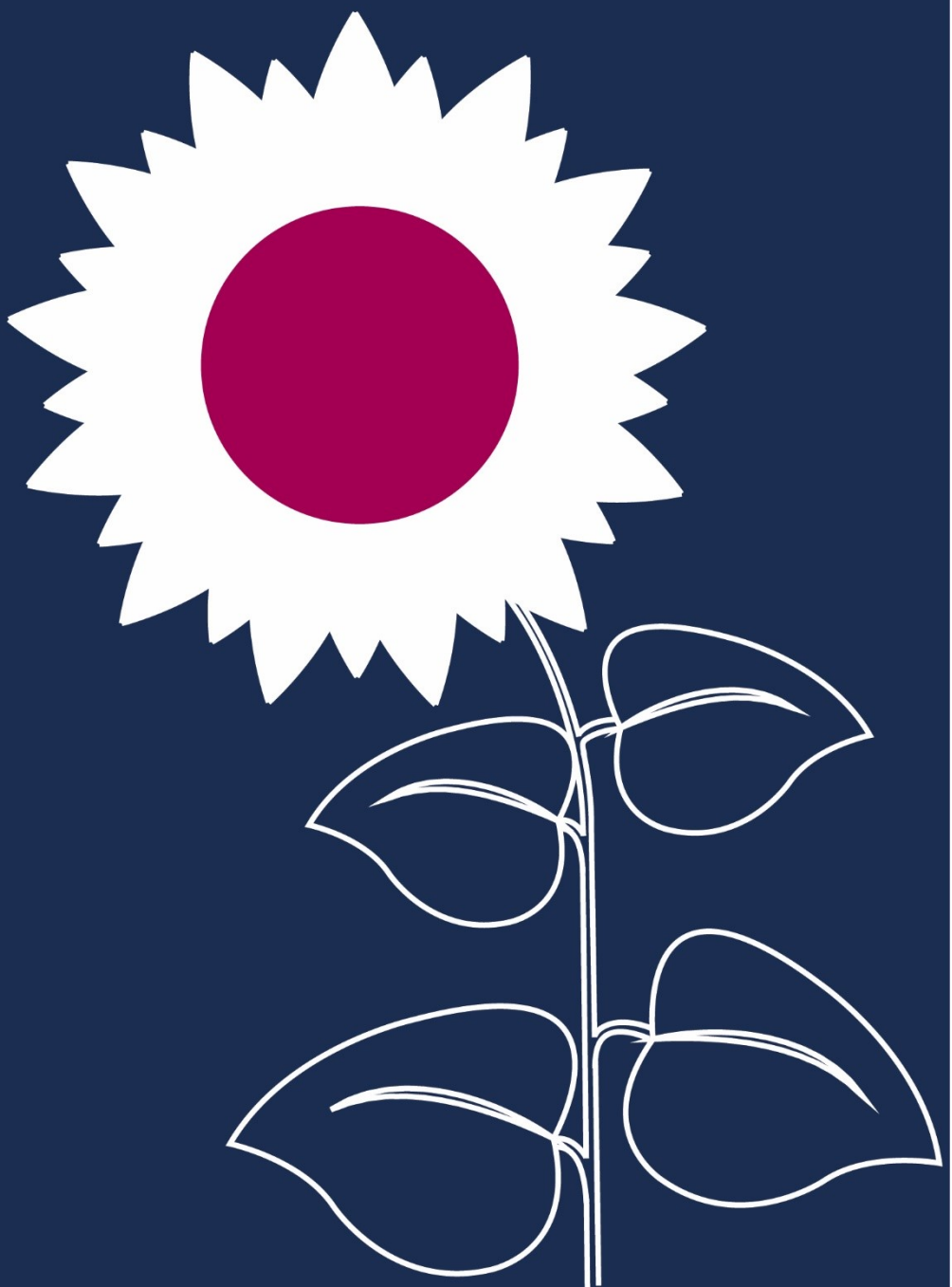
City of Stoke-on-Trent

Access to Computers – Guidance for Foster Carers

Tri x 5_1_16 July 2022

Review date July 2023



Access to Computers, Internet Safety and Use of Social Media

Guidance for Foster Carers

1.0 Introduction

1.1 On -line technology has changed the way children/young people 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/young people's access to computers and use of the internet whilst in the care of the Local Authority or under the supervision of staff or volunteers. Key to this is engaging with parents/carers to make them aware of internet safety issues.

1.2 It is also necessary for appropriate permissions to be established from those with parental responsibility for the child/young person, to take part in any on-line activity organised or promoted by the Local Authority. These permissions should be confirmed at the placement agreement meeting.

1.3 Staff and foster carers who unsure about what controls can be put in place, should seek advice from someone who has an up-to-date knowledge of current information technology.

2.0 Child/young person's use of computers and the internet

2.1 Children/young people'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 activity to another. These would include but are not limited to:

- Research to help with homework, projects and course work.
- Getting in touch with each other via Emails, Instant Messaging (IM), chat-rooms, discussion groups or to swap files, music,
- Playing online games; that can be downloaded from a website or they may play with others who are online (friends or strangers).
- Listening to music; downloaded from the internet or files from friends.
- Buying online
- Writing up project work or preparing presentations for school or College
- Use of Social Media for connecting and chatting with friends, contacts and people they can meet on the internet.

3.0 Associated risks of computers and internet usage

3.1 The main risks of on-line activities are personal and technological:

Personal Risk:

- Meeting someone online. 'Luring' is the term for online behaviour that leads to these meetings and is illegal. The vast majority of reported cases relate to children/young people over 15 years and female.
- Loss of privacy. Disclosing name, address, telephone number to a stranger can put the child/young person 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 feelings.
- On-line bullying; this is a common problem and the most common techniques are that children/young people are harassed or harass others via text messaging, internet chat rooms and emails.
- Making threats/law breaking; this can range from being rude to committing crimes online. It can also include putting someone else in jeopardy by publishing names, addresses or phone numbers of someone they know.
- Accessing 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/young person to search for material that they might not otherwise come across.
- Increased vulnerability; it is possible for children/young people to set up their own Web sites (at no cost). Anything posted can be seen by anyone visiting the site.
- Misrepresented Identity: It is easy for children/young people to forget that when they enter a 'chat room' 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 chat-room 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.
- Unmonitored activity i.e. Instant Messaging (IM); similar to chat but unlike in some chat rooms, there is never anyone else there to monitor activity.

Technological:

- 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.
- 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

4.0 Managing risks and promoting safe use of the internet

4.1 Recognising the potential threats to children/young people on the internet is the first step to protecting them. It is important to become familiar with how the child/young person uses the internet. It is also worth bearing in mind that some mobile phones and games consoles provide internet access.

4.2 The safe use of computers by all children/young people with whom staff work - whether they are placed in foster care, residential care or living with their parents or other members of their family should be monitored. It is important that social workers ensure parents and carers are aware of their responsibilities in relation to the child/young person's safety in this context, and that carers sign to confirm that they accept these as part of any written agreement

4.3 The following is recommended to promote the safe use of the Internet:

4.4 Location: keep the computer with internet connection in the kitchen area, family room, or other areas where the child/young person is 'independent' but not alone. This can be discussed with the child's social worker in order to ensure that we are recognising the child's best interests, it may be appropriate for a child to use their lap top/computer in their bedroom in line with their peers. All children are individual and as such this should be recognised when making decisions regarding their use of electronic devices. Children's safety is paramount and equally so is their self-esteem, their wishes and feelings need to be considered where it is appropriate.

4.5 Control: install filtering software, a comprehensive list is available on www.getnetwise.org. 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. Parental control software 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/young person sends emails to and blocking access to all or some chat-rooms.

4.6 Check: ask the child/young person 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.

4.7 Monitor on-line relationships: find out who they are sending emails to and who they are receiving them from. You should know if they visit chat-rooms or subscribe to news groups and you should understand what they do when they visit these places.

4.8 Review Accessibility: It is important to have rules about the sorts of websites and materials it is acceptable for the child/young person to access.

4.9 Discuss: Talk about what they do online. Having an open relationship with the child/young person 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.

4.10 Be open and honest: It is vital to openly discuss with the child/young person the possibility of them seeing or being sent sexually explicit or other worrying material. Children/young people 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/young people can feel most isolated and vulnerable to the control of sexual or other kinds of predators.

4.11 Manage and limit time: there are no hard and fast rules about what is excessive use of the Internet as it will vary from child/young person to child/young person, depending on their 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/young people may play on-line games, chatting or emailing each other under the pretext of doing homework.

4.12 Instil caution and care: children/young people 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. For more information contact Internet Content Rating Association www.icra.org

4.13 Moderated (supervised) chat-rooms: ask about policies enforced in the chat-room, the training given and checking done on the backgrounds of the people who are employed by them as moderators. More information on staying safe in chat-rooms can be found on the Home Office site www.thinkuknow.co.uk

4.14 Keep yourself informed: Children/young people may be exposed to risks because adults looking after them are unaware of the dangers they are confronted with. DCSF sponsor a site to help parents keep up with internet safety issues: www.parentsonline.gov.uk/safety/index

4.15 Practice guidance:
Filtering software should, however, not replace discussions about safety issues and ground rules as children/young people can gain access to the Internet in other places (friends' homes, internet cafes etc).

5.0 Glossary of terms

5.1 Chat-room: 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.

5.2 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.

5.3 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.

5.4 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.

5.5 Downloads: Transfer of information on to a computer which often is free. It can be images, games, music etc.

5.6 File Sharing: Accessing files on one computer from a different computer.

5.7 Filtering software: Allows blocking out of certain material from the computer such as websites with violent, racist or sexual content.

5.8 Filtered ISP: An Internet Service Provider (ISP) that sets criteria for determining content which is inappropriate for children/young people, and automatically blocks subscriber access to that content.

5.9 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.

5.10 Flaming: Posting or sending a deliberately confrontational message via news group, email, etc., usually in response to a previous message.

5.11 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.

5.12 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.

5.13 IRC: Internet relay chat, which is another form of online chat with software that can be downloaded.

5.14 MMS: Multi-media messaging service, which means sending messages between mobile phones or between mobile phones and computer email. These can be text messages, still images or short films.

5.15 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.

5.16 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

5.17 Social Media/Social Networking: Social Networking websites allow users to connect and communicate with others. People use social networking to keep in touch with friends, family, colleagues and to meet new people they haven't met in the real world. You've probably heard of some of them; www.facebook.com, www.myspace.com and www.bebo.com are a few examples.

5.18 Spam: Unsolicited 'junk' email sent to large numbers of people to promote products or services. Sexually explicit unsolicited email is called 'porn spam.'

Also refers to inappropriate promotional or commercial postings to discussion groups or bulletin boards.

5.19 Subscribe: Means giving your email address to an organisation and they send information about themselves or their activities, events etc.

5.20 White list: 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 White list. A White list can also be used to create exceptions to the rules that filter out 'bad' addresses and sites.

5.21 Worm: A program that reproduces itself over a network, usually performing malicious actions, such as using up the computers resources and possibly shutting the system down

5.22 The following organisations provide a wealth of guidance and information on their websites, where their contact details can be found.

www.kidsmart.org.uk
www.nch.org.uk
www.parentscentre.gov.uk
www.besafeonline.org
www.childnet-int.org
www.parentsprotect.co.uk/social_networking