Online Safety

At ACE 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 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.

1. Scope of the policy

This policy applies to; staff, children, parents/carers, visitors, students 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:

- Use technology as appropriate to enhance children's learning for example, showing clips on the tablets when learning about something new, or allowing children to take digital photos which can then be used to enhance displays of their work.
- Highlight for children how technology is used in different ways for example, explaining how computers are used to communicate with parents/carers.
- Raise awareness amongst staff and parents/carers of the potential risks associated with online technology.
- Maintain a safe and secure online environment for all children in our care; always checking online material directly before showing to the children and not allowing the children free access to the internet.
- 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 through our policies and procedures.

2. Use of hardware

Where staff have been issued with a device (e.g. laptop or tablet) for work purposes, personal use off site **is not** permitted, unless authorised by a member of the management team.

- The laptop contains personal information and photographs of children and should never leave the premises. The laptop is locked away at the end of each day.
- The tablet is sometimes used to take photographs or videos of the children or by the children and these are transferred to the computer immediately after use. The tablet is locked away at the end of each day.
- If a tablet is to be used off site all sensitive information and photographs and transferred beforehand.
- Nursery laptop/devices should only be used by authorised persons.

- Only technology owned by ACE will be used when staff are working with children, on the premises, on visits or outings. This includes mobile devices for everyday use and, in case of emergency, a nursery mobile phone is provided. Email will not be accessible via the tablet or laptop.
- Staff are not permitted to take photographs or record with technology not owned by ACE.

When using devices with children:

- Children using the tablet will be supervised at all times, with at least one member of staff present.
- On occasion, children will have supervised access to a variety of internet sites allowed by the firewall and strict filter settings, which filter out potentially inappropriate material such as adult text, images and videos.
- Staff must look at the website/resource page before showing the children any content. This must be done seconds before re-playing it with the children. Staff must feel confident that the content is suitable.
- Children are not able to search or install anything on an ACE device. Online searching and installing/downloading of new programs and applications is restricted to management.
- All staff have a shared responsibility to ensure that children are supervised when using the internet and related technologies. Staff should ensure appropriate and safe use as part of the wider duty of care, reporting issues of concern promptly to the manager.

Unsuitable internet sites **MUST** be reported to the management team, who will follow the Cambridgeshire County Council flowchart of procedures as appropriate. Any incidents which raise a concern will be logged and reported to www.ceop.police.uk if necessary. Designated child protection members of staff for reporting are:

- ACE Day Nursery - Sarah Piotrowski and Hanna Ochalik-Baca
- ACE Nursery School - Lisa Tuohy

3. Email

ACE nurseries have 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.

4.Social networking

ACE recognises that some employees may wish to access the internet on their own devices and participate in social networking on sites such as Facebook, Twitter and Instagram during breaks. Employees must not, however, access personal blogs/social networking sites using ACE internet systems or email address. Employees must not use their personal devices when working with the children.

ACE 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. Employees must ensure they do not breach the law or disclose any confidential information about ACE, children, families or other employees.

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 General Data Protection Regulations (GDPR).
- disclose the name of the setting or allow it to be identified by any details at all. This includes posting photos of children, 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.
- send social networking site 'friend requests' to, or accept them from, children, parents or carers who use the setting.

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.

Remember that anything posted online could end up in the public domain to be read by children, parents/carers or even future employers. 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/carers and employers may also question your suitability to care for children.

5. Sanctions

Misuse of technology/internet and failure to adhere to the rules and guidelines in this policy may be considered misconduct and could lead to disciplinary and /or criminal investigations and may result in:

- allegations process being followed
- the logging of an incident
- disciplinary action
- reporting of any illegal or incongruous activities to the appropriate authorities

6. Working with parents and carers

To assist families in understanding the risks associated with the Internet and e-safety, ACE will provide a link on our website to:
http://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

7. Monitoring systems

This policy will be reviewed annually; shared with staff and parent committee. The tablet/laptop filter settings will be checked every term to make sure they remain set to strict filter and recorded in the child protection folder.

8. Other relevant policies and guidance

- Use of mobile phones and technological devices
- Guidance for settings on the use of images and technological devices

Useful External contacts

Multi Agency Safeguarding Hub (MASH). For professional conversations, advice and guidance and to phone an urgent referral to social care	0345 045 1362
Early Years Safeguarding Manager	01223 714760
Local Authority Designated Officer (LADO)	01223 727967
Education Child Protection Service ecps.general@cambridgeshire.gov.uk	

Adopted: Summer term 2019

Review date: Summer term 2020

Signed: Sarah Piotrowski

Position: Manager