5.1.17 Computers and Internet Access

Relevant Chapters

Where concerns arise with regard to a young person's E-safety this chapter must be read in conjunction with the **Child and Adult Protection Procedure** and the Local Safeguarding Partnership or Vulnerable Adults Procedures in the area where the home is located. Also see the following relevant procedure; **Photographs, Videos and other Images**, which contain guidance/procedures on the use of images from the internet.

Contents

1. Introduction

On-line technology has changed the way children live their lives in many positive ways. It has also brought with it safety issues that require knowledge and awareness among those responsible for their welfare. These procedures set out the arrangements for safely managing children's access to computers and use of the internet whilst in the care of the company or under the supervision of staff or volunteers. Key to this is engaging with parents/carers to make them aware of internet safety issues. It is also necessary to obtain parents' permission for the child to take part in any on-line activity organised or promoted by the company.

2. Safe Use of Computers and the Internet

The **Guidance for Children's Safe Access to the Internet (see Appendix A)** provides essential information about Internet safety risks and risk management.

All computers should be protected by a 'firewall' and there should be filters in place to prevent people from accessing unsuitable material or receiving inappropriate or virus infected emails. This does, however, not replace the need to talk to the child, agree ground rules and monitor their activities as there are constantly new ways unwanted material can get pass existing security systems. There will also always be people trying to gain unauthorised access to networks and PCs.

Prior to accessing computers with Internet connection, written permission should be sought from parents and carers.

Scroll down or see here for **Appendix A: Guidance For Children's Safe Access to Computers and the Internet**

Appendix A: Guidance for Children's Safe Access to Computers and the Internet

Children's use of computers and the Internet

Children's use of computers is often different from adults. Many engage in a variety of Internet activities, quickly switching from one to another as their attention moves from one or several of the following activities:

1. Research to help with homework, projects and course work;
2. Getting in touch with each other via Emails, Instant Messaging (IM), chatrooms, discussion groups or to swap files, music;
3. Playing online games; that can be downloaded from a website or they may play with others who are online (friends or strangers);
4. Listening to music; downloaded from the internet or files from friends;
5. Buying online; there are thousands of companies, organisations and individuals with something to sell;
6. Writing up project work or preparing presentations; for school or College.

Risks

The main risks of on-line activities are:

- Meeting someone online. "Luring" is the term for online behaviour that leads to these meetings and is illegal. The vast majority of reported cases are over 15 years and female;
- Loss of privacy. Disclosing name, address, telephone number to a stranger can put the child and family members in danger;
- Getting into on-line fights; communication with text, or in writing can easily escalate into emotional disputes as it is difficult to know the intensity of someone's feelings;
- File sharing/downloads; file-sharing and downloads creates a risk that viruses or other malignant code could be spread to the computer over the network. It is also possible for others to track online activities and send that information to third parties;
- On-line bullying; this is a common problem and the most common techniques are that children are harassed or harass others via text messaging, internet chat rooms and emails;
- Making threats/law breaking; this can range from being rude and obnoxious to committing crimes online. It can also include putting someone else in jeopardy by publishing names, addresses or phone numbers of someone they know;
- Inappropriate material; many websites include material that is sexual, violent or hateful, or which advocate the use of weapons or harmful substances such as alcohol, tobacco, or illegal drugs. It is possible to inadvertently come across these sites when typing an address in a web browser or when using search engines. Usually because a word is mistyped or an imprecise key word is used. Unsafe links may also appear on safe sites tempting a child to search for material that he might not otherwise come across;

- Setting up a website; it is possible for children to set up their own Web sites (at no cost). Anything posted can be seen by a**n**yone visiting the site;

- Chat; it is easy for children to forget that they are in a public place and do not necessarily know the true identity of anyone in the chat room. It is also important to be aware that what may appear to be moderated chat by adults is instead software. This looks for particular words and if the words appear a moderator is notified and checks the content. If someone in the chatroom is found to be breaking the rules usually they will first be warned and then, if they persist, they can be thrown out and barred. However someone who is barred usually needs only to create a new email address. This gives them a new internet identity and they can get back in;

- Instant Messaging (IM); similar to chat but unlike in some chat rooms, there is never anyone else there to monitor activity;

- Excessive Internet use; can lead to children neglecting homework, and outdoor or other social activities. They may also run up heavy telephone bills;

- Computer viruses; or even people hacking into the computer (someone gaining unauthorised access) can cause serious damage. Some viruses can hand over control of the computer to someone who may be far away but who can use it for their own purposes, for example send email to others. Playing online games is for example a time when the computer is particularly vulnerable to a virus.

Managing risks and promoting safe use of the Internet

Recognising the potential threats to children and young people on the internet is the first step to protecting them. It is important to become familiar with how the child uses the internet. It is also worth bearing in mind that some mobile phones and games consoles provide internet access. The following is recommended to promote the safe use of the Internet:

- **Location**; keep the computer with internet connection in the kitchen area, family room, or other areas where the child is 'independent' but not alone; any equipment which has access to IT must be used as directed in individual My Plan/Personal Plan' which covers English and Welsh homes/schools;

- **Parental control**; install filtering software, a comprehensive list is available on https://www.getnetwise.org/.

- **Internet habits**; ask the child on a regular basis to show you the places they go to on the internet and be familiar with their patterns of use and time spent online. This will help detect any changes in behaviour that may be of concern;

- **On-line relationships**; find out whom they are sending emails to and who they are receiving them from. You should know if they visit chatrooms or subscribe to newsgroups and you should understand what they do when they visit these places;

- **Website access**; It is important to have rules about the sorts of sites and materials it is acceptable for the child to access;

- **Talk about what they do online**: Having an open relationship with the child is the key to being able to discuss with them the kinds of material, people or situations they may inadvertently or deliberately come across on the internet;

- **Be open and honest**: It is vital to openly discuss with the child the possibility of them seeing or being sent sexually explicit or other worrying material. Children may otherwise feel they may have done something wrong, and perhaps be fearful of telling you in case they get into trouble and/or have sanctions applied to them. It is precisely at this stage that children can feel most isolated and vulnerable to the control of sexual or other kinds of predators;

- **Time management**; there are no hard and fast rules about what is excessive use of the Internet as it will vary from child to child, circumstances and their on-line activities. Internet use for school and College should be encouraged whilst at the same time recognising that this may also need monitoring. Some children may play on-line games, chatting or emailing each other under the pretext of doing homework;

- **Viruses and hackers**; it is essential to install Anti-virus software and to subscribe to regular upgrades as this will help minimise the risks from viruses and hackers;

- **Be cautious and careful**; children need to know that unless and until they are absolutely certain of the identity of someone they are communicating with, they should proceed with caution and not necessarily accept everything a person says online at face value;

- **Parental control software**, these can be used to:

    - Control content;

    - Control contacts;

    - Control shopping and privacy;

    - Help with time management;

    - Improve general security;

    - Monitor and record activity, including who the child sends emails to and blocking access to all or some chatrooms;

      For more information contact; Internet Content Rating Association Family Online Safety Institute

      Filtering software should, however, not replace discussions about safety issues and ground rules as children can gain access to the Internet in other places (friend's homes, internet café's etc);

- **Moderated (supervised) chatrooms**: ask about policies enforced in the chatroom, the training given and checking done on the backgrounds of the people who are employed by them as moderators. More info on staying safe in chatrooms can be found on the Home Office site **Think U Know**;

- **Keep yourself informed**; children may be exposed to risks because adults looking after them are unaware of the dangers they are confronted with. Department for Education sponsor a site to help parents keep up with internet safety issues: **Parents Centre Website**.

Appendix B: Glossary

- **Chatroom**; a place on the internet accessed through a computer or mobile phone device, where people communicate by typing messages. People all over the world can communicate in a chart room, where everyone else can see what is being typed by anyone else, either on their computer screen or mobile device;

- **Cookie**; a piece of information sent by a Web server to a user's browser. Cookies may include information such as login or registration identification, user preferences, online "shopping cart" information, etc. The browser saves the information, and sends it back to the Web server whenever the browser returns to the Web site. The Web server may use the cookie to customize the display it sends to the user, or it may keep track of the different pages within the site that the user accesses. Browsers may be configured to alert the user when a cookie is being sent, or to refuse to accept cookies. Some sites, however, cannot be accessed unless the browser accepts cookies;

- **Data Mining or Online Profiling**; the practice of compiling information about Internet users by tracking their motions through Web sites, recording the time they spend there, what links they clink on and other details that the company desires, usually for marketing purposes;

- **Discussion group/Newsgroup**; online area, like an electronic bulletin board, where users can read and add or "post" comments about a specific topic. Users can find discussion groups, also referred to as "discussion boards," for almost any topic;

- **Downloads**; transfer of information on to a computer which often is free. It can be images, games, music etc;

- **File Sharing**; Accessing files on one computer from a different computer;

- **Filtering software**; allows blocking out of certain material from the computer such as websites with violent, racist or sexual content;

- **Filtered ISP**; An Internet Service Provider (ISP) that sets criteria for determining content which is inappropriate for children, and automatically blocks subscriber access to that content;

- **Firewalls**; are used to prevent unauthorised internet users from accessing private networks or individual computers connected to the internet. All messages entering or leaving the computer pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria;

- **Flaming**; Posting or sending a deliberately confrontational message via newsgroup, e-mail, etc., usually in response to a previous message;

- **Instant Messaging (IM)**; Technology similar to that of chat rooms, which notifies a user when a friend is online, allowing them to "converse" by exchanging text messages;

- **ICQ**; downloadable internet software that alerts someone to other people being online and allows contact to them. The software lets users chat, send messages and files, exchange web addresses and play games;

- **IRC**; internet relay chat, which is another form of online chat with software that can be downloaded;

- **MMS**; Multimedia messaging service, which means sending messages between mobile phones or between mobile phones and computer email. These can be text messages, still images, short films; or

- **Moderated chat room**; this is either an adult that is present or filtering software to make sure conversations taking place do not break the company's policies about online behaviour;

- **Plug-in**; a small piece of software that enriches a larger piece of software by adding features or functions. Plug-ins enable browsers to play audio and video;

- **Spam**; unsolicited "junk" e-mail sent to large numbers of people to promote products or services. Sexually explicit unsolicited e-mail is called "porn spam." Also refers to inappropriate promotional or commercial postings to discussion groups or bulletin boards;

- **Subscribe**; means giving your email address to an organisation and they send information about themselves or their activities, events etc;

- **Whitelist**; a list of 'good' email addresses or Web sites. Some filters are/can be configured to only accept email or allow access to Web sites from the whitelist. A whitelist can also be used to create exceptions to the rules that filter out "bad" addresses and sites;

- **Worm**; a program that reproduces itself over a network, usually performing malicious actions, such as using up the computer's resources and possibly shutting the system down.

Revision History

Date last updated: May 2020

Date of next review: May 2021

Date of release: December 2018

End