Policy Document:

Online Safety.

Policy Document:

Online Safety.

Policy statement
The Meadows Day Care Centre 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 adults 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 e-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.

Scope of the policy
This policy applies to everyone- staff, children, parents/carers, visitors and contractors accessing the internet or using technological devices on the premises. 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 early years setting.

Hardware and provision use
Where staff have been issued with a device (e.g. setting laptop or tablet) for work purposes, personal use is not permitted unless authorised by the Centre Manager. The Centres laptop/devices should be used by the authorised person only. Only technology owned by the Centre will be used on the premises and on setting visit or outings. This includes mobile devices for everyday use. Staff taking photographs or recording with technology not owned by the Centre is only allowed if prior permission is given by the Centre Manager and at last resort should Centre devices be unavailable.

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.

Centre issued devices only should be used for work purposes and, if containing sensitive information or photographs of children, should not leave the premises unless encrypted.

Online searching and installing/downloading of new programs and applications is restricted to authorised staff/management committee members only. Children should not be able to search or install anything on a setting device.

Centre issued devices should not leave the premises unless encrypted and this must be acknowledged in the policy. In the case of an outing, all data must be transferred/deleted from the setting's camera/device before leaving the setting.

Data storage and management

The Centre recognises that some staff members may wish to work on electronic documents, i.e., reports, whilst not at work. Any such electronic documents may only be transported out of the Centre e.g., on memory sticks, etc. with prior permission of the Centre Manager providing staff agree to the following:

- All electronic documents must be stored on a dedicated secure device.
- All storage devices must be kept secure at all times.
- The storage device must not be made accessible to, or be used by any other individual.
- All electronic documents are private and confidential and information contained in those documents must not be shared outside of the Centre.
- All PC/Laptop equipment used by the staff member must have suitable security software installed.
- Loss of any storage device or data may result in disciplinary procedures.

The electronic documents stored on all internal computer equipment will be 'backed-up' to the Microsoft Cloud through an Office 365 subscription or Google Cloud through the Centre's subscription. All data will be securely synced from the device to individual user accounts on the Microsoft Office 365 or Google server. Access to these files; either on Centre equipment or via logging into the cloud server; will be secured by the means of a password issued to users by the authorised Centre management/committee members.

The Centre recognises that authorised Centre management/committee members may need to access some electronic documents backed-up to the cloud whilst not on the premises. Access to these documents will be limited and the conditions; as shown above; for staff members apply.

Centre issued devices should not leave the premises unless encrypted. In the case of an outing, all data must be transferred/deleted from the setting's camera/device before leaving the setting.

Email

The Centre has access to a professional email account 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.

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.

Social Networking

Employees must not access personal blogs/social networking sites on Centre premises, use the Centre'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 condone employees writing about their work on social networking sites or web pages. If employees choose to do so, they are expected to follow the rules below.

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 Data Protection Act.
- 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.

Communication with children and young people, by whatever method, 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.

Staff should not: send social networking site 'friend requests' to, or accept them from, children or young people who use the Centre. Staff should also use caution when sending or accepting 'friend requests' from parents who use the Centre.

Failure to adhere to the rules and guidelines in this policy may be considered misconduct and could lead to disciplinary and /or criminal investigations.

Remember that anything posted online could end up in the public domain to be read by children, parents or even future employers – so be careful what you post and who you post it to. For example, posting explicit pictures of yourself could damage your reputation and that of your profession and organisation. Parents and employers may also question your suitability to care for children.

The Centre social media sites

The Centre social networking sites containing information about children attending the setting must be "closed" i.e., the users of the site are accepted and monitored by the appointed site administrator (a nominated member of staff with permission from the Centre Manager). No staff, families or children's personal information will be accessible by users of the site and the appointed site administrator will ensure that users' profiles are kept private. The appointed site administrator will moderate all postings to the site; they will view and quality assure these before they appear, for example, to ensure they do not reveal personal information.

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
- allegations process being followed

Other relevant policies and guidance

- Social Network and Blog policy.
- Use of Digital Photography policy.
    - Guidance for settings on the use of images and technological devices.
- Mobile Phone and Sharing of Images Policy.