08. ONLINE SAFETY & USE OF SOCIAL MEDIA

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 at ASK Kindergarten & Clubs (ASK).

This policy sets forth guidelines that employees should follow for all online communications that refer to ASK. This policy includes (but is not limited to) the following:

- Facebook
- Twitter
- Linkedin
- Flickr
- Instagram
- Snapchat
- Google+
- Tumblr
- YouTube
- about.me
- Myspace
- Personal blogs
- Personal websites

Social networking sites allow for more personal information to be accessed by the public than ever before. With this in mind, because of the very nature of our business, we have a strict policy regarding employees' use of these social networking sites.

Whilst we do not forbid employees from using social networking sites, we need to impose certain restrictions on an employee as to their profile content in relation to ASK, and to the passing of certain work related information which must comply with the law regarding copyright, plagiarism and the Data Protection Act.

Procedures

- Our designated person (manager/deputy) responsible for co-ordinating action taken to protect children is:

  Mark Stewart

Information Communication Technology (ICT) equipment

- Only ICT equipment belonging to ASK is used by members of staff and children.
- The designated person is responsible for ensuring all ICT equipment is safe and fit for purpose.
- The designated person ensures that safety settings are set to ensure that inappropriate material cannot be accessed.

Internet access

- Children do not normally have access to the internet and never have unsupervised access.
- If members of staff access the internet with children for the purposes of promoting their learning, written permission is gained from parents 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 on line
  - 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.
- All computers for use by children are located in an area clearly visible to staff.
- Children are not allowed to access social networking sites.
- Members of 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 members of staff have access to age-appropriate resources to enable them to assist children to use the internet safely.
- 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 at ASK. Parents and members of staff are not normally permitted to use ASK equipment to access personal emails.
- Members of staff do not access personal or work email whilst supervising children.
- Members of staff send personal information by encrypted email and share information securely at all times.

Electronic learning journals for recording children's progress

- Managers seek permission from the Registered Provider/owner 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.
- Members of staff adhere to the guidance provided with the system at all times.

Use and/or distribution of inappropriate images

- Members of 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 members of staff and/or responding to suspicions of abuse, is followed.
- Members of staff 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).

Use of social media

- ASK holds all employees individually responsible for reading, knowing and complying with, any social networking Terms of Service documents of the sites they use.
- Employees of ASK must not use the name of the business on any social networking site.
- Employees must not identify themselves as an employee of ASK. Anyone using social networking sites becomes, to some extent, a representative of their workplace, and everything he/she posts has the potential to reflect on the business and its image. If an employee has already revealed a connection to ASK, posts should contain disclaimers

that make it clear that opinions expressed are solely those of the author and do not represent the views of ASK.

- Employees of ASK must not identify themselves as working with children – this can lead to being a specific target in order for others to gain access to children for paedophile purposes.
- All information regarding anything to do with ASK is not to be discussed or referred to on any such sites, even in private messaging with restricted access between site members.
- There must not be any disclosure of personal information with regard to other members of staff of ASK, children attending the kindergarten or clubs, and parents or carers.
- Employees must not use any social networking site during working hours. Online times and times of posts can be seen by other users and they may assume that ASK allows access whilst working, thus compromising the safety of the children in our care.
- Employees must not refer to children or their parents in any way. ASK's relationship with parents is considered an important and valuable asset that can be irrevocably damaged through a thoughtless comment.
- ASK employees must not request to be network friends of parents of children currently attending the kindergarten or clubs or their known family members. In this social setting it is easy to cross the line by inadvertently discussing the child even with the parent's permission. All members of staff of ASK must comply with the Data Protection Act at all times, both in and out of work.
- We prefer that employees are not network friends with parents of children attending ASK though we realise that, in some cases, the parents may already be family friends with an employee. In such cases, no information whatsoever regarding the kindergarten, its employees or children, is to be divulged at any time. Confidentiality is of paramount importance. All members of staff of ASK must comply with the Data protection Act at all times and ASK employees must never share or post photographs that show any child from the kindergarten in any form, even with parental consent, at any time.
- Defamatory statements can lead to lawsuits against the author of the statement and can, at the very least, bring bad publicity to ASK.
- Social networking sites, by their very nature, are designed to enable anybody, anywhere in the world, to search for others. Even though you may think that only your friends can view your public profile, the chances are that it is openly available for anybody to see. The best advice is that you never post any comments or any photographs that can be misconstrued or misinterpreted in any way. You really do not know who might have a look at your profile and read anything that you choose to say.

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.

Other useful Pre-school Learning Alliance publications

- Safeguarding Children (2013)
- Employee Handbook (2012)