Online Safety (inc. mobile phones and cameras)

Chestnut Playgroup Linton

Policy Statement
We take steps to ensure that there are effective procedures in place to protect children, young people and vulnerable adults from the unacceptable use of Information Communication Technology (ICT) equipment or exposure to inappropriate materials in the setting.

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 staff 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 online 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. We will communicate our safe practice in the use of technologies with families and manage any concerns.

This policy applies to everyone - staff, children, parents/carers, visitors and contractors accessing the internet or using technological devices on the premises wherever possible. The policy is also applicable where staff or individuals have been provided with setting issued devices for use off-site.

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 setting.

Procedures
- Our Designated Person responsible for co-ordinating action taken to protect children is: **Samantha Redhead**

Information Communication Technology (ICT) Equipment
- Only ICT equipment belonging to the setting is used by staff and children.
- The Designated Person and the committee are responsible for ensuring all ICT equipment is safe and fit for purpose. Setting issued devices only should be used for work purposes.
- All ICT equipment has appropriate security protection in place, both in and out of setting. Setting issues devices should not leave the premises without security protection already in place.
- The Designated Person ensures that safety settings are set to ensure that inappropriate material cannot be accessed.
- All ICT equipment for use by children is located in an area clearly visible to staff.
- Typical use of any ICT equipment by a child should be comparatively short, usually no more than 10 to 20 minutes, except to allow for completion of a specific activity.
- 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 provider/manager. The settings laptop/devices should be used by the authorised person only. Only technology owned by the setting should be used on the premises and on visits or outings, unless permission otherwise given or in an emergency where the setting mobile is unavailable.
- Children will not use staff personal devices at any time. Any devices brought in from home will be securely stored for the duration of the child's attendance unless prior consent has been given by management. Any medical devices needed for the child's personal use will be risk assessed and managed with safety as a priority.

Internet Access
- Children do not normally have access to the internet and never have unsupervised access. 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.
- If staff access the internet with children for the purposes of promoting their learning, written permission is gained from parents/carers who are shown this policy.
- The Designated Person has overall responsibility for ensuring that children and young people are safeguarded and risk assessments in relation to online safety are completed.
- Children are taught the following stay safe principles in an age appropriate way prior to using the internet;
    - only go on line with a grown up
    - be kind online
    - keep information about me safely
    - only press buttons on the internet to things I understand
    - tell a grown up if something makes me unhappy on the internet

- Designated Persons 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 second hand computer is purchased or donated to the setting, the designated person will ensure that no inappropriate material is stored on it before children use it.
- Children are not allowed to access social networking sites.
- Staff report any suspicious or offensive material, including material which may incite racism, bullying or discrimination to the Internet Watch Foundation at www.iwf.org.uk.
- Suspicions that an adult is attempting to make inappropriate contact with a child on-line is reported to the National Crime Agency's Child Exploitation and Online Protection Centre at www.ceop.police.uk.
- The Designated Person ensures staff have access to age-appropriate resources to enable them to assist children to use the internet safely.
- 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 websites, apps and search results will be checked prior to children having access to them and safety and privacy settings are always kept at the highest level. Staff will model the safe use of devices and online learning including activities away from devices that may support children's understanding of the risks online (further information on these activities can be found via Uk Safer Internet Centre).
- If staff become aware that a child is the victim of cyber-bullying, they discuss this with their parents/carers and refer them to sources of help, such as the NSPCC on 0808 800 5000 or www.nspcc.org.uk, or Childline on 0800 1111 or www.childline.org.uk.

Email

- Children are not permitted to use email in the setting. Parents/carers and staff are not normally permitted to use setting equipment to access personal emails.
- The setting has its own email account(s) 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 (i.e., via Hotmail or Yahoo accounts etc.) with children who they have a professional responsibility for. This also prohibits contact with children who previously attended the setting, again unless there is a prior relationship with the family, and consent given as above. If a practitioner and family are friendly prior to the child coming into the setting, this information is shared with the manager prior to the child attending and boundaries are set and agreed. We would advise staff to avoid direct email contact with children, instead via their parents/carers, and to only do so with the families' express knowledge and consent.
- 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, just as an official letter would be. Care should be taken when forwarding emails from others.
- Staff do not access personal or work email whilst supervising children unless in an emergency.
- Staff send personal information by encrypted email and share information securely at all times.

Mobile Phones

- Children do not bring mobile phones or other ICT devices with them to the setting. If a child is found to have a mobile phone or ICT device with them, this is removed and stored in an agreed area in the playgroup, away from children, until the parent/carer collects them at the end of the session.
- Personal mobile phones are not used by our staff on the premises during working hours. These phones will be kept in an agreed area in the playgroup, away from children. Smart watches should have messaging and camera modes turned off if worn when working directly with children.
- If staff have a break time during their working hours, they may use their mobile phones during these times, in an agreed area not used by children or away from the playgroup.
- Staff, students or volunteers remain responsible for their own property and will bear the responsibility of any losses.
- In an emergency, personal mobile phones may be used in an area where there are no children present, with permission from the manager.
- Our staff and volunteers ensure that the setting telephone number is known to family and other people who may need to contact them in an emergency.
- If our members of staff or volunteers take their mobile phones on outings, for use in case of an emergency, they must not make or receive personal calls, or take photographs of children.
- The playgroup will display a notice advising visitors and parents/carers that mobile phones are not to be used in the playgroup. If a visitor or parent/carer is seen using their mobile phone, they will be asked to use it away from the playgroup. We make an exception if a visitor's company or organisation operates a lone working policy that requires contact with their office periodically throughout the day. Visitors will be advised of a quiet space where they can use their mobile phone, where no children are present.
- In circumstances where there is a suspicion that the material on the setting's mobile phone or technological devices may be unsuitable and provide evidence relating to a criminal offence, the 'Allegations of Abuse' process will be followed (please refer to the setting's 'Child Protection and Safeguarding Policy').
- The setting's mobile phone must only be used for work related matters and have no social media apps downloaded on it.

- The setting's mobile phone and other technological devices remain the property of the setting at all times and should not be taken off of the premises (with the exception of outings or other off-site trips), without permission.
- These rules also apply to the use of work-issued mobiles, and when visiting or supporting staff in other settings.
- Staff, students or volunteers who ignore this policy and use a mobile phone or other technological device on the setting premises without permission may face disciplinary action.
- Exceptions will be made when staff or students need to use their device for medical recording such as in the case of recording sugar levels for a diabetic. The setting will risk assess the use of the device in this instance and remind the student/staff/family member of the strict use of the device for only this purpose.

For all visitors to setting (including parents & carers):
- Mobile phones and technological devices must only be used away from the children and where possible, off site.
- In exceptional circumstances, such as a family emergency, visitors should seek permission from the setting manager to use their mobile phone or technological device within the setting.
- The setting's main phone number can be used for emergencies.
- Photos of children must not be taken without prior discussion with the setting manager and in accordance with the General Data Protection Regulation and Data Protection Act 2018 (GDPR) and within setting policy.
- Visitors remain responsible for their own property and will bear the responsibility of any losses.
- Exceptions may be made when visitors need to use their device for medical recording such as in the case of recording sugar levels for a diabetic. The setting will risk assess the use of the device in this instance and remind the visitor of the strict use of the device for only this purpose.

Cameras and Videos, Use of Images
- It is recognised that one of the key ways to support children's development, and engage parents/carers in children's learning, is through photographs that record their children's activities and achievements. We aim to achieve a balance between safeguarding the children in our care and ensuring families can celebrate their children's achievements through the use of technology.
- We will seek permission from parents/carers to take photographs of their children for this purpose (see the Admission form). A signed consent form is obtained from the child's parent/carer, and is kept on the child's file, covering all cases where images of children are to be used. Parents/Carers can choose to opt out if they no longer wish to be included. These photographs will normally be taken by staff using the playgroup's own camera or mobile phone.
- For specific occasions where an external photographer comes into playgroup to take photographs of the children, parents/carers are informed in advance.
- Our staff and volunteers must not bring their personal cameras or video recording equipment into the setting, unless to take photographs of the staff or setting premises only for work purposes, and with direct permission from the Manager and/or Committee. This includes any device with the ability to capture pictures or videos including, but not limited to, smartphones and smart watches.
- Where parents/carers request permission to photograph or record their own children at special events, general permission is gained from all parents/carers for their children to be included. Parents/carers are advised that this is for personal use and they do not have a right to photograph anyone else's child or to upload photos of anyone else's children. Any other use would require the consent of the parents of other children in the image.
- Where a parent/carer has given consent, but a child or young person declines to have an image taken, it should be treated as consent not having been given and other arrangements should be made to ensure that the child/young person is not photographed/filmed.
- Staff may challenge anyone who is using a camera, mobile phone or video recorder at the setting whom they do not recognise.
- If photographs of children are used for publicity purposes, parental consent must be given and safeguarding risks minimised, for example, ensuring children cannot be identified by name. Where possible, general shots of group activities rather than close up pictures of individual children should be used. Children should be in suitable dress.
- Care will be taken in relation to particularly vulnerable children such as Children in Care, recently adopted or those who have fled domestic abuse.
- Where there is a safeguarding concern where abuse is suspected, the setting should not take images of a child's injury, bruising or similar even if requested by Children's Social Care as per the guidance. The 'Log of Concern and Body Map' must be used to record all factual observations where abuse is suspected.
- In circumstances where there is a suspicion that the material on the setting's mobile phone or technological devices may be unsuitable and provide evidence relating to a criminal offence, the 'Allegations of Abuse' process will be followed (please refer to the setting's 'Child Protection and Safeguarding Policy').
- The setting Designated Safeguarding Lead will be responsible for filtering and monitoring the use of devices within the setting, ensuring that they seek support from an IT specialist should there be concerns about the device and content.
- Recommendations for more information can be found from the Safer Internet Centre.
- Further consideration must be given to requirements within the Early Years Online Safety Considerations for Managers, UK Council for Internet Safety.

Social Media
- Setting social networking sites may contain photographs but will not contain information about children attending. No staff, families or children's personal information will be accessible by users of the site. The manager/administrator will moderate all postings to the site; they will review, and quality assure these before they appear, for example, to ensure they do not reveal personal information. Permission from families will be gained prior to photographs being published.

- Staff are advised to manage their personal social media security settings to ensure that their information is only available to people they explicitly choose to share information with.
- Staff are advised to not accept service users, children and parents/carers as friends on social media due to the risk of a breach of expected professional conduct.
- Staff are advised to avoid personal communication, including on social networking sites, with the children and parents/carers with whom they act in a professional capacity. If a practitioner and family are friendly prior to the child coming into the setting, this information is shared with the manager prior to the child attending and boundaries are set and agreed.
- Staff should not: send social networking site 'friend requests' to, or accept them from, children, young people or parents/carers who use the setting. All communication with children and young people 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. Failure to adhere to the rules and guidelines in this policy may be considered misconduct and could lead to disciplinary and/or criminal investigations.
- In the event that staff name the organisation or workplace in any social media they do so in a way that is not detrimental to the organisation or its service users.
- Staff observe confidentiality and refrain from discussing any issues relating to work.
- Staff should not share information they would not want children, parents/carers or colleagues to view.
- Staff should report any concerns or breaches to the designated person in their setting.
- Staff must not access personal blogs/social networking sites using 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 encourage employees writing about their work on social networking sites or web pages. If employees choose to do so, they are expected to follow the following rules. 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.

Electronic Learning Journals For Recording Children's Progress

- Managers seek permission from the committee prior to using any online learning journal. A risk assessment is completed with details on how the learning journal is managed to ensure children are safeguarded.
- Staff adhere to the guidance provided with the system at all times.

Use And/Or Distribution Of Inappropriate Images

- Staff are aware that it is an offence to distribute indecent images. In the event of a concern that a colleague or other person is behaving inappropriately, the Safeguarding Children and Child Protection policy, in relation to allegations against staff and/or responding to suspicions of abuse, is followed.
- Staff are aware that grooming children and young people online is an offence in its own right and concerns about a colleague's or others' behaviour are reported (as above).

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
- the allegations of harm process being followed using the relevant flowchart

Further Guidance

- NSPCC and CEOP *Keeping Children Safe Online* training: www.nspcc.org.uk/what-you-can-do/get-expert-training/keeping-children-safe-online-course/
- Developmentally Appropriate Technology in Early Childhood (DATEC) Final Report: www.datec.org/
- The Information Commissioner Office website https://ico.org.uk/
- Guidance to the General Data Protection Regulation (GDPR) https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation
- Child Exploitation and Online Protection: www.ceop.gov.uk
- Guidance for settings on the use of images and technological devices
- Safeguarding Children and Protecting Professionals in Early Years Settings: Online Safety Considerations guidance as referenced in the Statutory Framework for the Early Years Foundation stage,2024, 3.6
- Safeguarding Children and Protecting Professionals in Early Years Settings: Online
- Safety Guidance for Practitioners (UK Council for Internet Safety, Feb 2019)

Policy adopted: October 2015 Last reviewed: October 2024

Signed: . . . . . Name: Emily Steele Position: Chair