their knowledge or consent.
* Staff must not accept friend requests or communications from parents (past or present). If there is an existing relationship this must be discussed with the setting DSL practitioner who will decide how this will be managed and will provide staff with clear guidance and boundaries and record any action taken.
* Staff are aware that civil, legal or disciplinary action can be taken against staff if they are found to have bought the setting or the profession into disrepute.
* Staff are aware that under no circumstances should they, either at work or in any other place, make, deliberately download, possess or distribute material they know to be illegal.
* Staff are aware if they or another member of staff are targeted online (bullying or harassment) they should inform the setting DSL.
* All staff, students and volunteers are personally responsible for reading, understanding and enforcing this policy.
* The nursery DSL is responsible for overseeing staff are familiar with and able to comply competently with the settings safeguarding and Child protection policies and will monitor and review this policy to ensure the procedures are carried out effectively and amend or update as necessary.
* Staff are aware of their personal responsibility with regards to upholding the staff code of practice and whistle blowing policy.

**How technology is used within our setting:**

The nursery provides tablets (ipads 3) for staff to use in the setting. These are connected to the internet via wi-fi and are screen locked with a pin code. Staff use these tablets to photograph and record the children’s progress and attainment. This is downloaded to a secure platform digital learning journey (Tapestry). Only parents can access their child’s learning journey with a secure link which is password protected This is overseen and monitored by the second DSP Leander Trunks). The staff tablets are not used by the children in the setting or for personal use. They are stored securely in a locked metal cupboard when not in use in line with Data Protection requirements. Only employed staff know the pin code and can access the tablets (ipads). The content is monitored regularly, including checking results of searches by the DSL.

*UK Safer Internet Centre (https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring)*

**Nursery lap tops**: The settings lap tops (2) which are located in the nursery office. They are connected to the internet / wi-fi and are used to record children’s reports, personal records, professional reports and one planning information. Sensitive Information is password protected and information is deleted as appropriate when the child leaves the setting. Lap tops have screen locks / pin code or password protected and are stored securely in a locked metal cupboard when not in use. The content is monitored regularly, including checking results of searches by the DSL.

**Transferring personal, sensitive information**: Sensitive information with the child’s personal details such as reports, assessments and records, including their digital learning journeys will be managed, stored and shared safely and securely online. It will be transferred securely via the internet/wi-fi, either through a requested secure link/portal or by password protecting the document in accordance with Data Protection Regulations (GDPR) and Data protection legislation.

**Children’s tablets:** The children have the use of Amazon Fire Kindle tablets. These are programmed with age-appropriate programmes and activities. They are password protected, have filters and the children cannot access the internet without an adult. Children are always within close proximity of a responsible adult when using the tablets and will be closely supervised when using the tablets with internet / wi-fi access and only age appropriate apps, websites and online tools will be used with the children.

**Parents Facebook page:** Parents can access the nursery fb page through invitation only. We share information about what’s going on, updates and initiatives and activities, ideas and resources to support the home learning environment. We will not share personal information, show photographs or personal details that identify any child or family in our setting. **Open fb page:** We also have an open fb page which advertises our setting and is open to the public domain. We will not share personal information, photographs or personal details that identify any child or family in our setting.

**The setting website:** The setting has a website where parents, prospective parents/carers, staff or student applicants and any interested parties can access freely. We will not share personal information, photographs or personal details that identify any child or family in our setting.

**Procedures: How this policy fits into our role on a day to day basis:**

* Work in partnership with parents and carers to educate young children on how to use technology safely and how to stay safe on-line:
* The children are taught these stay safe principles in an age-appropriate way;
* only go online with a grown up
* be kind online
* keep information about me safe
* only press buttons on the internet to things I understand
* tell a grown up if something makes me unhappy on the internet
* We will also seek to build children’s resilience in relation to issues they may face in the online world, and will address issues such as staying safe, having appropriate friendships, asking for help if unsure, not keeping secrets as part of social and emotional development in age-appropriate ways.
* If a used computer is purchased or donated to the setting, the designated person will ensure that it is cleared and no inappropriate material is stored on it before children use it. All old devices will be cleared of any information before safe disposal.
* Staff report any suspicious or offensive material that may cause harm, distress or concern, including material which may incite; racism, bullying, harassment, grooming, abuse or discrimination to the nursery DSL who will contact the appropriate local safeguarding agency and / or the Police and to the Internet Watch Foundation at [*www.iwf.org.uk*](http://www.iwf.org.uk/)*.*
* Suspicions that an adult is attempting to make inappropriate contact with a child on-line will be reported to the National Crime Agency’s Child Exploitation and Online Protection Centre at [www.ceop.police.uk](http://www.ceop.police.uk/)**.**

**Staff must:**

* Appropriately supervise children whenever they are using devices
* Check apps, websites and tools prior to using them with children, this should include checking the results of searches
* Use age-appropriate apps, websites and online tools with children
* Model safe practice when using technology with children
* Ensure data is shared online in accordance with data protection (GDPR) requirements

**The Manager/SDLP’s Will:**

* Access training/information to ensure they understand the unique risks associated with online safety for early years children and have the relevant knowledge and up to date capability required to keep children safe online
* Provide staff with quality and up-to-date ‘online safety’ training at induction and it will form part of the setting full team annual SG in-house training.
* Ensure staff and parents are aware of the UKCIS framework (Education for a Connected World) which provides information about the skills and competences that children and young people need to have with regards to online safety from the age of 4 upwards. (*The two Johns*)
* Know how to report a problem and when to escalate a concern.

**Staff are:**

* Aware that under no circumstances should any member of staff, either at work or in any other place, make, deliberately download, possess, or distribute material they know to be illegal, for example child sexual abuse material.
* Aware of the need to manage their digital reputation, including the appropriateness of information and content that they post online, both professionally and personally.
* Staff understand they should discuss online expectations and behaviour with their friends and colleagues - for example, have they discussed what photos of them can and cannot be shared by their friends on social media.
* Are aware that no matter what privacy settings are used, anything posted online can become public and permanent and could be misinterpreted and/or used without their knowledge or consent.

**Managers will ensure that all children:**

* Receive age appropriate online safety education throughout the curriculum.
* Use age-appropriate apps, tools and resources.

**Email**

* Children are not permitted to use email in the setting. Parents and staff are not normally permitted to use setting equipment to access personal emails other than in regards to training.
* Staff do not access personal or work emails whilst supervising children.
* Staff send personal, sensitive information about a child password protected or through a secure link or portal.
* Staff share information securely or anonymise information when communicating with other staff.

**Mobile phones – children** *(also see Mobile Phone and wearable device acceptable use policy***)**

* Children must not bring mobile phones or other ICT devices such as smart watches, cameras to the setting. If a child is found to have a mobile phone, wearable technological device, it will be removed and stored securely in a locked cupboard/drawer in the office until the parent collects them at the end of the session and they will be asked to ensure they do not bring it to nursery in future. The setting will not be responsible for the loss or damage to personal mobile phones or wearable devices.

**Cameras, videos and smart watches (all wearable technology)**

* Our staff and volunteers are aware they must not bring personal cameras or video recording equipment into the setting (children’s areas). This includes; mobile phones, tablets, wearable devices, cameras, recorders etc.)
* Photographs and recordings of children are only taken for valid reasons with parent/carer consent i.e. to record their learning and development, outings, for parents, or for displays within the setting.
* Photographs used for marketing purposes require specific written permission/consent from parents. Photographs will be digitally uploaded and/or printed and stored securely or destroyed after use or a reputable printing company will be used if they need to be outsourced. If photographs of children are used for publicity purposes, specific parental consent must be given and safeguarding risks minimised, for example, ensuring the children cannot be identified by name, address or their DOB.
* Parents are informed that they must not photograph / record the children at the nursery during events such as Nativity, race days, graduation and parties without specific consent of the manager/DSL and will be closely supervised at all times (all parties must give specific consent to the photograph/recording prior to it being taken).
* All photographs and video content shared with parents/cares remain the property of The Mulberry Bush Montessori Nursery and **must not** be shared, posted or downloaded online.

**Social media**

* Staff observe confidentiality and refrain from discussing any issues relating to their work or the children and their families.
* Staff should report any concerns or breaches of nursery policy on social media or online safety to the DSL.

**Infrastructure and Technology: Some forms of online abuse**

* **Prevent:** We must ensure children at our setting are safe from the potential harm of extremist material and terrorism when accessing the internet within the setting by establishing appropriate levels of filters, monitoring and adult supervision. (*Prevent Duty).*
* **Online abuse:** The internet can be a great place for children to play, learn and connect, but it can also put them at risk of online abuse. Online abuse is any type of abuse that happens on the internet. It can happen across any device that’s connected to the web, like computers, tablets and mobile phones. Children can be at risk of online abuse from people they know and from strangers. It might be part of other abuse taking place offline like bullying, grooming or sexual abuse. It can happen via: social media, texts and messaging apps, emails, online chats, online gaming, live streaming
* **Child Exploitation:** A type of sexual abuse when they are exploited, they are given things, like gifts, drugs, money in exchange for the sexual activities.
* **Grooming:** Building a relationship**,** trust and emotional connection with the child so they can manipulate, exploit and abuse them.
* **Sexual Abuse:** Can happen in person or online. When a child is forced or tricked into sexual activity and they may not be aware it is wrong or be too afraid to tell.
* **Bullying:** Bullying is behaviour that hurts someone else, physically or emotionally. Can include name calling, hitting, pushing, spreading rumours, threatening or undermining someone.
* **Cyber Bullying:** Cyber bullying takes place online. Unlike bullying offline it can follow the child wherever they go, via social networks, gaming and mobile phones.
* **Criminal exploitation and gangs** (County lines): Child abuse where children are manipulated into committing crimes, often drugs related.

**Further information, support and advice on online safety can be found at:**

* *EYFS DFE 2024, Working Together 2023*
* *Prevent Duty 2015 updated 2023*
* *Keeping Children safe in education 2023*
* *Online safety guidance for practitioners*
* *Whistleblowing-helpline:(*[*https://www.nspcc.org.uk/what-you-can-do/report-abuse/dedicated-helplines/whistleblowing-advice-line/*](https://www.nspcc.org.uk/what-you-can-do/report-abuse/dedicated-helplines/whistleblowing-advice-line/)*)*
* *Internet Watch Foundation (*[*https://www.iwf.org.uk/*](https://www.iwf.org.uk/)*)*
* *Child Exploitation and Online Protection centre (https://wwwceop.police.uk/ceop-reporting)*
* *UK Safer Internet centre helpline for professionals (*[*https://saferinternet.org.uk/professionals-online-safety-helpline*](https://saferinternet.org.uk/professionals-online-safety-helpline)*)*
* *NSPCC (*[*https://www.nspcc.org.uk/what-we-do/about-us/partners/nspcc-o2-online-safety-partnership/*](https://www.nspcc.org.uk/what-we-do/about-us/partners/nspcc-o2-online-safety-partnership/)*)*