

## **Internet Safety for Parents**

This document has been produced to offer guidance to parent and carers in the safe use of the Internet.

### **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.

**WHAT CAN PARENTS DO TO REDUCE THE RISKS**

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.

## Advice 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 Child Exploitation and Online Exploitation at <https://www.ceop.police.uk/safety-centre> or Childline on 0800 1111

## 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 forum:
  - 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 with parental 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 Internet Guard Dog 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. Chrome, Internet Explorer, Edge or Safari.
- 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, addresses 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.

For further information please visit <http://www.vodafone.com/content/digital-parenting.html/>