INTERNET SECURITY POLICY

PERSONAL INTERNET SECURITY

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.

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. Schools must also have 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 digital devices 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 digital devices.
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 and USB drives (except work disks) to school.
2. Pupils should not be allowed to use computers unless properly supervised.
3. Work disks should be inspected at random. In particular, large graphics files (which could contain pornographic pictures) should be inspected.
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. As in the previous paragraph, external modems should be locked away when not in use and ISDN routers switched off.

THE BENEFITS OF THE INTERNET

The Internet is sometimes referred to as the 'information super highway' and it is now the largest depository of human knowledge and has massive educational implications. Nearly any transaction such as shopping, banking, booking holidays, making flight reservations or trading stocks and shares can be conducted on-line and interactive competitive computer games can be played.
Most schools are now on-line and, in many homes, children are logging on to e-commerce sites, private bulletin boards, and the general Internet. Parents need to understand the nature of these systems.

THE NATURE OF THE RISK:

The Internet is sometimes referred to as the 'on-line society' or the 'information highway', and like all societies it is made up of all sorts of characters – most will be trustworthy but some will not. Young people therefore need parental supervision and common sense advice on how to safely go on-line. Problems are relatively infrequent but we need to equip young people with the skills to protect themselves and others when on-line. Computer Bulletin Board Services (BBS) can be operated by individuals, groups, associations or businesses. A substantial number of BBS feature 'adult' material and most, but not all, attempt to limit access to adults only. Internet Service Providers (ISPs) are commercial, self-regulated businesses that provide access to the Internet.
The Internet is not governed by any entity and the definition of the age of an adult varies between countries - indeed there may be no distinction or effective child protection laws. This leaves no effective limits or checks on the kind of information that is maintained by and accessible to Internet users and therefore children may be exposed to inappropriate material of a sexual, racist or violent nature.
Teenagers are particularly at risk because they often use the computer unsupervised and because they are more likely than younger children to participate in on-line discussions regarding companionship, relationships, or sexual activity. Some risks associated with pupils' use of the Internet and e-mail are:

1. **Exposure to Inappropriate Material**
   The Internet makes it very easy to access sexually explicit, pornographic and anarchic material.
   Categories of inappropriate material which are often used by security programmes are:
   Partial Nudity; Nudity; Sexual Acts/Text; Gross Depictions; Intolerance (Racial/Ethnic); Satanic or Cult; Drugs and Drug Culture; Militant/Extremist; Violence/Profanity; Questionable/Illegal; Gambling; Sex Education and Alcohol & Tobacco.

2. **On-line Financial Transactions**
   Anyone with access to a credit card (including a child who has taken his/her parents card) can purchase goods and services on-line – therefore keep your cards as safe at home as when away from home!
3. **Physical Molestation**
   Another risk is that, while on-line, a child might provide information or arrange an encounter that could risk his or her safety or the safety of other family members. In a few cases, paedophiles have used on-line services and bulletin boards to gain a child's confidence and then arrange a face-to-face meeting.
4. **Unwanted Interactions or Harassment**
   A third risk is that a child might encounter E-mail or bulletin board messages that are harassing, demeaning, or belligerent. Pupils and teachers can also be targeted with racist e-mails.
5. **Falsification or Illegal use**
   E-mail messages can be created by pupils which falsely purport to come from a third party. Pupils can also use the School's system to run an e-commerce business or to hack in to other computer systems.
6. **Breaches of system security**
   Unauthorised access or failure to follow security protocols can allow electronic viruses to enter the School's computer systems.
7. **Burglary**
   Disclosure of your daily routines or arranging face to face meetings can give opportunities for your home to be burgled.

<u>WHAT CAN PARENTS DO TO REDUCE THE RISKS</u>

ISPs and some private BBS have systems in place for parents to block out parts of the service they feel are inappropriate for their children. ISPs mostly provide high quality editorial control of the material contained on their systems and parental controls for editing and censoring the material 'visible' on their systems. If parents wish to utilise or find out about any available parental controls then they should contact the particular ISP to find out how the control systems can be applied.

The Internet and some private bulletin boards contain areas designed specifically for adults who wish to post, view, or read sexually explicit, racist or anarchic material. Like all safeguards, be aware that there will always be cases where individuals, groups or organisations fail to enforce them or where children find ways around them.

Children need parental supervision and common-sense advice in order that their experiences whilst on-line are happy, healthy, and productive. Children need to conduct independent actions in order to develop, however, they still need parental involvement and supervision (direct and indirect) in their daily lives if security is to be maintained. Therefore, the same general parenting skills that apply to the "real world" also apply while on-line.

Rules For Parents

- Stay in touch with what your children are doing by spending time with them whilst they are on-line, i.e. make on-line time a family activity;
- Make sure that you know the services your child uses. Find out what types of information and services are offered and whether there are ways for parents to protect their child.
- Keep the computer in a family room rather than a child's bedroom.
- Learn yourself about how to access the services - ask your child to explain the services to you;
- Go on-line yourself so that you are familiar with and understand the potential benefits and risks associated with Internet access. If you don't know how to log on, get your child to show you.
- Seek out the advice and counsel of other local Internet users and become familiar with the appropriate systems;
- Get to know your child's 'on-line friends' just as you do their other friends.
- If you are concerned about your child's on-line activities, talk to him/her about it;
- Develop an agreed set of 'Family Internet Rules' - see later for an exemplar;
- Make sure that your child is familiar with, and adheres to, your 'Family Internet Rules';
- Post your 'Family Internet Rules' near the computer as a reminder.
- Monitor your child's compliance with these rules;
- Should you become aware of the presence of child pornography on-line report this immediately to the National Society for the Prevention of Cruelty to Children on Phone: 0800 800 500.

Family Internet Rules:

1. Always keep to the agreed times of day to be on-line, the length of time to be on-line, and the areas that you can visit.
2. Never give any passwords to anyone outside your family – even friends!
3. Always tell a parent about any threatening or bad language you see on-line.
4. Never give out any of the following information during a 'chat' session or when in a BBS:
   - Your real name (use a pseudonym – a false name);
   - Your parents or brothers'/sisters' real names (use pseudonyms – false names)
   - Home address;
   - Home telephone number;
   - Parents' work address/telephone number;
   - The name, address or location of your school.
5. Never send an on-line person any photographs or anything else without first checking with a parent.
6. Never arrange for someone you meet on-line to visit your house.
7. Never arrange a face-to-face meeting with another computer user without your parents permission. If a meeting is to be arranged let your parents arrange this for you. The first meeting should be in a public place and at least one parent should accompany you. Your house should remain occupied during the meeting to prevent burglary.
8. Never respond to messages or BBS items that are suggestive, obscene, threatening or that make you feel uncomfortable. If you encounter such messages then tell a parent immediately.
9. Remember that what you read on-line is not necessarily true, e.g. the person who says she is a 15 old girl could in fact be a middle aged man.
10. Make sure that you're dealing with someone you trust.
11. Never try and order something on-line unless you are over 18 years old.

SELECTING AN ON-LINE SECURITY PROGRAMME

Programmes are now available for domestic and school computer systems, such as Cyber Patrol, McAfee and Norton Internet Security, which provide facilities for setting and monitoring Internet security. When selecting such a programme consideration should be given to its facilities. At the basic level an Internet personal security programme should:

- Feature at least two levels of parental password control;
- Restrict access to certain times of the day;
- Limit the total time spent on-line in a day;
- Be able to allow on-line access to be customised for each member of the family;

- Block access to Internet sites that are deemed inappropriate - including those sites accessed via a proxy server;
- Be pre-loaded with a listing of researched Internet sites containing questionable materials as well a listing of researched Internet sites containing suitable material for children;
- Allow parents to select the content categories they wish to block;
- Allow parents to deny access to additional sites not included on the 'questionable list';
- Have facilities for reporting cumulative use of the Internet;
- Have weekly updates on the 'questionable list' available for download;
- Control access to the major on-line services and to local applications such as games and personal financial managers;
- Be able to set on-line access according to individual interests, needs and ages;
- Provide control through Internet applications and web browsers, e.g. Internet Explorer, Safari, Firefox and Crome.
- Prevent children from disabling the programme or simply renaming blocked applications;
- Prevent children from keying in selected words, phrases or numbers while logged onto an on-line service or directly onto the Internet;
- Prevent children from sending out their names, address and phone numbers on-line; • Be easy to use!

THE SYMPTOMS OF DISTRESS AND MISUSE IN CHILDREN

If the Rules for parents and 'Family Internet Rules' are followed then what follows in this section will not be relevant. Excessive time spent on-line (especially late at night) is not good for many reasons, i.e. sleep, school work and social skills may suffer. Although the signs of child distress are well documented many of the symptoms taken in isolation can occur in situations where nothing untoward is occurring or has ever occurred. Many of these signs may also be indications of other medical, social or psychological problems or simply normal child development. Parents therefore need to be careful and thoughtful in ascertaining whether something is wrong. The large number of signs and symptoms described in this policy need to be considered in the light of normal child development, e.g. an interest in sexual topics and members of the opposite sex is to be expected in a youngster of 14, but in an 8 year old, such behaviour may well be a cause for concern. A child may show signs of stress and distress as listed below:

- a lack of concentration and a fall-off in school performance;
- aggressive or hostile behaviour;
- moodiness, depression, irritability, listlessness, fearfulness, tiredness, temper tantrums, short concentration span, acting withdrawn or crying at minor occurrences;
- difficulties in relationships with peers;
- low self esteem;

- wariness, insecurity or truancy;
- disturbed sleep;
- general personality changes such as unacceptable behaviour or severe attention seeking behaviour;
- a sudden change in school performance.

SECTION B.

The Internet Permission Form

Dear Parent,

As part of the School's I.C.T. programme we offer pupils supervised access to the Internet. However, it is government policy that, before being allowed to use the Internet, all pupils must obtain parental permission and therefore, both they and you are requested to sign and return the enclosed form as evidence of your approval and their acceptance of the school rules on this matter.

Access to the Internet will enable pupils to explore a vast source of information stored in thousands of libraries, databases, and archives throughout the world. Families should be warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

Whilst our aim for Internet use is to further educational goals and objectives, pupils may find ways to access other materials as well. We believe that the benefits to pupils from access to the Internet, in the form of information resources and opportunities for collaboration with other schools and organisations, exceed any disadvantages. Ultimately though, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the school supports and respects each family's right to decide whether or not to apply for access.

During school, teachers will guide pupils towards appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, videos, movies, radio and other potentially offensive media.

We would be grateful if you could read the enclosed guidance documents (derived from Sections A-C of this policy) and then complete the permission slip which follows.

Yours sincerely,

Head teacher

""----------

Internet Parental Permission Form
Please complete and return this form to the Head teacher.

Name of Pupil…….. **Form** …….

As a school user of the Internet, I agree to comply with the school rules on its use. I will use the network in a responsible way and observe all the restrictions explained to me by the school.

Pupil Signature ……. **Date** …./…./….

As the parent or legal guardian of the above named pupil, I grant permission for my child to use electronic mail and the Internet. I understand that pupils will be held accountable for their own actions. I also understand that some materials on the Internet may be objectionable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information and media.

Name of Parent/Guardian ……. (PLEASE PRINT IN BLOCK CAPITALS)

Parent/Guardian Signature ……. **Date** …./…./….

Compiled by:	Revision Number
Approved by:	Revision date __/__/