E-Safety Policy

Policy Title	E-safety Policy
Statutory	Yes
Policy Version	1
Policy Author	Mrs A Majcher
Ratified By	FGB Autumn
Date Ratified	Sept 2017
Review Period	3 Years
Next Review Period	September 2020
Distributed To	All staff
To be published on website	No
Changes to this policy	N/A
This policy has been impact assessed against race, gender and disability and no adverse impact has been identified.	

Carrington Junior School

E-SAFETY POLICY

Policy for E-Safety and Acceptable Usage

At Carrington Junior School, we recognise the importance of using, and developing a good understanding of new technologies to enhance learning. Moreover we are aware that the technology will play a fundamental part in the present and future lives of our children and that ICT in our schools should reflect ICT in society.

The school is committed to the developing our ICT in order to create ICT users with the skills necessary to quickly adapt to new technologies, as well as creating effective communication between pupils, staff, parents and the wider community to share our school news.

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.

Network Safety:

- All users need to log on using their username, this is specific to them.
- 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; however they are encouraged to only save the work they need to and not to save too many pictures and large files.
- Access to other users "My documents" areas are restricted by the network. Pupils are taught not to access another user's work without permission.
- On the network there is a 'handout and resources area' where many different groups of users can save work so that it is available to others. Pupils are taught how to access the shared resource area, however we expect pupils to be respectful of other people's work and not to delete anything without permission.
- Pupils are only allowed to print their work under the instruction of an adult. Work prints to the networked photocopier.
- Children will be taught not to change or alter any settings. Although children are unable to access a large part of the network, they still need to be taught the importance of this.
- Only the network administrators are permitted to install software on to the network. Staff requiring additional software must log a support call to be dealt with by the ICT administrators. If apps are required for the tablets or other mobile devices, staff need to ask the ICT tech support; if these are paid apps, permission must be sort from the subject specific budget holder, for example maths**.**
- 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.*

Internet Safety:

- E-Safety is included as an ICT teaching unit in every year group, ensuring that children understand the dangers of the internet and how to keep themselves safe, progressing at an age-appropriate rate. It also features in some PSHCE lessons.
- The school system is filtered by the internet provider for the safety of the children and staff. These filters are designed to protect the children and staff from accidental or deliberate access of unsuitable materials. The network administrators can manually block site addresses which are considered unacceptable, or unblock those sites which are acceptable and have been incorrectly blocked.
- 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. Children are also taught that whilst the internet is useful, not everything on the internet is true and that children need to use trustworthy sources and websites.
- Children are taught to report to the nearest adult, immediately, anything that they see which they find upsetting, inappropriate, or which they believe should have been blocked by the filtering system. All reports of this nature will be logged by the school E-Safety coordinators.
- We teach pupils to make no attempt to access a website that they know to be unsuitable for children and/or containing offensive language, images, games, other media or social networking sites.
- Pupils accessing the internet at home are subject to the controls placed upon them by their parents/carers. 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.**

VLE Safety:

Children can use the VLE for school work and to aid learning. However VLE use is monitored. We teach and expect all children to communicate sensibly through the VLE, being respectful of all other users and members of the community.

Email safety:

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 the school or at home for school purposes. We remind children that when setting up an email account, the email account provider has terms and conditions which should be read and adhered to. Many email account providers set a minimum age limit of 11 years. Most personal email websites are blocked by the school's filtering system, however there is the possibility that some may not be.

Website safety:

Websites accessed out of the school do not come within the safeguards that we set within the school. However, the children are taught that they need to also be very careful when using online sites. They should **never give their real name, school, age or location.** Children are taught the dangers of giving out personal information to strangers on the internet and should always use a nickname rather than their real name. Children should never put a photo of themselves online wearing their school uniform as it makes them easily identifiable and gives a stranger information about where they live. Children are taught that the people that they are communicating with may not be who they think they are – people can lie online.

Digital Images:

- Digital still and video cameras are used for recording events as well as being essential tools for everyday learning experiences across the curriculum. When children arrive at Carrington Junior School, all parents/carers have the opportunity to opt out of their child's image being used by the School. Some images celebrating the work of pupils involved in everyday and special event activities may be selected to be shown on the school website, the closed school Facebook group or Twitter account. On the website we will never state a child's full name with their image. The school will happily remove any image of a child on the school website at their parent/carer's request. Images on twitter will only ever be group shots.
- 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.
- **Staff may not take photos of the children in any state of undress or in swimwear. (Please refer to the staff acceptable use policy with regards to the school's cameras or devices with the ability to capture images, videos or audio recordings).**

Usernames and Passwords:

- Children have a variety of usernames and passwords for the network (username only), different online software packages and the VLE. They are taught not to reveal these to anyone aside from their parent/carers. They understand that staff keep a copy of these securely in order to protect them any incident of E-Safety and also to allow the child access when they may have lost or forgotten their username or password. Children must never be allowed to log on as someone else. (Please refer to the staff acceptable use policy for staff passwords and accounts).

Cyber Bullying:

- The school takes all forms of bullying very seriously. Cyber-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 Whole School Policy on Behaviour, including bullying**.** All incidences of cyber bullying are recorded by the E-Safety coordinators. Cyber bullying which takes place outside of school hours, if reported by a pupil or parent/carer, will be dealt with as far as is reasonably possible by school staff.

Mobile Phones:

- Pupils are not permitted to have mobile phones in the school. Pupils are taught that they shouldn't have a mobile phone on their person in the school and that if a phone is brought into the school, it will be confiscated by a member of staff and only returned to an adult. Pupils must not carry a mobile phone in the school. (Please refer to the staff acceptable use policy with regards to mobile phones that belong to staff).

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, first names only may be used.

Use of electronic communication and recording devices (ECRD):

- **ECRD** includes any device with the capability to capture or record audio, photograph or video or is capable of receiving or transmitting any type of communication between persons.
- Carrington Junior School believes that pupils, school staff, volunteers, visitors and governors should not be subject to having a video or audio recording taken of them without their consent. This aspect of the E-Safety policy protects the privacy rights of pupils, school staff, volunteers, visitors and governors. This means that volunteers, visitors, parents/carers and pupils are not allowed to bring ECRD into the School for the purpose of use them for capturing audio, photographs or video of any person without having obtained that person's consent and the permission of the head teacher.
- The head teacher gives permission for parents/carers (as a member of the ticketed audience) to use an ECRD during whole school or class performances or productions. Any parent or carer has the right to ask for their child to be removed from a production or performance if they do not wish for their child to potentially be recorded in the process of a group recording.
- Carrington Junior School does permit the use of ECRD devices by school staff only in school for the purposes of school based teaching and learning. The use of these ECRD devices is closely monitored by the Head teacher. Use of any audio, photograph or video captured outside of the school is subject to permission having been granted by each pupil's parent or carer (a copy of which will be held on the School's records).

Data Protection Act:

- The Data Protection Act 1998 gives you the right to access information held about you or your child by the school. The school has the right to charge for supplying this information. Further information on the Data Protection Act can be obtained from the Department of Constitutional Affairs – www.justice.gov.uk

Child protection:

- Any E-Safety incident which raises concerns about a child protection issue will be reported to the school designated person and referred to Social Care as appropriate.

E-Safety Rules for KS2

Key Stage 2

Think then Click
E-Safety Rules for Key Stage 2:
. I am not allowed mobile phones in school. . I ask permission before using the Internet. · I only use websites that an adult has told me are safe. . I do 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 am always myself and do 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 do not use Internet chat rooms. . I will not put or send pictures of myself on the Internet.

For further details please download our E-Safety policy on the school website: http://www.cheppingviewprimaryschool.org/Policies

E-SAFETY
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: _________________________ Class: ______________Signed:
____

Updated September 2017