Carniny Primary School

E-Safety Policy

At Carniny Primary School, 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 pupils and play an important role in their everyday lives. Whilst the school 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 school has created this policy with the aim of ensuring appropriate and safe use of the Internet and other digital technology devices by all pupils and staff. The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

The E-Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

1. Scope of the policy

The policy applies to all members of the school community who have access to and are users of the school ICT systems, both in and out of school. In relation to incidents that occur during school hours, we will work with parents, staff and pupils to ensure E-Safety of all involved, apply sanctions as appropriate and review procedures. In relation to incidents that occur outside school hours, the school will work with pupils and parents to keep all pupils safe and offer educative support where appropriate. E-Safety outside school hours is primarily the responsibility of the parents. If inappropriate activity occurs outside school hours, with the intention of having a negative effect on any member of the school community, and is is brought to our attention, we will liaise with appropriate external agencies as to an appropriate way forward. Any issues that arise inside school as a result of E-Safety incidents outside school, will be dealt with in accordance with school policies. (see also Social Media Policy and Positive Behaviour Policy).

2. Risk Assessment

"21st century life presents dangers including violence, racism and exploitation from which pupils need to be reasonably protected. At an appropriate age and maturity they will need to learn to recognise and avoid these risks – to become "Internet-wise" and ultimately good "digital citizens". Schools need to perform risk assessments on the technologies within their school to ensure that they are fully aware of and can mitigate against the potential risks involved with their use. Pupils need to know how to cope if they come across inappropriate

material or situations online. The school risk assessments should inform the teaching and learning, develop best practice and be referenced in the school's Acceptable Use Policy".
DENI E-Safety Guidance, Circular number 2013/25

The main areas for risk for Carniny Primary School can be categorised as the Content, Contract and Conduct of activity.

Content

- Access to illegal, harmful or inappropriate images or other content.
- Access to unsuitable video/internet games.
- Inability to evaluate the quality, accuracy and relevance of information on the internet.

Contact

- Inappropriate communication/contact with others, including strangers.
- The risk of being subject to grooming by those whom they make contact with on the internet.
- Cyber bullying.
- Unauthorised access to/loss of/sharing of personal information.

Conduct

- The potential for excessive use which may impact on the social and emotional development and learning of the young person.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The sharing/distribution of personal images without an individual's consent or knowledge.

As with all other risks, it is impossible to eliminate these risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. In Carniny Primary School we understand the responsibility to educate our pupils in E-Safety issues. We aim to teach appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the Internet and related technologies in, and beyond, the classroom.

3. Roles and Responsibilities

As E-Safety relates closely to Child Protection within the School, the designated Child Protection team have ultimate responsibility in ensuring that the policy and practices are embedded and monitored. The Principal/ICT Coordinator will ensure that Senior Management and Board of Governors are informed of relevant E-Safety issues in relation to the school.

It is the role of the ICT Coordinator to lead and monitor the implementation of the E-Safety policy throughout the school. Teaching staff are responsible for ensuring that E-Safety issues are embedded in all aspects of the curriculum and other school activities.

4. Staff Development

All staff will receive regular information and training on E-Safety issues from the ICT Coordinator.
New staff members will receive a copy of the E-Safety Policy and Acceptable Use Policy and sign an Acceptable Use Agreement.
All staff will incorporate E-Safety into their activities and promote awareness in their lessons.

5. Dealing with E-Safety issues

Issues of Internet misuse and access to any inappropriate material by any user should be reported to the ICT Coordinator and recorded in the E-Safety incident log book. Issues of a Child Protection nature will be reported to the designated teacher and dealt with according to the school's Child Protection Policy. Incidents of pupil misuse will be dealt with in accordance with the school's Positive Behaviour Policy. Incidents of staff misuse will be referred to the Principal.

6. E-Safety and Pupils

Pupils will use the school ICT system in accordance with the Pupil Acceptable Use Policy. This policy will be discussed with them at the start of each school year as a set of rules that keep everyone safe online. Rules for using Computers/iPads (Appendix 1a and 1b) will be displayed in all classrooms and the ICT suite, along with 'SMART' tips for staying safe online (Appendix 2). These will be discussed with the pupils at the start of each school year.
Pupils will take part in an E-Safety Awareness Day once a year. They will be informed that all internet use is filtered and monitored.

7. E-Safety and Parents/Guardians

Parents/Guardians play a crucial role in ensuring that their children understand the need to use the internet in an appropriate way and support the E-Safety Policy outlined by the school. They will be required to read the Acceptable Use Policy for Pupils and sign the agreement following discussion with their child at the start of each school year. The E-Safety Policy will be available for all parents/guardians on the school website. Carniny Primary School will endeavour to promote E-Safety in the school community by holding parents' evenings and/or sending home relevant E-Safety leaflets produced by reputable sources.

8. E-safety and Staff

All staff will have an up-to-date awareness of E-Safety matters and of the current E-Safety Policy and practices. They will have read, understood and signed the school's Staff

Acceptable Use Policy. Staff will be made aware that Internet and email is monitored and tracked by the c2k system

9. Networks within school

Pupil and staff access to the internet, on desktop and laptop computers, is through a filtered service provided by c2k. School owned iPads use the Classnet filtering system.
These filtering systems provide an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering systems cannot, however, provide a 100% guarantee that they will do so, because the content on the web changes dynamically and new technologies are constantly being developed. Neither the school, nor c2k, can accept liability under such circumstances.

School owned iPads use the Classnet filtering system.

Permission is sought from parents before pupils access the internet.

10. Digital and video images of children

Written permission is sought from parents/guardians to cover the use of photographs of pupils on the school website, in the local press and for displays etc. within school.

(a) School Website

The school website promotes and provides up-to-date information about the school, as well as providing an opportunity for pupils to showcase their work and other aspects of school life. In order to minimise the risk of any images of pupils on the school website being used inappropriately the following steps are taken:

- Group photos are used where possible with general labels/captions and pupil names are not included.
- The website does not include home addresses, telephone numbers, personal e-mails or any other personal information about pupils or staff.

(b) Storage of images

Digital and video images of children are, where possible, taken with school equipment. Images are stored on the school network or school iPads and accessible only by staff and pupils when they are required for a lesson.

11. Mobile phones

Carniny Primary School does not allow the use of mobile phones by children in school or on school trips. Mobile phones can be brought to school but must be switched off while the children are in school. Staff should not use mobile phones during designated teaching sessions.

12. Social Media

The school c2k system will block access to social networking sites so pupils will not have access to these in school. Pupils and parents will be advised that the use of social networking sites outside school is inappropriate for primary school aged children. However, Carniny Primary School acknowledges that some pupils may still use them. They will be advised to use the SMART principles (Appendix 1) when using these sites. It is suggested that they set and maintain profiles on such sites to maximum privacy settings and deny access to unknown individuals.

School staff will not 'add' or 'accept' pupils as 'friends' on any social networking site.

Please see related policy 'Social Media Policy'.

This E-Safety Policy has been developed by the ICT Coordinator and agreed by Staff and the Board of Governors. It will be available from the School Office and for viewing on the school website. The E-Safety Policy will be reviewed annually.

Appendix 1a

P1 – P3 Computer/iPad rules

- We only use the Internet when the teacher allows us.
- We only visit the web page we are told to visit.
- We always ask for help if we get lost on the Internet.
- We only use the program we are told to use.
- We ask a teacher before printing anything.

Appendix 1b

P4 – P7 Computer/iPad rules

- We ask permission before using the Internet.
- We only use websites that an adult has chosen, unless we are asked to do an independent search.
- We tell an adult if we see anything we are uncomfortable with.
- We never give out personal information or passwords online.
- We do not use Internet chat rooms or social networking sites in school.

Childnet International
www.childnet.com
THINK U KNOW

Be smart on the internet

S — SAFE Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

M — MEETING Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

A — ACCEPTING Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R — RELIABLE Information you find on the internet may not be true, or someone online may be lying about who they are.

T — TELL Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

KidSMART

www.kidsmart.org.uk

Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.