E SAFETY POLICY

play-to-learn

MONTESSORI NURSERIES AND PRE-SCHOOLS

Statement of Intent

This policy has been written to protect and safeguard the children in our care, in line with the safeguarding and welfare requirements of the Early years foundation stage (EYFS) statutory framework , Safeguarding Children and EY professionals - Online safety considerations and Keeping children safe in education.

We accept that the internet and social media are inherent to people's lives and important for sharing information as well as a learning tool. However, we are also aware that this global network comes with its own risks and dangers and therefore e-safety should be embedded across all areas of the organisation, linking to existing policies concerning behaviour, child protection, data protection and the staff code of conduct. Developments in technology have transformed learning in recent years, and early years practitioners should embrace the opportunities offered by advances in information and communications technology (ICT), while ensuring children are safeguarded and protected from potential harm.

We believe that children flourish best when they are offered opportunity to experience using different forms of media and technology which is aimed at their own personal developmental ability. We ensure that access to this technology is safe and protected and that we operate in line with our values and within the law when creating, using, and sharing images of children and young people.

This policy is drawn up to protect all parties – the children, the staff and the setting and aims to provide clear advice and guidance on how to minimise risks and how to deal with infringements. This policy should be read in conjunction with other statutory and local guidance:

- Children Act
- Information sharing advice for safeguarding practitioners
- Inspecting safeguarding in early years, education and skills settings
- Statutory framework for the early years foundation stage
- Understanding and Supporting Behaviour - safe practice for schools and educational settings
- What to do if you're worried a child is being abused
- Working together to safeguard children

The policy is reviewed regularly by the Leadership Team

- Each setting has an E-safety Co-ordinator. This will be the Designated Safeguard Lead as it is considered that the roles overlap.
- The Business E-Safety coordinator is Michelle Wisbey, Preschool Director

Updated: March 10, Feb 13, Oct 13, Jan 16, Sept 18, July 19, May 2020, April 2022
Next Annual review date: September 2022

Context

Early Years settings are increasingly using devices, such as tablets, directly with children. This can be a great way of role modelling positive use of technology; however, if the activity isn't suitably planned it can cause issues.

The setting plays an essential role in helping young children learn the foundations of safe online behaviour. Even if children don't have access to technology within your setting, they will be using it at home, with their friends or in other public spaces. Children are naturally curious in understanding the world we live in; it is our responsibility to enable them to do so, including helping them to recognise the value of technology and use it safely. Role modelling safe use of the internet should become part of our everyday practice.

As a setting we have a duty to provide developmentally appropriate experience ICT in its various forms to build a foundation on which children can develop their knowledge with internet, e-mail and computer use and we have a duty of care to ensure that every child is safe whilst using the virtual or digital world.

Assessing Risk

All early year's provisions have a duty to ensure that children are protected from potential harm, both within and beyond the learning environment, and therefore it is vital that online safety is a priority for staff. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a setting computer or device. The setting cannot accept liability for material accessed, or any consequences of Internet access.

The setting will regularly audit ICT use to establish if the e-Safety policy is continuing to be effective and changes will be implemented where necessary.

What online risks might children in early years settings experience?

Early years children could be at risk of…

- Content (what they may see):
- Exposure to inappropriate videos. pictures or messages which might upset, worry, or frighten them
- Imitating harmful or inappropriate behaviour they see online
- Searching for inappropriate content on purpose or stumbling upon it by accident. This would include using voice activated tools to search for content
- Inadvertently giving apps or websites permission to share their location or other personal information
- Spending real money via in-app or in-game purchases
- Contact (who might communicate with them):
- Being abused online (including sexually) by people they don't know, such as when gaming or using video chat
- Being abused online (including sexually) by people they know, such as friends and family members
- Sending images or information to people on the device's contact list
- Conduct (how they might behave):
- Exhibiting unhealthy behaviours and boundaries around their use of screens
- Being unkind to each other online as well as offline; this could be using mean words or by excluding others from their games
- Using words or terminology which are not appropriate for their age

- Engaging in unhealthy relationships
- As part of natural development, early years children may exhibit curiosity about their own and others' private body parts; if this occurs via technology children may be at risk of taking inappropriate or indecent images and videos of themselves – the Brook traffic light tool can help practitioners to determine whether sexual behaviour is normal healthy sexual development or harmful behaviour which is a cause for concern.

Online risks that should be recognised include:

- prolonged exposure to online technologies, particularly from an early age
- exposure to illegal, inappropriate, or harmful content
- grooming
- cyberbullying
- making, taking and distribution of illegal images and "sexting"
- physical, sexual, and emotional abuse
- identity theft
- privacy issues
- addiction to gaming or gambling
- pressure from the media and targeted advertising
- theft and fraud from activities such as phishing
- viruses, malware, etc
- damage to professional online reputation through personal online behaviour.

How to minimise risk include:

- Check apps, websites, and search results before using them with children.
- Children will be given clear objectives for internet use set as age appropriate.
- Children should always be supervised when accessing the internet.
- Ensure safety modes and filters are applied - default settings tend not to ensure a high level of privacy or security. But remember you still need to supervise children closely.
- Role model safe behaviour and privacy awareness.
- Talk to children about safe use, for example ask permission before taking a child's picture even if parental consent has been given.
- Make use of home visits to inform your understanding of how technology is used within the home and the context of the child with regards to technology.
- Check privacy settings to make sure personal data is not being shared inadvertently or inappropriately.
- Children will be limited on the amount of time they spend accessing an electronic device.

Evaluating online content

- The setting manager will ensure that the use of internet derived tools and programmes by staff and the child, is age appropriate and complies with copyright law.

Managing technology and devices within the setting

- The use of mobile phones in the classroom by staff, parents and carers' is forbidden to ensure the safety of the children. ***Staff mobile phones can only be used in the setting office during working hours.***

- Staff should **NOT** take photos of children on any personal IT devices.

- Wearable technology e.g., smart watches. These must **NOT** be Bluetooth activated whilst in working in the setting. This will be reviewed, and any staff infringements will lead to wearable technology being banned in the setting.

- The setting currently uses iPad for observational record keeping. All iPads contain cameras which can take both still and video images. The cameras are for the sole purpose of providing photographic evidence for a child's developmental observational records.

- The setting iPad camera(s): this is used by individual staff to evidence children's learning. It is the responsibility of the setting manager/deputy and all staff to ensure its safe use. Photographs from this camera are used on our observational record keeping system and occasionally on the website. The memory storage on the camera roll will be cleared on a weekly basis.

- Children's camera: this is for use by the children to record their favourite work, their friends, and their learning journey. These photographs are used to evidence children's achievements and ability in the use of ICT.

- Video camera: footage the children take is shared with the children to increase their confidence with the use of ICT.

- We do not allow children to bring any personal handheld games technology into the setting.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff and children need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

- When using digital images, staff will ensure that they help the children to understand about the risks associated with the taking, using, sharing, publication and distribution of images.

- Staff and children are allowed to take digital/video images to support educational aims, but must follow setting regulations concerning the sharing, distribution, and publication of those images. **Those images should only be taken on setting equipment.**

- Children should be appropriately dressed when taking digital/video images.

- Videos published on the website, or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images.

- Children's full names will not be used anywhere on a website or other social media sites, particularly in association with photographs and videos.

- Care is taken not to include photographs and videos of those children whose parents and carers have requested that their child's image should not be used for advertising or displays.

- Staff will remove photos from the setting iPad weekly.

Publishing children's images and work

- Photographs that include children's will be selected carefully so that individual children cannot be identified or their image mis-used. Where possible we will use group photos rather than full face photos of individual children.

- A child's full name will not be used anywhere on a setting web site or other on-line space, particularly in association with photographs.

- Written permission from parents or carers' will be obtained via the enrolment form before photographs of children are published on setting web site or used in promotional material.

- Work produced by the children will only be published with permission of parent/carers.

- Where parents request permission to photograph or record their own children at special events, permission will first be gained from all parents for their children to be included. (Please see child's enrolment form)

- Photographs and recordings of children are only taken if there is written permission to do so from all parents (Please see child's enrolment form)

What do staff need to be aware of when using social media in their personal life?

Using social media can be great but it can have risks for early years practitioners. The boundaries between the offline and online world are easily blurred; this can have potentially serious consequences for professionals.

Know the setting's policy and procedures

- Staff should read and understand the setting policies and procedures fully; use of social media is covered in the staff code of conduct

- The setting uses social media as a communication tool with parents/carers, staff must follow the guidance set out in the setting policies, such as not sharing photos without consent or using your own personal devices to share content on behalf of the setting.

- The setting uses online learning journals, staff should understand how these should be used safely and in line with the setting data protection obligations.

- Staff should understand the setting policy regarding using work provided devices.

- If staff are unsure of the policies and procedures in your setting, they should contact the Designated Safeguarding Lead (DSL) to find out where they can find this information.

Protect your online reputation

- Content posted online can be copied, shared, or misinterpreted and can potentially be public and permanent. This can influence personal and professional perceptions about you, both positively and negatively.

- It is important to role model positive behaviour and be professional online; posting derogatory comments is never acceptable. Staff should uphold the reputation of the setting,

professionally and personally. Disciplinary or legal action could be taken if you post something online which brings the profession or the setting into disrepute.

- Ask yourself when posting pictures or comments online; “would I say or do this in a face-to-face situation?” and “would it be appropriate for a child, their parents/carers or my manager to see this?”. If the answer to either of these questions is no, it’s probably best not to share it online in the first place!

- speak with your friends and family about your online reputation; it’s important that they understand what photos of you can and can’t be posted on social media.

Manage online relationships

- You should not add parents of children at your setting as friends online; this can blur professional relationships and put you at risk of allegations. If there is a pre-existing relationship or situation which means this is not achievable, you should discuss this with the DSL at your setting and/or your manager so that they are aware and can give you advice.

- Do not give out your personal contact details to children or parents/carers; professional communication should always be through a work provided email, setting-approved digital platform or phone number.

- If you are concerned about something you see on social media, such as comments posted by a parent, make sure you report it to your DSL. If you are concerned about content posted by a colleague, follow your setting’s allegations policy.

What should staff do if they are worried about a child or a colleague online?

- If you are concerned about a child online, follow your child protection procedures and report and record to your DSL or your manager.
  You can also contact a helpline for support and advice:
  - Professionals Online Safety Helpline – Advice and support for professionals working with children with any online safety issues children in their care may face – 0344 381 4772 or helpline@saferinternet.org.uk
  - NSPCC helpline – Advice and support for anyone who is worried about a child or needs information about child protection – 0808 800 5000
- Be aware that early years children may take or share photos of their private body parts; these photos would likely, in a legal context, be considered to be indecent images of children. If you are aware of indecent images of a child, do not print, forward, save or share these images (this is illegal); report concerns immediately to your DSL.

What should staff do if they have a concern?

Here are some important things to consider in the event of a concern about a child:

- If you are worried about a child for any reason, it is important to tell someone straight away. Follow the setting child protection policy and report concerns immediately to the DSL so that the correct steps are taken from the start.
- Ensure that you are familiar with reporting procedures in the setting and that confidentiality is not promised to the child, or parent or carer in question as this could compromise subsequent investigations.
- Ensure that the child’s own words are used and are not changed in any way when recording a concern; avoid asking leading questions.
- A calm and non-judgemental approach is key, particularly if it is about a sensitive issue.

If you are concerned about the behaviour of a colleague online, follow your allegations procedures and report and record to your DSL or your manager. If you are unhappy with the response you

receive, follow the setting whistleblowing policy, you can also contact the NSPCC whistleblowing helpline.

Protecting personal data

- Personal data will be recorded, processed and made available in accordance with the General Data Protection Regulation 2018
- Children's academic records are stored on a secure online learning app in line with, as the General Data Protection Regulation 2018.
- The setting computer and iPad is password protected
- Confidential records and Individual children's education files are password protected and only authorised staff have access to this information.

Authorisation

- All staff will be required to adhere to the Staff Code of Conduct Policy. Any infringements of the ICT & Social Media rules are deemed a disciplinary offence.

Handling e-Safety complaints

- Complaints of ICT misuse will be dealt with by the e-Safety Co-ordinator.
- Any complaint about staff misuse will be referred to Michelle Wisbey, Principal
- Staff are given information about infringements and sanctions.

Staff

- Understand their safeguarding responsibility with regards to E-safety and are clear about how it fits into their role on a day-to-day basis
- Understand and follow the procedures for reporting and recording online safety concerns, in line with the child protection policy.
- 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 - there are details of useful websites that will provide links to appropriate content at the end of the document
- Model safe practice when using technology with children
- Ensure data is shared online in accordance with the settings data protection responsibilities
- Staff are trained and provided with regular updates on online safety issues

Managers

- They are aware of how and why technology is used within the setting by staff and children. This should include types and number of devices, if they are connected to the internet and if so, how (e.g., Wi-Fi)

- Access to the setting's network and IT infrastructure is secure, such as use of passwords, screen locks, protected devices if removed from site

- Appropriate filtering and monitoring are in place and the setting has documented how decisions have been made; advice regarding appropriate filtering and monitoring is available from the UK Safer Internet Centre

- Access to setting's devices is managed and monitored

- Setting's devices are kept securely and in line with data protection requirements.

- Physical safety of users has been considered e.g., posture of children/staff when using devices.

- Personal data is managed securely online, in accordance with the statutory requirements of the General Data Protection Regulations (GDPR) and Data Protection legislation. This should include considerations given to the use of online learning journals or apps if used by staff.

Parents and carers

- Parents' and carers will be reminded of their responsibilities and the setting policy via newsletters, web site and other communications.

Responsibilities

The responsibilities of the setting manager are:

- to ensure that all members of staff have read and understood this policy, and to make them aware of the severity of their actions should they choose not to put the policy into practice.
- to make sure the parents are aware of this policy.

The responsibilities of staff are:

- to read and confirm understanding of this policy.
- to work according to the terms set out in this policy.

The responsibilities of parents are:

- to be aware of this policy and what measures can be taken at home to keep children safe from harm regarding e-safety.

The responsibility of the Business Owner is:

- to ensure that all members of staff have read and understood this policy, and to make them aware of the severity of their actions should they choose not to put the policy into practice