NORMAN COURT

Norman Court Montessori CIC
E-Safety Policy

At Norman Court Montessori CIC we ensure that there are effective procedures in place to protect, young people and adults from the unacceptable use of Information Communication Technology (ICT) equipment or exposure to inappropriate materials.

Procedures

Information Communication Technology (ICT) equipment
- Only ICT equipment belonging to the setting is used by staff and/or children.
- The staff are responsible for ensuring all ICT equipment is safe and fit for purpose.
- All computers have virus protection installed.
- There is a firewall in place to ensure internet access is limited to safe and appropriate sites.
- Children in the nursery, after school club and holiday club do not bring ICT devices with them to the setting. If a child is found to have an ICT device with them, this is removed and stored in the management office until the parent collects them at the end of the session.

Internet access
- Children do not normally have access to the internet and never have unsupervised access.
- The staff members will only access the internet with the children for the purposes of promoting their learning.
- All staff have responsibility for ensuring that children and young people are safeguarded.
- Children are taught the following stay safe principles in an age appropriate way prior to using the internet;
  - 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
- Staff members 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 nursery, the designated officers will ensure that no inappropriate material is stored on it before children use it.
- All computers for use by children are located in an area clearly visible to staff members.

- Staff members 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 Designated Safeguarding Lead and reported to the police
- If staff become aware that a child is the victim of cyber-bullying, they discuss this with their parents 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 nursery. Parents and staff members are not permitted to use the nursery equipment to access personal emails unless requested by the manager of the setting and in the confinement of the nursery office i.e. to access the log in details for an online training course.
- Staff members do not access personal or work email whilst supervising children.
- Staff members share information securely at all times.

Social media
- Staff members are advised to manage their personal security settings to ensure that their information is only available to people they choose to share information with.
- Staff members are not permitted to accept service users, children and parents as friends due to it being a breach of expected professional conduct.
- Staff members are not permitted to put their place of work on any social media site.
- In the event that staff members 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 members observe confidentiality and must refrain from discussing any issues relating to work
- Staff members should not share information they would not want children, parents or colleagues to view.
- Staff members should report any concerns or breaches to the manager of the setting.
- Staff members avoid personal communication, including on social networking sites, with the children and parents 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 must be shared with the management team prior to a child attending and an agreement is reached in relation to agreed boundaries.
- Social media accounts for the organisation are managed and maintained by the setting manager and marketing manager. Photographs used for social media marketing follow permission provided by parents/guardians.

Use and/or distribution of inappropriate images
- Staff members 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 Allegations Against a Member of Staff policy followed.
- Staff members are aware that grooming children and young people on line is an offence in its own right and concerns about a colleague's or others' behaviour are reported (as above).