Carleton Community High School - IT DEPARTMENT

COMPUTER AND PERSONAL INTERNET SECURITY & SAFETY

Principle

We must put measures into place now in order to prevent computer misuse - only then will we feel confident that we have taken all reasonable steps to protect ourselves and the children in our charge.

SECTION A. Virus Introduction And Copyright Breaches

A list of all software purchased by the School under site-licences is kept separately by the I.T. Co-ordinator. The School Policy is that only software purchased by the School is allowed to be used on school premises. Pupils are not allowed to bring private software disks, memory sticks or programmes downloaded from the cloud, into school and, in particular, 'arcade' games software is banned. This policy is designed not only to ensure that the School is not in breach of copyright laws but also to reduce the risk of viruses being introduced into school computer systems. Pupils are encouraged to provide their own 'work disks' but these must not be used to store software which is subject to copyright restrictions.

Staff action:

1. Pupils who are found to be in breach of this policy should have their disks confiscated.
2. Confiscated disks should be forwarded to the I.T. Co-ordinator who will eliminate any viruses and also check to see if a breach of copyright has been made. In such cases, the I.T. Co-ordinator will forward a report to senior management who will decide on appropriate action to be taken.
3. Virus protection software should be installed on all hard disks and cloud servers. This software should be updated at frequent intervals to deal with new strains of viruses as they appear.

SECTION B. Unauthorised Access

Internal Systems

A great deal of information of a personal, confidential and sensitive nature is stored in school computer systems, either on floppy disk or hard disk. Such data is subject to the Data Protection Act and precautions must be taken to protect it from unauthorised access. The following actions are recommended:

1. Set access to files so as to limit access to the owner of the file only.
2. Use a password system in order to restrict access to authorised personnel only. N.B. a dedicated hacker can break down a password within 24 hours, so passwords should be changed regularly.
3. When memory sticks which contain confidential data are not in use, they should be locked in a safe or a secure area.
4. Some computer systems incorporate a physical locking device for the hard disk. If a hard disk is used to store confidential data, it should preferably be physically locked or if this is not possible, the computer containing it should be locked in a secure area.

External systems

Hackers can gain access to data contained within any computer system which is connected to a telephone line via a modem or to a local area network (LAN). We have both a need to protect our data from unauthorised access (internal & external) and a duty to prevent our pupils from 'hacking' into external computer systems when using school computers via analogue or digital telephone systems using modems or ISDN connections. The following actions are recommended in addition to those listed previously:

1. Pupils should not be allowed to access the Internet or any other external communications system unless they are supervised by a member of staff.

2. Logging-in passwords and codes for the Internet and other communications channels should not be divulged to pupils and these should be securely locked away when not in use.
3. Initial logging-in procedures for the Internet should be carried out by the supervising teacher and not by the pupils themselves.

SECTION C. Protecting Pupils From 'On-line' risks

Teachers and other employees in charge of pupils have a common law duty to act as any reasonably prudent parent would to ensure the Health and Safety of pupils whilst they are in their charge. The School has written Health and Safety policies, perform risk assessments and inform staff about any measures intended to control these risks.
There is naturally concern about all forms of computer misuse but the greatest specific threats to children's well being is from contact with undesirable characters, computer pornography and anarchic views. Since we have a duty of care, we must obviously take steps to counter these threats. It is an offence, under the Obscene Publications Acts, to publish an obscene article and since computer disks and CD ROM's contain information which can be displayed in words and pictures, they are therefore articles in the spirit of the law. Furthermore, under the terms of the Children Act 1978, it is an offence to possess pornography which involves children under the age of 16.

There are two obvious ways by which computer pornography can be brought into the School. It could be downloaded from the Internet or any other external communications system or it could simply be carried into the School on floppy disks or CD ROM's.
In order to protect our pupils from the dangers of such pornography, the following actions are recommended.

1. As in Section A, pupils should not bring CD ROM's memory sticks or data pens into school.
2. Pupils should not be allowed to use computers unless properly supervised.
3. Access to external social media, forums, video and picture sharing sites is forbidden.
4. As in the preceding paragraph, no pupil should be allowed to access the Internet or any other external communications channel unless under direct supervision, and they should not have access to logging-in codes and procedures.
5. The School should only allow access to the Internet through approved 'service providers' who provide a 'walled-garden' service to ensure that all unsuitable material is filtered out.
6. This filter system is updated daily with details of new and suspicious sites.