

# Camphill Primary School



## E-Safety Policy

May 2018

## **Context**

This policy is based on and complies with DENI Circular 2007/1 on Acceptable Use of the Internet and Digital Technologies in Schools and DENI Circular 2011/22 on Internet Safety.

The above circulars state that:

"Used well, digital technologies are powerful, worthwhile educational tools; technical safeguards can partly protect users, but education in safe, effective practices is a key goal for schools."

This document sets out the policy and practices for E-Safety - the safe and effective use of the Internet and related technologies in Camphill Primary School.

## **Care and responsibility**

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. With these opportunities we also have to recognise the risks associated with the internet and related technologies. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school.

Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to / loss of / sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The sharing / distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication / contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video / internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the Internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate the risk 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 any scenarios which may arise. In Camphill Primary School we understand the responsibility to educate our pupils in E-Safety issues. We aim to teach pupils 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 context of the classroom.

"Schools have the responsibility to ensure that there is a reduced risk of pupils accessing harmful and inappropriate digital content and should be energetic in teaching pupils how to act responsibly and keep themselves safe." DENI Safeguarding and Child Protection in Schools - A Guide for Schools, 2017.

(For further Information please see the above file.)

### **Roles and Responsibilities**

As E-Safety is an important aspect of Child Protection within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the ICT Co-ordinator to keep abreast of current E-Safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The ICT Co-ordinator has responsibility for leading and monitoring the implementation of E-Safety throughout the school. The Principal/ICT Co-ordinator have the responsibility to update Senior Management and Governors with regard to E-Safety and all governors should have an understanding of the issues relevant to our school in relation to local and national guidelines and advice.

### **E-Safety Skills Development for Staff**

- All staff will receive regular information and training on E-Safety issues through the Co-ordinator at staff meetings.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community.
- New staff members will receive a copy of the E-Safety policy and Acceptable Use Agreement and sign an Acceptable Use Agreement.
- All staff are encouraged to incorporate E-Safety into their activities and promote awareness within their lessons.

## **Handling of E-Safety Issues**

Issues of Internet misuse and access to any inappropriate material by any user should be reported to the ICT Co-ordinator to be recorded in the E-Safety log. Issues of a child protection nature will be reported to the designated teacher and dealt with in accordance with the Camphill Primary School Child Protection Policy. Incidents of pupil misuse of technology which arise will be dealt with in accordance with the school's Positive Behaviour Policy.

## **E-safety and pupils**

E-safety will be discussed with pupils when they receive their Acceptable Use Agreement. This should be discussed as a set of rules that will keep everyone safe when using technology in school. Activities throughout the school year including Internet Awareness Day will refresh E-Safety and further pupils' understanding. Pupils will be informed that all network and Internet use is monitored.

## **E-Safety and Parents**

The Camphill Primary School E-Safety policy will be published on the school website and parents will be encouraged to read the document. Parents will be required to read the Acceptable Use Agreement for pupils and sign this agreement following discussion with their child. Camphill Primary School will look to promote E-Safety awareness within the school community which may take the form of parents' information evenings, information leaflets or links on the school website.

## **E-Safety and Staff**

All staff will be introduced to the E-Safety policy and its importance explained. Staff will be asked to read and sign the Acceptable Use Agreement for Staff which focuses on E-Safety responsibilities in accordance with the Code of Conduct for employees. Staff should be aware that all Internet traffic and email is monitored, recorded and tracked by the c2k system.

"Staff must exercise caution when using information technology and be aware of the risks to themselves and others. Regard should be given to the school's E-Safety and ICT Acceptable Use Policy at all times both inside and outside of work." DENI Safeguarding and Child Protection in Schools - A Guide for Schools, 2017.

## **The Internet**

The Internet is a unique and exciting resource. It brings the world into the classroom by giving children access to a global network of educational resources. There is no doubt that the use of the Internet is an essential skill for children as they grow up in the modern world. The Internet is, however, an open

communications' channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restriction. This brings young people into contact with people from all sectors of society and with a wide variety of materials, some of which could be unsuitable.

## **Networks**

Pupil access to the Internet is through a filtered service provided by c2k, which should ensure educational use made of the resources is safe and secure, protecting users and systems from abuse. Parental permission is sought from parents before pupils access the Internet.

School owned iPads are connected to the internet via the MERU wifi system provided by c2k and subject to the same filters as the PCs and laptops within school.

## **Teaching and Learning**

### **Internet use**

- The school will plan and provide opportunities within a range of curriculum areas to teach E-Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school will be discussed with pupils through Internet Awareness Day.
- Pupils will be made aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils will also be aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/guardian, teacher/trusted member of staff.
- The school Internet access is filtered through the c2k managed service.
- No filtering service is 100% effective; therefore all children's use of the internet is supervised by an adult.
- Use of the internet is a planned activity. Aimless surfing is not encouraged. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge, location, retrieval and evaluation.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Children will be taught to be 'Internet Wise'. They will be made aware of Internet Safety Rules and encouraged to discuss how to cope if they come across inappropriate material.

## **E-mail**

- Pupils may only use c2k e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- The forwarding of chain mail is not permitted.
- Children will not always be given individual e-mail addresses. In some instances children may have access to a group e-mail address to communicate with other children as part of a particular project. Messages sent and received in this way will be supervised by the teacher.

## **School Website**

The Camphill Primary School website promotes and provides up to date information about the school, as well as giving pupils an opportunity to showcase their work and other aspects of school life.

In order to minimise risks 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.
- At times photographs may be used alongside the child's first name, with Parental permission.
- The website does not include home addresses, telephone numbers, personal e-mails or any other personal information about pupils or staff.

## **Social Networking**

- The school c2k system will block access to social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of cyber-bullying to the school.
- School staff will not add children as 'friends' if they use these sites.

## **Password Security**

- Adult users are provided with an individual login username and password, which they are encouraged to change periodically. Login details should not be shared with pupils.
- All pupils are provided with an individual login username and password.
- Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.
- Staff Areas/Folders are the individual responsibility of each teacher to ensure they protect the security and confidentiality of the school network.

## **Mobile Phones**

Camphill Primary School does not allow the use of mobile phones by children in school or on school trips.

It is important to be aware of the safety issues regarding mobile phones which now increasingly have Internet access. Staff use of mobile phones, only when necessary, should be discreet. Mobile phones should not be used in the classroom setting and should not be visible to pupils throughout school.

This Policy was updated in May 2018.

Related Policies:

\*Acceptable Use of Mobile Phones and Related Technologies

\*Acceptable Use of the Internet and Digital Technologies

\*Child Protection

\*Positive Behaviour