E-Safety Policy
August 2020
Review August 2021

Statement of intent

At the Acorn Childcare Centre (the Centre) we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for children and play an important role in their everyday lives. Whilst the Centre recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use. Our Centre has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all children and staff. The Centre is committed to providing a safe learning and teaching environment for all children and staff, and has implemented important controls to prevent any harmful risks.

1. Legal framework

1.1. This policy has due regard to the following legislation, including, but not limited to:

Human Rights Act 1998
Data Protection Act 2018
Freedom of Information Act 2000
Regulation of Investigatory Powers Act 2000
Safeguarding Vulnerable Groups Act 2006
Education and Inspections Act 2006
Computer Misuse Act 1990, amended by the Police and Justice Act 2006
Communications Act 2003
Protection of Children Act 1978
Protection from Harassment Act 1997
General Data Protection Regulation (GDPR) May 2018

1.2. This policy also has regard to the following statutory guidance:

DfE (2019) 'Keeping children safe in education'

1.3. This policy will be used in conjunction with the following Centre policies and procedures:

Behaviour Management & Exclusions Policy
Anti-Bullying Policy
Data Protection Policy
Safeguarding & Child Protection Policy

Allegations of Abuse Against Staff Policy
Staff Acceptable Use Policy & Agreement
PSHE Policy
Teaching & Learning Policy

2. Use of the internet

2.1. The Centre understands that using the internet is important when raising educational standards, promoting children's achievement and enhancing teaching and learning.

2.2. Internet use is embedded in the statutory curriculum and is therefore an entitlement for all children, though there are a number of controls the Centre is required to implement to minimise harmful risks.

2.3. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:

Access to illegal, harmful or inappropriate images
Cyber bullying
Access to, or loss of, personal information
Access to unsuitable online videos or games
Loss of personal images
Inappropriate communication with others
Illegal downloading of files
Exposure to explicit or harmful content, e.g. involving radicalisation
Plagiarism and copyright infringement
Sharing the personal information of others without the individual's consent or knowledge

3. Roles and responsibilities

3.1. It is the responsibility of all staff to be alert to possible harm to children or staff due to inappropriate internet access or use, both inside and outside of the Centre, and to deal with incidents of such as a priority.

3.2. The Directors are responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard children. The Directors have appointed the Centre Manager to be the E-Safety Officer to monitor this on its behalf.

3.3. The E-Safety Officer is responsible for ensuring the day-to-day e-safety in the Centre, and managing any issues that may arise.

3.4. The E-Safety Officer is responsible for chairing the E-Safety Committee, which includes representatives of the Centre's staff, directors and parents. WE DO NOT HAVE A COMMITTEE. DO YOU WANT TO REMOVE THIS ENTRY?

3.5. The Data Protection Officer is responsible for ensuring the safeguarding of sensitive data and information regarding internet use and concerns flagged.

3.6. The E-Safety Officer will ensure that relevant staff receive CPD to allow them to fulfil their role and train other members of staff.

3.7. The E-Safety Officer will provide all relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach children about online safety.

3.8. The Directors will ensure there is a system in place which monitors and supports the E-Safety Officer, whose role is to carry out the monitoring of e-safety in the Centre, keeping in mind data protection requirements.

3.9. The E-Safety Officer will regularly monitor the provision of e-safety in the Centre and will provide feedback to the Directors.

3.10. The E-Safety Officer will maintain a log of submitted e-safety reports and incidents.

3.11. The E-Safety Officer will establish a procedure for reporting incidents and inappropriate internet use, either by children or staff.

3.12. The E-Safety Officer will ensure that all members of staff are aware of the procedure when reporting e-safety incidents, and will keep a log of all incidents recorded.

3.13. Cyber bullying incidents will be reported in accordance with the Centre's Anti-Bullying Policy

3.14. The Directors will hold regular meetings with the E-Safety Officer to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs, as part of the Centre's duty of care. The Directors may appoint an E-Safety Director to manage this on its behalf

3.15. The Directors will evaluate and review this E-Safety Policy on an annual basis, taking into account the latest developments in ICT and the feedback from staff/children.

3.16. The E-Safety Officer will make recommendations to the Directors, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.

3.17. The E-Safety Office is responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.

3.18. All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-Safety Policy.

3.19. All staff will ensure they understand and adhere to the Centre's Acceptable Use Agreement.

3.20. Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.

3.21. The E-Safety Officer is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

3.22. All children will be made aware of their responsibilities regarding the use of Centre-based ICT systems and equipment, including their expected behaviour, at an age-appropriate level.

4. E-safety education

4.1. Educating children:

- An e-safety programme will be established and taught across the curriculum on a regular basis, ensuring that children are aware of the safe use of new technology both inside and outside of the Centre.
- Children will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material and the validity of website content.
- Children will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.
- Clear guidance on the rules of internet use will be presented in appropriate places around the Centre.
- Children are instructed to report any suspicious use of the internet and digital devices.
- PSHE lessons will be used to educate children about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.
- The Centre will hold e-safety events, such as Safer Internet Day and Anti Bullying Week, to promote online safety.

THIS IS VERY SCHOOL BASED. I WILL ADD FOR DISCUSSSION AT DIRECTOR MEETING.

4.2 Educating staff:

- A planned calendar programme of e-safety training opportunities is available to all staff members, including whole Centre activities and CPD training courses.
- All staff will undergo e-safety training on an annual basis to ensure they are aware of current e-safety issues and any changes to the provision of e-safety, as well as current developments in social media and the internet as a whole.
- All staff will employ methods of good practice and act as role models for children when using the internet and other digital devices.
- All staff will be educated on which sites are deemed appropriate and inappropriate.
- All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.
- Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand this E-Safety Policy.
- The E-Safety Officer will act as the first point of contact for staff requiring e-safety advice

4.3 Educating Parents

- E-safety information will be directly delivered to parents through a variety of formats, including newsletters, the Centre website and social media.
- Twilight courses and presentations will be run by the Centre for parents.
- Parents' evenings, meetings and other similar occasions will be utilised to inform parents of any e-safety related concerns.

5. E-safety control measures

5.1. Internet access:

- Internet access will be authorised once parents have returned the signed Admission Form to the Centre for all children who have been granted internet access.
- Children from Y1 and above who attend Malcolm Sargent Primary School (the School) are provided with usernames and passwords, and are advised to keep these confidential to avoid any other children using their login details.
- Children' passwords will be changed on an annual basis and their activity is continuously monitored by the School.
- The School ensures that management systems are in place to allow staff to control workstations and monitor children's activity.
- The School ensures that effective filtering systems are in place to eradicate any potential risks to children through access to, or trying to access, certain websites which are harmful or use inappropriate material. These are provided by the internet service provider and managed by the School's IT consultants, Ark Ltd.
- The School ensures that filtering systems are used which are relevant to children's age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.
- The School controls the Centre's IT systems and ensures that use of appropriate filters and monitoring systems does not lead to 'over blocking', such that there are unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the School.
- The School ensures that all Centre systems are protected by up-to-date virus software.
- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.
- Master users' passwords will be available to the Centre Manager on request to the School for regular monitoring of activity.
- All internet use is monitored by the School for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy.

- The School uses monitoring and safety software called Securus, which is updated regularly by Ark Ltd.
- Securus actively flags and informs the School of any concerns or inappropriate activity, along with photographic evidence and details of user, time and date. Any such activity relating to the Centre will be passed to the Centre Manager.
- Inappropriate internet access will be dealt with through the Disciplinary Policy.

6 Email:

- School children from Y1+ and all staff will be given approved email accounts and are only able to use these accounts. Centre children will not be given such accounts due to their age.
- The use of personal email accounts to send and receive personal data or information is prohibited.
- No sensitive personal data shall be sent to any other children, staff or third parties via email.
- Children are made aware that all email messages are monitored and that the filtering system will detect inappropriate links, viruses, malware and profanity.
- Staff members are aware that their email messages are monitored through the Securus software
- Any emails sent by children to external organisations will be overseen by their room manager/teacher and must be authorised before sending.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.
- Staff ensure good practice regarding confidentiality to sensitive data and information by encrypting emails containing such content. This is done by typing the word 'encryptmail' in the subject line of the email they are sending. It ensures the email is password protected to be viewed by only the person in the 'send' list.

7 Published content on the Centre website and images:

- The Centre Manager will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- Contact details on the Centre website will include the phone number, email and address of the Centre – no personal details of staff or children will be published.
- Images and full names of children, or any content that may easily identify a child, will be selected carefully, and will not be posted unless and until authorisation from parents has been received.
- Children are not permitted to take or publish photos of others without permission from the individual.
- Staff are able to take pictures, though they must do so in accordance with Centre policies in terms of the sharing and distribution of such. Staff will not take pictures using their personal equipment.

- Any member of staff that is representing the Centre online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the Centre, or any information that may affect its reputability.
- The Centre will ask parent's permission for use of photos throughout the Centre, in the media and online, and will comply with these permissions.

8 **Mobile devices and hand-held computers:**

- The Centre Manager may authorise the use of mobile devices by children where it is seen to be for safety or precautionary use.
- Children are not permitted to access the Centre's Wi-Fi system at any times using their mobile devices and hand-held computers.
- Mobile devices are not permitted to be used during Centre hours by children or members of staff.
- Staff are permitted to use hand-held computers which have been provided by the Centre, though internet access will be monitored for any inappropriate use by the E-Safety Officer when using these on the Centre premises.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- Mobile devices will not be used to take images or videos of children or staff.
- The Centre will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.

9 Network security:

- Network profiles for each School child and staff member are created, in which the individual must enter a username and personal password when accessing the ICT systems within the Centre.
- Passwords have a minimum and maximum length, to prevent 'easy' passwords or mistakes when creating passwords.
- Passwords will expire after 90 days to ensure maximum security for children and staff accounts.
- Passwords should be stored using non-reversible encryption.

10 Virus management:

- Technical security features, such as virus software, are kept up-to-date and managed by the IT Consultants for the Centre, Ark Ltd.
- The E-Safety Officer will ensure that the filtering of websites and downloads is up-to-date and monitored.

11 E-safety committee:

- The E-safety Policy will be monitored and evaluated by the Centre's e-safety committee on an annual basis.

- The committee will include a member(s) of the Centre staff, the E-Safety Officer and the designated safeguarding lead (DSL), as well as Directors and parents.

12 Social Media & Networking

- Staff may not access social media whilst supervising the children, unless it is part of a curriculum activity.
- Members of staff should avoid using social media in front of children.
- Members of staff **must not** "friend" or otherwise contact children or parents/carers through social media.
- If children or parents/carers attempt to "friend" or otherwise contact members of staff through social media, they should be reported to the Centre Manager.
- Members of staff should avoid identifying themselves as an employee of the Centre on social media.
- Members of staff **must not** post content online which is damaging to the Centre or any of its staff or children.
- Where members of staff use social media in a personal capacity, they should make it clear that their views are personal.
- Members of staff must not post any information which could identify a child, class or the Centre.
- Members of staff should not post anonymously or under an alias to evade the guidance given in this policy.
- Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal.
- Members of staff should be aware that if their out-of-work activity brings the Centre into disrepute, disciplinary action will be taken.
- Members of staff should regularly check their online presence for negative content via search engines.
- If inappropriate content is accessed online, the E-Safety Officer should be informed.
- Attempts to bully, coerce or manipulate members of the Centre community, via social media, by members of staff will be dealt with as a disciplinary matter.
- Members of staff should not leave a computer or other device logged in when away from their desk, or save passwords.
- Staff members should use their Centre email address for Centre business and personal email address for their private correspondence; the two should not be mixed.
- Children may not access social media during lesson time, unless it is part of a curriculum activity.
- Breaches of this policy by children will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to prosecution, or exclusion.
- Members of staff should exercise caution and consider their professionality and professional boundaries at all times when using social media, and when profiles and comments they make online are visible to the wider Centre community.
- Children and parents/carers should not post anonymously or under an alias to evade the guidance given in this policy.

- Children and parents/carers **must not** post content online which is damaging to the Centre or any of its staff or children.
- Children must not sign up to social media sites that have an age restriction above the children's age.
- If inappropriate content is accessed online on Centre premises, it must be reported to the Centre Manager.
- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the Centre Manager.
- Children are regularly educated on the implications of posting personal data online outside of the Centre.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the Centre as a whole.

13 Cyber bullying

a. For the purpose of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images online.

b. The Centre recognises that both staff and children may experience cyber bullying and will commit to preventing any instances that should occur.

c. The Centre will regularly educate staff, children and parents on the importance of staying safe online, as well as being considerate to what they post online.

d. Children will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHE lessons as well as sex and relationship education.

e. The Centre will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and children.

f. The Centre has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-Bullying Policy.

g. The Centre Manager will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their Local Authority of the action taken against a child.

14 Reporting misuse

- The Centre will clearly define what is classed as inappropriate behaviour in the Acceptable Use Agreement, ensuring all children and staff members are aware of what behaviour is expected of them.

- Inappropriate activities are discussed and the reasoning behind prohibiting activities due to e-safety are explained to children as part of the curriculum in order to promote responsible internet use.

14.1 Misuse by children:

- Staff have the power to discipline children who engage in misbehaviour with regards to internet use.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the E-Safety Officer.
- Any child who does not adhere to the rules outlined in the Acceptable Use Agreement and is found to be wilfully misusing the internet, will have a letter sent to their parents explaining the reason for suspending their internet use.
- Members of staff may decide to issue other forms of disciplinary action to a child upon the misuse of the internet. This will be discussed with the Centre Manager in advance and will follow the Behaviour Management & Exclusions Policy.
- Complaints of a child protection nature, such as when a child is found to be accessing extremist material, shall be dealt with in accordance with our Safeguarding and Child Protection Policy.

14.2**Misuse by Staff**

- Any misuse of the internet by a member of staff should be immediately reported to the Centre Manager.
- The Centre Manager will deal with such incidents in accordance with the Whistleblowing Policy, and may decide to take disciplinary action against the member of staff, following the Staff Code of Conduct and Disciplinary Policy.
- The Centre Manager will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

15 Use of illegal material:

- In the event that illegal material is found on the Centre's network, or evidence suggest that illegal material has been accessed, the police will be contacted.
- Incidents will be immediately reported to the Internet Watch Foundation and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.
- If a child protection incident is suspected, the Centre's child protection procedure will be followed – the DSL and Centre Manager will be informed and the police contacted.

16 Monitoring and review

a. The e-safety committee will evaluate and review this E-Safety Policy on an annual basis, taking into account the Centre’s e-safety calendar, the latest developments in ICT and the feedback from staff/children.

b. This policy will also be reviewed on an annual basis by the Directors; any changes made to this policy will be communicated to all members of staff.

c. Members of staff are required to familiarise themselves with this policy as part of their induction programme.