Pool House CP School
Computer System Integrity Policy

Virus Introduction And Copyright Breaches.

At Pool House a list of all software purchased by the School under site-licences is kept separately by the I.C.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 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.

Staff action:

1. Pupils who are found to be in breach of this policy will have their disks confiscated.
2. Confiscated disks will be given to the I.C.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.C.T. Co-ordinator will forward a report to the Head teacher who will decide on appropriate action to be taken.
3. Virus protection software should be installed on all hard disks and floppy disks to reduce the risk of infection. This software should be updated at frequent intervals to deal with new strains of viruses as they appear.

Unauthorised Access

Internal Systems

A great deal of information of a personal, confidential and sensitive nature is stored in school computer systems, either on software 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 daily.
3. When software that contains confidential data is not in use, it 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. N.B. This is not necessary when accessing the NGFL.
3. Initial logging-in procedures for the Internet should be carried out by the supervising teacher and not by the pupils themselves.

4. External modems should be securely locked away and ISDN routers switched off when not in use.
5. All external communications activity should be logged on a telephone record sheet.
6. The school should use a 'firewall' to protect its own internal data and programmes.

Summer 2021