06 Safeguarding children, young people and vulnerable adults' procedures

06.9 E-safety (including all electronic devices with imaging and sharing capabilities)

An E-safety audit is included in these procedures (see 6.9a) to assist with compliance to the EYFS.

Online Safety

It is important that children and young people attending Maidenbower Preschool Playgroup receive consistent messages about the safe use of technology and can recognise and manage the risks posed in both the real and the virtual world.

Terms such as ‘e-safety’, ‘online’, ‘communication technologies’ and ‘digital technologies’ refer to fixed and mobile technologies that adults and children may encounter, now and in the future, which allow them access to content and communications that could raise issues or pose risks; the issues are:

Content – being exposed to illegal, inappropriate or harmful material

Contact – being subjected to harmful online interaction with other users

Conduct – personal online behaviour that increases the likelihood of, or causes, harm

I.C.T Equipment

- The manager at Maidenbower Preschool Playgroup ensures that all computers have up-to-date virus protection installed.
- Tablets are only used by educators at Maidenbower Preschool Playgroup for the purposes of observation, assessment, and planning and to take photographs for individual children’s learning journeys.
- Staff follow the additional guidance provided with the system
- Screen based assistive technologies may be used to support staff or children in the setting on a case by case basis
    - The setting manager will regularly spot check devices to ensure they are being used safely and securely.
    - Families should be informed of how the setting is supporting children’s use of technology.

Content

- Children should not be alone when using devices. Screen time should be with the co-engagement of an adult
- Screen time for under 2s should be avoided and children 2-5 years should be limited to less than one hour per day – this includes time spent on screens at home.

- Any content should be slow, repetitive and predictable to support children's learning. It should be free of adverts, scrolling and autoplay features.
- Staff should use their professional judgement when assessing educational tools, software and apps.

Internet access

- Children never have unsupervised access to the internet.
- The setting manager ensures that risk assessments in relation to e-safety are completed.
- Only reputable sites with a focus on early learning are used (e.g., CBeebies).
- Video sharing sites such as YouTube are not accessed due to the risk of inappropriate content.
- Children are taught the following stay safe principles in an age-appropriate way:
    - only go online with a grown up
    - be kind online **and** 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
- Staff at Maidenbower Preschool Playgroup support children's resilience in relation to issues they may face online, and address issues such as staying safe, appropriate friendships, asking for help if unsure, not keeping secrets as part of social and emotional development in age-appropriate ways.
- All computers for use by children are sited in an area clearly visible to staff.
- 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.

The setting manager ensures staff have access to age-appropriate resources to enable them to assist children to use the internet safely.

Strategies to minimise risk include:

- Check apps, websites and search results before using them with children.
- 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/discussions with families 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. (Source: https://www.gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-guidance-for-practitioners
- Staff keep up to date with news and research on internet safety

Personal mobile phones and other internet-enabled devices – staff and visitors

- Personal mobile phones and internet enabled devices are not used by staff at Maidenbower Preschool Playgroup during working hours. This does not include breaks where personal mobiles may be used off the premises or in a safe place, e.g. staff room. The setting manager completes a risk assessment for where they can be used safely. This includes smart watches and meta glasses.
- Personal mobile phones are switched off and stored in lockers or a locked office drawer.
- In an emergency, personal mobile phones may be used in the privacy of the office with permission.
- Staff ensure that contact details of the setting are known to family and people who may need to contact them in an emergency.
- Staff do not take their mobile phones or other internet enabled devices on outings.
- Members of staff do not use personal equipment to take photographs of children.
- Parents/carers and visitors do not use their mobile phones on the premises. There is an exception if a visitor's company/organisation operates a policy that requires contact with their office periodically throughout the day phones still should be stored away from any areas that children access and setting phone number given to visitors so that they are still contactable. Visitors are advised of a private space where they can use their mobile.
- Medical evidence is required for an exemption such as diabetes where the phone is used to alert the staff member of reduction in sugar levels. Any electronic devices which are used to manage medical needs must be agreed with the manager. A risk assessment for the storage and management of devices is completed by the manager

Cameras and videos

- Members of staff at Maidenbower Preschool Playgroup do not bring their own cameras or video recorders to the setting. They do not use their own personal phones to take any images or videos.
- Photographs/recordings of children are only taken for valid reasons, e.g., to record learning and development, or for displays, and are only taken on equipment belonging to the setting. Children are given the opportunity to consent to their photograph being taken, even if parent/carer permissions are in place.
- Camera and video use is regularly monitored by the setting manager or designated safeguarding lead.

- Where parents/carers request permission to photograph or record their own children at special events, general permission is first gained from all parents/carers for their children to be included. Parents are told they do not have a right to photograph or upload photos of anyone else's children.
- All photographs at Maidenbower Preschool Playgroup are printed on setting equipment and **should not** be outsourced for printing to an external company.
- Photographs/recordings of children are only made if relevant permissions are in place by parents or guardians. We will advise parents of why we are capturing the image, the security measures that are in place to safely store the image and devices used, how long it will be kept for and how it complies with GDPR legislation and a data protection impact assessment is completed.
- Photographs and Image scraping

  Maidenbower Preschool Playgroup recognises that although some apps and websites provide the option of covering children's faces with emojis and stickers, with the development of AI tools, these can be reconstructed with highly accurate facial likeness. Any photographs used for publicity, will have parent consent and safeguarding risks minimised by ensuring that children are not able to be identified.

  Using stickers and emojis, to protect children's privacy, can be removed or bypassed using editing tools and technology such as image scraping. This means a child's face can still be identifiable or recoverable.

For reference Image guidance for education settings - UK Safer Internet Centre

Closed circuit television (CCTV)

Maidenbower Preschool Playgroup uses Closed-Circuit Television (CCTV) as a supplementary safeguarding measure to help promote the safety, security and wellbeing of children, staff, families and visitors. CCTV is used to support safeguarding practices, assist in the investigation of incidents, protect nursery property, and provide reassurance that high standards of care and professional conduct are maintained.

CCTV cameras are located in designated areas of the nursery (not the toilet or nappy changing areas) and are monitored only by authorised members of the leadership team such as the manager or designated safeguarding lead. Recorded footage will be accessed solely for legitimate safeguarding, security, health and safety, or investigative purposes, and in accordance with data protection legislation and the nursery's Data Protection and Privacy Policies.

To protect the privacy and rights of children, staff and visitors, the nursery does not permit live remote access to CCTV footage from personal devices or off-site locations. Access to recorded footage is strictly

controlled, securely stored, retained only for an appropriate period, and shared externally only where there is a lawful basis to do so.

The nursery recognises the potential risks associated with surveillance, including privacy concerns and unauthorised access to recordings. These risks are mitigated through clear governance arrangements, restricted user permissions, password-protected systems, staff training, routine audits of access, secure storage of footage, and regular reviews of the necessity and proportionality of CCTV use.

CCTV is not intended to replace effective safeguarding practices, supervision, professional judgement, or positive relationships with children and families, but to complement and strengthen the nursery's overall safeguarding arrangements.

Cyber Bullying

If staff become aware that a child is the victim of cyber-bullying at home or elsewhere, they discuss this with the parents and refer them to help, such as: NSPCC Tel: 0808 800 5000 www.nspcc.org.uk or ChildLine Tel: 0800 1111 www.childline.org.uk

Use of social media

Staff are expected to:

- understand how to manage their security settings to ensure that their information is only available to people they choose to share information with
- ensure [name of setting] is not negatively affected by their actions and do not name the setting
- are aware that comments or photographs online may be accessible to anyone and should use their judgement before posting
- are aware that images, such as those on SnapChat may still be accessed by others and a permanent record of them made, for example, by taking a screen shot of the image with a mobile phone
- observe confidentiality and refrain from discussing any issues relating to work
- not share information they would not want children, parents or colleagues to view
- set privacy settings to personal social networking and restrict those who can access them
- not accept service users/children/parents as friends, as it is a breach of professional conduct
- report any concerns or breaches to the designated safeguarding lead in their setting
- not engage in personal communication, including on social networking sites, with children and parents with whom they act in a professional capacity. There may be occasions when the educator and family are friendly prior to the child coming to the setting. In this case information is shared with the manager and a risk assessment and agreement in relation to boundaries are agreed

Use/distribution of inappropriate images

- Staff are aware that it is an offence to distribute indecent images and that it is an offence to groom children online. In the event of a concern that a colleague at [setting name] is behaving inappropriately, staff advise the designated safeguarding lead who follows procedure 06.2 Allegations against staff, volunteers or agency staff.

Supporting families with their child's screen use

- Staff share messages with families on healthy screen use at home during settling in, by providing updates during handover conversations, in newsletters and via the learning portal. Guidance can be found here https://beststartinlife.gov.uk/screen-time-under-5s/

For further information, refer to

- https://help-for-early-years-providers.education.gov.uk/health-and-wellbeing/screen-use
- https://www.ncsc.gov.uk/guidance/early-years-practitioners-using-cyber-security-to-protect-your-settings
- Help for early years providers : Internet safety

https://www.gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations

- https://www.internetmatters.org/advice/0-5/#checklist_for_preschool

Online Safety in the Early Years | LGFL