



# E-SAFETY POLICY

**Related Documents:**

Safeguarding Children Policy  
Anti-Bullying Policy  
Data Protection Policy  
Behaviour Policy and Discipline Procedures

Date: 13<sup>th</sup> June 2011

Date for Review: November 2013

### **Purpose of E-Safety**

Canterbury Steiner School's E-Safety policy has been developed with the aim of maximising the significant educational benefits of the internet whilst minimising the associated risks.

The purpose of this E-Safety Policy is to enable the School to create a safe e-learning environment that:

- promotes the teaching of ICT within the curriculum
- ensures the school fulfils its duty of care to pupils
- provides clear expectations for staff and pupils on acceptable use of the internet

### **Educational Benefits of the Internet and ICT**

Despite the potential dangers of the internet for pupils, these inherent risks are not used by School teachers to reduce children's use of ICT. The School encourages its staff to make use of ICT for lessons and project work. ICT can make a significant contribution to children's education and social development by:

- raising educational attainment, engaging and motivating pupils to learn and improving their confidence
- improving pupil's research and writing skills
- allowing children with disabilities to overcome communications barriers
- improving a pupil's wellbeing through the social and communications opportunities offered
- providing access to a wide range of educational materials and teaching resources.

## The Risks

The risk associated with use of ICT by children can be grouped into 4 categories.

<b>CONTENT</b>	Exposure to inappropriate images, pornography, information advocating violence, racism or illegal and anti-social behaviour that cannot be evaluated in a critical manner.
<b>CONTACT</b>	Chat rooms, social networking sites, adults seeking to gain the trust of young people (“grooming”) with a view to sexually abusing them. Risk of cyber-bullying, disclosing personal information (addresses, mobile numbers etc)
<b>COMMERCE</b>	Vulnerability to unregulated commercial activity, potentially serious financial consequences for themselves and parents, vulnerability to fraud or identity theft.
<b>CULTURE</b>	Involvement in inappropriate, anti-social or illegal activities, exposure to unsuitable materials or inappropriate social networks, using information in a way which breaches copyright laws.

## Computer / Internet Addiction

Children are prone to computer addiction which can have a negative impact on their health, social, emotional development and their educational attainment. Studies have established recurring links between computer addiction and depression. It disrupts sleeping patterns, takes away from time spent outdoors and being generally physically active. For young children in particular this can lead to significant developmental issues. School ICT lessons commence in Class 9.

**See Appendix 1 for a useful summary of the many benefits and associated risks of ICT (pp. 8-9)**

## Elements of E-Safety

### Safe Systems

The suppliers of the hardware and software of the School's computer network provide on-going technical support and advice to help maintain E-Safety. This includes:

- An effective firewall
- Anti-virus software
- Username and password protected areas for individual pupils and staff
- Filtering software for search engines and browsers to protect pupils and staff
- A technical support line for instant response to technical issues

### Safe practices

Only Classes 9, 10 and 11 are offered access to the internet. It is School policy for parents/guardians to complete the Internet Parent Permission Form before pupils can use the internet at the School.

See Appendix 2 for comprehensive guidelines and the Code of Conduct.

## Policy Implementation

### Roles and Responsibilities

#### 1) E-Safety Officer

The **Upper School Chair** takes on the role of **E-Safety officer**, providing a central point of contact for E-Safety issues who can then co-ordinate and update policy as appropriate.

E-Safety officer responsibilities:

- providing the first point of contact and advice for school staff, governors, pupils and parents.
- liaising with the school's IT supplier to ensure they are kept up to date with E-Safety issues and to advise of any new trends, incidents and arising problems to the College and Administrator.

- raise the profile of E-Safety awareness with the school by ensuring access to training and relevant E-Safety literature when appropriate.
- maintain a file of internet related incidents and co-ordinate any investigation into breaches. All incidents must be recorded using an E-Safety incident form and filed in the E-Safety folder in the School office.
- assess, as far as is reasonably practicable, the impact and risk of emerging technology (eg. a new social networking website).

Staff should familiarise themselves with Appendix 1 (see end of document). It is a useful summary of the many benefits and risks of ICT (emailing, social networking, browsing etc).

## Responding to Incidents

- All incidents, whether involving pupils or staff, must be recorded in the E-Safety incident file using an incident form.
- The E-Safety officer should periodically review the E-Safety incident file for evidence of emerging patterns of individual behaviour or weaknesses in the school's E-Safety system. This information should be used to update the E-Safety policy.
- E-Safety incidents involving safeguarding issues should be reported to the appropriate Child Protection Officer (CPO), who will make a decision as to whether or not to refer the matter to the police or the child protection local authority (LA).

The E-Safety Policy seeks to reduce risks but it cannot eradicate online risk entirely. The School cannot accept liability for material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment and to keep online security up to date.

## **Unintentional access of inappropriate websites**

- Teachers should reassure pupils that they have done nothing wrong and discuss the incident with the class to reinforce the E-Safety message.
- The incident should be reported to the E-Safety contact officer and details of the website address and URL provided.
- The E-Safety contact officer should liaise with the IT manager to ensure that access to the site is blocked and the school's filtering system updated.

## **Intentional access of inappropriate websites by a pupil**

- If a pupil deliberately accesses inappropriate or banned websites, they will be in breach of the acceptable use policy and subject to appropriate sanctions (see Behaviour Policy and Discipline Procedures).
- The incident should be reported to the E-Safety contact officer and details of the website address and URL recorded.
- The E-Safety contact officer should liaise with the School network manager to ensure that access to the site is blocked.
- If appropriate, the pupil's parents should be notified of the incident.

## **Inappropriate use of ICT by staff**

- If a member of staff witnesses misuse of ICT by a colleague, they should report this to the E-Safety officer and the Administrator immediately.
- The E-Safety contact officer should notify the network manager so that the computer or laptop is taken out of use and securely stored in order to preserve any evidence. A note of any action taken should be recorded on the E-Safety incident report form.
- The E-Safety contact officer should arrange with the network manager or School's IT team to carry out an audit of use to establish which user is responsible and the details of accessed materials.

- Once the facts are established, the College Chair and Administrator should take any necessary disciplinary action against the staff member and report the matter to the school governors and the police where appropriate.
- If the materials viewed are illegal in nature the College Chair and Administrator should report the incident to the police and follow their advice, which should also be recorded on the E-Safety incident report form.

## **Laptops and Mobile Phones**

It is against School policy for pupils to use mobiles in School (see Dress and Appearance Policy). In terms of E-Safety, most modern mobiles ('Smartphones') have internet connectivity which would give unregulated private internet access only to certain pupils. If a mobile is heard or any pupil is seen using a mobile anywhere on the School site it will be confiscated for the remainder of the day and possibly longer depending on the nature of the incident.

For the same reason, unless a pupil has obtained special permission to bring in their laptop for School work, any laptops found being used at School will also be confiscated.

Pupils posting images, comments, sound recordings, videos or any other material pertaining to any staff member, trustee, pupil, parent or anyone with a connection to the School on websites, YouTube, Facebook or any other social networking sites will be dealt with under the exclusion policy.

## **E-Communication between Staff and Pupils**

- Staff must not email pupils from private email accounts. Only School email accounts should be used. Emailing between staff and pupils should only be for assistance with school work.
- Texting between staff and pupils is not allowed except in an emergency situation on a class trip.
- It is against School policy for staff Facebook users to add current pupils as friends or accept friendship requests from pupils.
- Staff found to contravene the E-Communication guidelines could face a disciplinary hearing.

## Appendix 1: Description of ICT Applications (Benefits & Risks)

Technology/ Application	Description/ Usage	Benefits	Risks
<b>Internet</b>	<ul style="list-style-type: none"> <li>• Enables the storage, publication and retrieval of a vast range of information</li> <li>• Supports communications systems</li> </ul>	<ul style="list-style-type: none"> <li>• Provides access to a wide range of educational materials, information and resources to support learning</li> <li>• Enables pupils and staff to communicate widely with others</li> <li>• Enhances schools management information and business administration systems.</li> </ul>	<ul style="list-style-type: none"> <li>• Information is predominantly for an adult audience and may be unsuitable for children</li> <li>• The vast array of information makes retrieval difficult without good research skills and ability to critically evaluate information</li> <li>• Access to sites promoting illegal or anti-social activities, extreme views or commercial and gambling sites.</li> </ul>
<b>Email</b>	<ul style="list-style-type: none"> <li>• Allows written communications over the network and the ability to attach documents.</li> </ul>	<ul style="list-style-type: none"> <li>• Enables exchange of information and ideas and supports collaborative working.</li> <li>• Enhances written communications skills</li> <li>• A good form of communication for children with some disabilities.</li> </ul>	<ul style="list-style-type: none"> <li>• Difficulties controlling contacts and content</li> <li>• Use as a platform for bullying and harassment</li> <li>• Risks from unwanted spam mail, particularly for fraudulent purposes or to introduce viruses to systems</li> <li>• Hacking</li> <li>• Unsolicited mail.</li> </ul>
<b>Chat/instant messaging</b>	<ul style="list-style-type: none"> <li>• Chat rooms allow users to chat on-line in real time in virtual meeting places with a number of people;</li> <li>• Instant messaging allows real-time chat for 2 people privately with no-one else able to join. Users have control over who they contact through “buddy lists”.</li> </ul>	<ul style="list-style-type: none"> <li>• Enhances social development by allowing children to exchange experiences and ideas and form friendships with peers.</li> <li>• Use of pseudonyms protects the child’s identity.</li> <li>• Moderated chat rooms can offer some protection to children.</li> </ul>	<ul style="list-style-type: none"> <li>• Anonymity means that children are not aware of who they are really talking to.</li> <li>• Chat rooms may be used by predatory adults to contact, groom and abuse children on-line.</li> <li>• Risk of children giving away personal information that may identify or locate them.</li> <li>• May be used as a platform to bully.</li> </ul>

<b>Social networking sites</b>	<ul style="list-style-type: none"> <li>• On-line communities, including blogs and podcasts, where users can share text, photos and music with others by posting items onto the site and through messaging.</li> <li>• It allows creation of individual profiles.</li> <li>• Users can develop friends lists to allow access to individual profiles and invite comment.</li> </ul>	<ul style="list-style-type: none"> <li>• Allows children to network with peers and join forums to exchange ideas and resources.</li> <li>• It provides a creative outlet and improves ICT skills.</li> </ul>	<ul style="list-style-type: none"> <li>• Open access means children are at risk of unsuitable contact.</li> <li>• Risk of children posting unsuitable material on-line that may be manipulated to cause them embarrassment or distress.</li> <li>• Children may post personal information that allows them to be contacted or located.</li> <li>• May be used as a platform to bully or harass.</li> </ul>
<b>File sharing (peer-to-peer networking)</b>	<ul style="list-style-type: none"> <li>• Allows users to share computer capability, networks and file storage.</li> <li>• Used to share music, video and other materials.</li> </ul>	<ul style="list-style-type: none"> <li>• Allows children to network within a community of peers with similar interests and exchange materials.</li> </ul>	<ul style="list-style-type: none"> <li>• Illegal download and copyright infringement.</li> <li>• Exposure to unsuitable or illegal materials.</li> <li>• Computers are vulnerable to viruses and hacking.</li> </ul>
<b>Mobile phones and multi-media equipment</b>	<ul style="list-style-type: none"> <li>• Mobile phones now carry other functions such as cameras, video-messaging and access to internet and email.</li> </ul>	<ul style="list-style-type: none"> <li>• Provide children with a good means of communication and entertainment.</li> <li>• They can also keep children safe and allow them to be contacted or stay in contact.</li> </ul>	<ul style="list-style-type: none"> <li>• Their mobile nature makes supervision of use difficult leading to risks of unsuitable contacts or exposure to unsuitable material on the internet or through messaging.</li> <li>• Risk from violent crime due to theft.</li> <li>• Risk of cyberbullying via mobile phones.</li> </ul>

## Appendix 2: ICT Code of Conduct for Pupils

### ICT Code of Conduct for Pupils (Also recommended for use outside school)

#### Pupil Guidelines

- Pupils are expected to behave responsibly when using the school's ICT facilities, including the internet, just as they are expected to do so in a classroom or other school area. General school rules apply.
- The ICT facilities are expensive and must be treated with great care.
- Pupils should not expect files stored on servers to be private. Staff may review files and communications to ensure that pupils are using the system responsibly.
- The internet is provided for educational purposes so that:
  - Pupils can enhance their learning and research skills
  - Pupils with disabilities can overcome educational difficulties
  - Pupils can gain basic fluency and confidence when using the internet
- Access is a privilege, not a right – and can be rescinded.
- Individual users of the internet are responsible for their behaviour and communication over the network

The following are not permitted:

- Disclosing your assigned network password to other pupils or to anyone else.
- Using other pupils' network passwords.
- Trespassing in other pupils' folders, work or files.
- Violating copyright laws, especially the illegal copying of software.
- Intentionally wasting limited resources, such as server processing time, ink and paper.
- Sending or displaying offensive messages or pictures.
- Sending junk mail.
- Revealing your photograph, phone number or other personal details on web pages or in emails without written parental and school permission.
- The use of the internet to buy, sell or advertise.
- The participation in chat rooms or newsgroups except where these are educational and supervised by a member of staff.
- Post to / read sites such as Twitter, Facebook, blogs, etc during school hours.
- Subscribe to internet mailing lists without specific permission from the supervising ICT teacher in each case.