E-Safety and Acceptable Use Policy

Policy Title	E-Safety and Acceptable Use Policy
Statutory	Yes
Policy Version	3
Policy Author	Mrs A Majcher
Ratified By	FGB
Date Ratified	Summer 2021
Review Period	2 years
Next Review Period	July 2023
Distributed To	All Staff/Parents/Governors
To be published on website	Yes
Changes to this policy	Wording updated in E-Safety Rules for Key Stage 2 – page 12
This policy has been impact assessed against race, gender and disability and no adverse impact has been identified.	

E-Safety and Acceptable Usage Policy

Our e-safety policy will operate in conjunction with other policies including those for pupil behaviour, curriculum subjects, data protection and security.

It involves all members of staff from the Headteacher to any new member of staff. Through its compliance, it will ensure that everyone knows and understands their responsibilities and can act up on them.

Contents

"The internet and e-mail are powerful tools to open up new opportunities for people of all ages. The Government wants everyone to have access to the wealth of cultural, scientific and intellectual material to be found on the internet. But we are equally determined to ensure that pupils are protected from unsuitable material and that they can access appropriate material safely."

Michael Wills (2001) - Minister for Learning and Technology

Introduction

New technologies have revolutionised the movement, access and storage of information with important implications for all schools. Use of ever more powerful computers, broadcast media, the internet, digital recorders of sound and images together with increased opportunities to collaborate and communicate are changing established ideas of when and where learning takes place. At Carrington Junior School, we recognise that learning is a life-long process and that e-learning is an integral part of it. Ensuring that we provide pupils with the skills to make the most of information and communication technologies is an essential part of our curriculum. The school is committed to the continuing development of our Computing infrastructure and embracing new technologies so as to maximise the opportunities for all pupils, staff, parents and the wider community to engage in productive, cooperative and efficient communication and information sharing.

However, as in any other area of life, children are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities which are inappropriate, or possibly illegal.
E-safety seeks to address the issues around using these technologies safely and promote an awareness of the benefits and the risks.

This policy sets out clearly our expectations on pupils, staff, parents and members of the wider community to ensure best practice.

Key: Normal text gives context and information
Italic text indicates teaching given to pupils
Bold texts indicate key expectation to ensure positive and safe use

Acceptable Use of E-Technologies by Staff

It is important that when members of school staff communicate with pupils they remember their professional role.

Communication between children and young people – by whatever method – should take place within clear and professional boundaries. This includes the wider use of technology such as mobile phones, text messages, emails, digital cameras, videos, web-cams, websites and blogs.

This means that staff should:

- *NOT* give their personal contact details to pupils, including their mobile telephone number or personal email address.
- *NOT* use the internet or web-based communication channels to send personal messages to pupils.
- *BE AWARE* of information that they are putting into the public domain (Facebook, Twitter, etc.). Do *NOT* allow children or young people - associated with the school – to be listed as their 'friends' and Do *NOT* allow themselves to be listed as a 'friend' on their sites.
- *NOT* request or respond to any personal information from a pupil.
- *KNOW* that it is the legal responsibility of ALL members of staff to report child protection concerns and follow the school Child Protection Policy.

Email or text communications between a member of staff and a pupil may lead to disciplinary and/or criminal investigations. This also includes communications made through internet sites.

Use of Social Media

On Facebook or other internet communication: discussing school or referring to any child, staff member or groups of children is very unprofessional and against safeguarding and confidentiality practices.

No member of staff should ever allow a child or ex-pupil to become a 'friend' on Facebook or any similar website or mobile communications. This is a serious safeguarding issue. Staff need to ensure their security settings are fixed carefully on Facebook as a lack of security could lead to parents or children knowing about your personal life compromising your professionalism of working in a school.

Physical Safety

- All electrical equipment in the school is tested annually to ensure that it is safe to use.
  Pupils are taught about the dangers of electricity as part of the science and PSHE curriculum. **We expect pupils to behave appropriately near electrical sockets and appliances.**
- Workstations are cleaned and sanitised regularly. *Pupils are taught to avoid taking food and liquids anywhere near the computers.* **We expect all users to refrain from eating and drinking when working at a computer.**
- Health and safety guidance states that it is not healthy to sit at a computer for too long without breaks. *Pupils are taught correct posture for sitting at a computer and that sitting for too long at a computer can be unhealthy.* **We expect all users to take responsibility for their own physical well-being by adopting good practices.**
- Computers and other IT equipment can be easily damaged. *Pupils are taught the correct way to use IT equipment.* **We expect pupils to respect IT equipment and take care when handling and using.**

Network Safety

- All staff users need to log on using a unique username and password. Pupils log on with their year group login. *Pupils are taught that they should only access the network using those particular logins.* **We expect all users to only logon using their individual or year group username.**
- Each user is given an allocation of disk space for the storage of their work. *Pupils are taught how to save their work into their "My documents" area.* **We expect pupils to save and keep their work to build up a portfolio of evidence.**
- Access to other users "My documents" areas are restricted by the network. *Pupils are taught not to access another user's work without permission.* **We expect pupils to respect the privacy of all other users and to make no attempt to access or interfere with another user's work.**
- On the network there are "shared resource" areas where many different groups of users can save work so that it is available to others. *Pupils are taught how to access and save to these shared resource areas.* **We expect pupils to respect the**

contributions of others, not to delete or alter others' work and to ensure that they only save work to shared areas with permission.

- Each user has the capability to print their work. *Pupils are taught to only print when necessary to save resources for financial and environmental reasons.* **We expect pupils to only print out work when directed by staff to do so.**
- The network software prevents changes being made to computer settings. *Pupils are taught that making changes may prevent the computer from working properly.* **We expect all users to make no attempt to alter the way the computer is set up.**
- Only the network administrators are permitted to install software on to computers. *Pupils are taught that the network or an application may not function properly if programs are installed.* **We expect all users to make no attempt to load or download any program onto the network.**
- All users of the network can be monitored remotely by the network administrators. *Pupils are taught that their use of the network can be monitored.* **We expect all users to understand that their use is subject to monitoring.**

Internet Safety

- When using a network workstation all access to the Internet is protected by a number of different filters. These filters are designed to prevent accidental or deliberate access to unsuitable materials. In addition, the network administrators can manually add site addresses which are considered to be unacceptable. However, no system is 100% safe and we expect users to behave responsibly. *Pupils are taught that the internet contains many websites that are useful but that there are also websites that are unpleasant, offensive, not child-friendly or can damage your computer.* **We expect pupils to make no attempt to access a website that they know to be unsuitable for children and/or containing offensive language, images, games or other media.**
- Pupils accessing the internet at home are subject to the controls placed upon them by their parents. However, any home use of the Internet made in connection with the school or school activities; any of its staff, pupils and governors or any partnership organisation will be subject to this policy and any breach dealt with as if the event took place at school. **We expect all members of our school community to behave as positive ambassadors of the school in all school related activities made through the internet.**
- The school website contains school policies, newsletters and other information. **We expect all persons accessing the school website to treat the content with respect and make no attempt to reproduce, use or alter any part in any way with malicious intent. No part can be reproduced for commercial reasons without written permission from the school.**

Email & Seesaw Safety

- Some classes have a class email address which pupils can send homework or school- related questions to. The class teacher monitors the pupil's use of email. *Pupils are taught that emails sent to their class email should have a clear learning purpose and be written in a polite style which is appropriate to the person that will receive it*. **We expect all users to communicate appropriately through email.**
- Some pupils will have their own webmail accounts at home. As these are independent of the school they do not necessarily come with the safeguards that we set for email usage. Therefore, we do not permit the use of personalised email accounts by pupils at school or at home for school purposes. *Pupils are taught*

that using a personalised webmail account in school or for school use is not permitted. **We expect pupils to use school issued email accounts only.**

- The majority of families are signed up to the Seesaw app and therefore have a communication link with class teachers. The class teacher will use Seesaw to: keep parents updated on children's work and progress, update the whole class on notifications, respond to parents' questions and to let parents know about homework that has been set.
- All communication will use a professional tone. Class teachers are expected to keep parents updated on their children's progress weekly (1 maths, 1 English and weekly spelling results per week. 1 topic and 1 science per half term).
- **Important communication/ information will be copied to CPOMs so that SLT are aware. This is strictly confidential.**

Home Learning

- With the home-school communication now readily available, children should have immediate access to remote/home learning should the need for it come.
- Staff will ensure any home learning is accessible for all children – mainly online or by post in very rare circumstances.
- Any learning sent home should enable children to be as independent as possible to relieve extra pressure on parents/carers. This can include: teacher videos, Power-points with voice overs or being directed to specific websites – these websites must be checked and verified by staff before being sent out.
- Teachers will ensure communication with the class and have regular updates with families of vulnerable children.
- Staff will be available for contact via Seesaw during school hours.
- Any marking or feedback of home learning will follow the school marking policy.

Digital Images

- Digital still and video cameras are used for recording special events as well as being essential tools for everyday learning experiences across the curriculum. As part of pupil induction, parents are asked to sign a consent form for images of their children to be used for school purposes. Some images celebrating the work of pupils involved in everyday and special event activities may be selected to be shown on the school website. On the website we never state the child's full name with their image (see policies regarding GDPR). **The school will happily remove any image of a child on the school website at their parents' request.**
- Digital images may be shared with partner schools and organisations as part of collaborative learning projects. This can include live video conferencing. All such use is monitored and supervised by staff. *Pupils are taught to seek permission before copying, moving, deleting or sending any images taken within school.* **We expect all pupils to seek permission from staff before sharing images outside of the school environment.**

Cyber-bullying

- The school takes bullying very seriously and has robust procedures for identifying and dealing with it. E-bullying is the use of any communication medium to offend, threaten, exclude or deride another person or their friends, family, gender, race, culture, ability, disability, age or religion. *Pupils are taught about bullying as part of the PSHE curriculum*. **We expect all members of our community to**

communicate with each other with respect and courtesy. Bullying of any type will not be tolerated by the school and will be dealt with under the procedures within the Behaviour & Exclusions Policy.

Mobile Phones

- Pupils are not permitted to have mobile phones in school. We recognise that our oldest pupils may walk on their own to and from school and parents may wish them to have a mobile phone for emergencies. However, we discourage this on security grounds as they are easily lost, damaged or stolen although with written consent this can be made possible. *Pupils are taught that they should not have a mobile phone on their person in school and that any phone brought in must be handed to the office for the duration of the day*. **We expect pupils not to carry a mobile phone in school. During the coronavirus pandemic no mobile phones are allowed in school.**

Other Technologies

- **Podcasting** – Some pupils will be given opportunities to create oral recordings. Some of these recording may be made available as podcasts through the internet so that they can be shared with interested members of the school community.

Copyright

- Though there are lots of free to use resources on the internet, the majority of image, sound and music files are covered by copyright laws. Some can be used for educational reasons without permission provided that the source is stated and that they are not made available outside the school. Some cannot be used under any circumstances, this is particularly so for music but can apply to other types of file e.g. photographic images. Care therefore needs to be taken with multi-media work which incorporates anything downloaded from the internet or any other published source that it is not uploaded onto the school's website or broadcast through any other technology. *Pupils are taught that the people who put their work on the internet may not always want people to copy or use their work and that they should check whether they have permission.* **We expect all users to respect copyright laws.**
- It is important to know what work is original and when chunks of text have been copied from other sources such as the internet. *Pupils are taught that they should not present the work of others as their own work. Older pupils are taught about copyright and how to extract or paraphrase information through appropriate referencing.* **We expect all pupils to make it clear what is their own work and what is quoted from other sources.**

GDPR

- In line with GDPR guidelines, we must be transparent with regards to the information we hold about a child. When displaying a child's work, we must obey the guidelines (separate policy). When a child leaves the school, their Intellectual Property must be offered to them OR disposed of (again obeying the GDPR guidelines).

Appendix 1

Helpful Websites

- Child Exploitation and Online Protection Centre (CEOP)
  An excellent site providing information on child abuse and other related issues. Parents and children are able to report attempts at grooming to the global taskforce. http://www.thinkuknow.co.uk/
- Childnet International
  a non-profit organisation working with others to "help make the Internet a great and safe place for children". The site contains excellent Internet safety information for parents and children.
  http://www.childnet-int.org/
- National Children's Charity (NCH)
  Loads of useful information to help keep your children safe online.
  http://www.nch.org.uk/information/index.php?i=134
- Kidsmart
  More good ideas and a 10 minute online presentation
  http://www.kidsmart.org.uk/parents/advice.aspx
- Bullying Online
  Advice on what to do if you think your child is being bullied.
  http://www.bullying.co.uk/parents/parentsl_advice.htm
- Childnet International
  Interactive resource dealing with the main causes for concern.
  http://www.kidsmart.org.uk/POL_IPSA_Mac%2BPC/main.html
- Chat Danger
  An excellent site with lots of good information on using chat rooms, email & mobile phones etc
  http://www.chatdanger.com/
- MSN Web Cracker
  A site designed by teenagers for teenagers to help them understand the importance of safe surfing.
  http://www.websafecrackerz.com/

Appendix 2

Glossary of Terms

Email	Text-based messages sent through the internet
Internet	A global network of computers which allow efficient communication from any point to any point
Network	A group of computers linked together and often managed by a server
Podcast	One of a series of sound files uploaded on to the internet and downloaded (or streamed) by subscribers
Server	A computer that controls access to a network of computers and usually stores data for all users
Webmail	Email service which is held on a secure website and can be accessed anywhere on the internet

Appendix 3

It was agreed by all staff during a Computing INSET in October 2018 that one of these posters would be on display in every classroom and the Computing Suite itself. It was also included in a newsletter that went out in the same month.

Appendix 4

Staff E-Safety Agreement

Staff should:

- Not give their personal details to pupils.
- Not use the internet – or web-based communication channels – to send personal messages to pupils.
- Mobile phones must not be used to record images of pupils. School cameras may be used to record images, but these must be downloaded to the school network and not be taken home. All staff have the right to access these files for educational purposes only.
- Colleagues should keep their usernames and passwords a secret.
- Staff should not use the usernames and passwords of any other adult working in the school.
- It is the responsibility of all staff to 'log off' from the 'Staff' log-in screen after using a PC. Private and sensitive information should not be freely visible to pupils and other adults.
- The Internet should **only** be used in school for educational/ school purposes. It should not be used for personal purposes such as booking holidays or ordering groceries.
- Staff – in order to protect the school network from viruses – should only use encrypted memory sticks although the One Drive is preferred.
- Accidental – or otherwise – access to inappropriate or banned content (including pornographic, racial hatred or religious hatred websites or forums) must be reported to the Computing Coordinator in the first instance. The URL will then be reported to Turn It On for blocking.
- School laptops or netbooks must not be used for any illegal or inappropriate activities, e.g. access to, viewing or sharing of banned content.

Use of Social Media

On Facebook or other internet communication discussing school or making reference to any child, staff member or groups of children is very unprofessional and against safeguarding and confidentiality practices.

No member of staff should ever allow a child or ex-pupil to become a 'friend' on Facebook or any similar website or mobile communications. This is a serious safeguarding issue.

Staff need to ensure their security settings are fixed carefully on Facebook as a lack of security could lead to parents or children knowing about your personal life compromising your professionalism of working in a school.

I understand that the above actions could lead to disciplinary action and will compromise my position as a professional working in school.

I have read and shall comply with the above safeguarding and health and safety matters.

I understand that all members of staff have a responsibility for safeguarding and health and safety in the school.

Signed: _____ Date: _____

Print Name: _____

E-Safety Rules for Key Stage 2

Think then Click

E-Safety Rules for Key Stage 2:

- The internet is a useful tool for finding information and learning skills. It is important to use it safely and sensibly at all times.
- I will ask permission before using the internet.
- I will only use websites that an adult has told me are safe.
- I will not search the internet for things that I know adults would not like me to look at.
- I understand that I will not be allowed to use the internet if I break any E-Safety rules.
- I will tell an adult if I see anything I am uncomfortable with.
- I will immediately close any web page I am not sure about.
- I will only e-mail people an adult has approved.
- I will only send e-mails or post messages that are polite and friendly.
- I will never give out my name or any personal information or passwords.
- I know that my teacher has a copy of my usernames and passwords in case I lose or forget them.
- I will not pretend to be anyone or anything I am not while online.
- I will not use the internet in a way which may harm or cause upset to others.
- I know that my teacher and the internet service provider will check sites that I have visited.
- I will never arrange to meet anyone in person through the internet.
- I will not open e-mails sent by anyone I don't know.
- I will not use internet chat rooms or pop-ups.
- I will not put or send pictures of myself on the internet.
- I will not download images, software or apps from the internet.
- If I misuse the internet, I may receive a sanction.

For further details, please download our E-Safety and Acceptable Use policy on the school website.

Please sign and return.

I confirm that I have read the school's E-Safety rules and the E-Safety policy and discussed it with my child.

Parent/Carer name: _____ Signed: _____

I have read the E-Safety rules and I have talked about them with my family. I will follow them at all times.

Child's name: _____ Date: _____