TRAFFORD
COUNCIL

Services for Children, Young People and Families

Children in care

Children's homes

Safe and proper use of computers and the internet

Reviewed April 2020

Reviewed by: Sally Rimmer

Date to be Reviewed:January 2022

The Internet, like so many other technological advances, is not immune from criminal abuse, and can bring its own dangers, not least to children. Behaviour on the Internet is subject to the same rule of law as elsewhere. We need to take precautions on the internet to protect children from harm.

The benefits of ICT and the internet are immense – Trafford Council wants children and young people in care and care leavers to access these benefits. In doing so, the Children in Care Service is also taking steps to avoid the potential dangers as far as possible.

We all need to ensure that taking sensible precautions to protect ourselves and our children on-line should become as commonplace as it is to lock our doors or not talk to strangers.

Carers have a crucial role to play, whatever their internet experience or expertise. This guidance is not intended to alarm, but to alert to the potential dangers that children and young people may face online and help carers to help them use the PC and the Internet positively and safely.

What is the internet?

The internet is a large number of computers all over the world linked together with cables and standard phone lines. A number of companies specialise in providing this service for a fee.

What is the World Wide Web?

To make the appearance of information available through the internet more attractive, and to help people find information, it is possible for special pages of information to contain text, colours, and pictures, sound and even video. These pages collectively make up what is known as the World Wide Web. Most of these pages include information on the location of other pages on the World Wide Web, and it is possible to follow up links between pages with similar or related content. Moving from one page to another, regardless of where in the world they might be located, is called browsing or surfing the net or web.

What is email?

This is merely a way of sending messages from one person to another via the internet. Each internet user has a unique e-mail address (such as anybody@anything.com) and by sending a message to this address, the recipient can read the message the next time he or she connects to the internet. Internet e-mail addresses are usually provided when you connect to the internet.

What are news groups?

These are collections of messages written for public readership rather than addressed to an individual. Each collection or group of messages is about a particular subject or theme. Individuals can reply to these messages, and these replies are also public. In this way it is possible to track a multi-way conversation about an important issue of the day. At present there are more than 10,000 different topics available for discussion, from specialist science research to special interest support groups. Most of the media and public concern for pornography on the internet refers to news groups.

What are the dangers of the internet referred to in the media?

There is material on the internet that would be offensive to most people, such as pornography and racist material, and this can be accessed by children if using the internet unsupervised. Software can be installed to try to 'filter' known offensive locations of material of this kind, but there is too much for this filtering to be completely effective, and the locations change frequently. The only way to lock access to this kind of material is to have a restricted range of pages available, in which case many of the advantages of the global and dynamic nature of the internet may be lost.

Child, carer and staff guidelines for internet use

Trafford Council aims to promote good behaviour on the internet as in other areas of caring for children.

The internet is provided for children to do homework, conduct research, access learning activities and communicate with others. Access is an opportunity but not an automatic right – access requires responsibility.

Individual users of the internet need to be guided to use it safely and sensibly.

Computer storage areas and discs should not be considered private. Children should be made aware that staff/carers may review files and communications to ensure that the system is being used responsibly and carers and users need to note that Trafford Council reserves the right to check the content of materials produced or accessed on equipment bought via funds available to Trafford Council. Files stored on servers or discs may not therefore always remain private.

Children, young people and carers need to be aware that the following are not acceptable:

1. Sending or displaying offensive messages or pictures
2. Using obscene language
3. Harassing, insulting or attacking others
4. Damaging computers, computer systems or computer networks
5. Violating copyright laws
6. Using others passwords
7. Trespassing in others folders, work or files
8. Intentionally wasting limited resources
9. Spreading computer viruses
10. Attempts to hack into other computer systems

There is no automatic right for a child/young person to access the internet. If a child is getting into any kind of difficulty or is behaving irresponsibly in relation to computer use, the concern needs to be raised and addressed with the child's social worker as with any other concern that could arise in the child's life.

The installation of 'Cyber Guard' is strongly recommended or a similar programme on each computer as a means to reduce access to inappropriate material, unless special circumstances exist and an alternative agreement reached.

Young people will in many cases be more IT aware than most staff and carers.

Passwords need to be kept secure. In each setting the approach to use of passwords and the approach to safety, needs to be considered by staff/carers and confidentiality and security addressed.

All staff have a responsibility to seek to adapt and advance the use of ICT. Staff teams should seek to be aware of training opportunities which may be accessible.

Trafford Council expects staff and carers do all they can to be alert to potential dangers related to the internet in the same way as potential dangers in other aspects of caring for the child/young person; by offering guidance, and generally caring as a good parent and including talking to the child/young person, being vigilant and active in giving positive interest and attention.

Within day to day care and supervision, and backed by statutory visits and reviews, checks should be made as a matter of good care practice and to ensure that ground rules for responsible internet use to be confirmed and recorded in respect of each

child/young person and that access to the internet is beneficial and well managed for each child/young person.

Children's homes

Staff can only access the internet for business only and with endorsement of the line manager.

Staff are bound by Trafford Code of Conduct and The Acceptable Use Policy. The registered manager should ensure that every member of staff has signed it.

Managers need to know that use of the PC can be tracked on different levels. This will involve checking of some PCs.

Staff use should not impede young people's use of equipment unless this is written into the child's individual risk assessment.

Acceptable use of the internet

Where the computer system is owned by Trafford Council and is made available to the placement to further the education and development of children and enhance their 'life chances'.

Trafford Council reserves the right to examine or delete any files that may be held on its computer system or to monitor any internet sites visited (and will conduct checks of some machines as part of the implementation of its policies).

Social workers and carers are used to considering whether there are risks to children from contacts by phone, letter or face to face. The internet adds another dimension to this, but the same principles should be applied.

Carers, staff and children/young people accessing the internet should sign a copy of the Acceptable Use internet statement and return it to the child's social worker (in foster care and other settings) or to the manager (in Trafford's Children's Homes).

Rules for internet use

Children and young people should be guided to:

- ask permission from a carer/member of staff before using the internet
- not load content onto the computer without permission
- make sure the e-mail messages sent are polite and responsible

- only use his/her own login and password, which will be kept secret, and will not use anyone else's password, login or mailbox
- not access other peoples files
- not give his/her name, home address or telephone number or anything else that could identify him/her on the internet or on e-mail
- not arrange to meet anyone at any time he/she has been in touch with via the internet.

Also efforts will be made to ensure he/she understands that:

- Carers/staff will check computer files and monitor the internet sites visited from time to time
- All internet activity should be appropriate to carer/staff roles and responsibilities and to the child/young persons personal and educational development
- Access should only be made through a password, which should not be made available to anyone else
- Activity that threatens the integrity of the ICT system, or activity that attacks or corrupts other systems, is forbidden
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received
- Use for gambling is not acceptable
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same care about levels of language and content should be applied as for letters or other media
- Use of the network to access inappropriate materials such as pornographic, racist or other offensive material is not acceptable

E-safety guidance for staff and carers

Introduction

Mobile phones and the internet are now an integral part of children's lives. It opens up many educational and social opportunities giving children access to a global world of information.

Whether on a computer at school, laptop at home, mobile phone, or games console children will access the internet wherever they are. The Byrone Report (2008) concluded that the internet cannot be made 100% safe and should be a central concern for parents/carers.

Online safety skills are skills for life and if your child understands the risks and makes sensible and informed choices online they can get the most from the internet and stay safe.

Mobile phones

Mobile phones increase the children's feeling of independence as they can:

- Plan arrangements and visits with family and friends
- Play games, download ring tones, and take pictures
- Access the internet providing them with access to their emails, social networking and gaming sites

Risks

- Children can access information from the internet and TV wherever they are without parental/teacher supervision
- With picture and video messaging children need to be increasingly careful about the images they share. It is very easy for inappropriate images to be shared around a number of phones, changed and put online where it is impossible to get back
- Children need to be aware that they put themselves at risk of mobile phone bullying (cyber-bullying) if they give out their mobile number to people they don't know or fully trust

Reducing the risks

- Phones come with filtering software included so children won't access inappropriate websites or contacts. Check the phone has this capability.
- Keep reminding the child that any image they send on their mobile can be changed and stored online and that once they have sent an image they have lost control of it.
- Help children to understand that they should not give out personal details, e.g. mobile phone numbers, address, email address to strangers or other young people who they don't trust

Internet safety

- Help children to understand that they should never give out personal details to online friends they do not know offline
- Explain to children what information about them is personal i.e. address, email address, mobile number, school name, sports club, arrangements for meeting friends and family, pictures or videos of themselves or family
- Children need to be aware that they need to think carefully about the type of information and pictures they post on their profiles as anyone can change or share these images of them
- It is easy to forget that the internet is not a private space and this can lead to risky behavior online
- If children receive spam or junk mail and texts remind them never to believe their contents, never reply to them or use them
- Explain to children not to open files from people they don't know as they won't know what they contain e.g. a virus or inappropriate image or film
- Help children to understand that some people lie online so never meet up with any strangers alone
- Always keep telling children it is never too late to tell someone if something makes them feel frightened or uncomfortable

What is social networking?

Social networking websites like Facebook, TikTok and Instagram offer children a central place on the web where they can create their own online profile containing personal information e.g. name, email address, hobbies, likes, dislikes, photos, videos and also set up contacts on 'friends' lists with whom to share it.

Most social networking sites have a minimum age of 13yrs. Children might be accessing their social networking from a home computer, a friend's laptop or on a mobile phone. They also may have more than one social networking profile and hundreds of contacts on their 'friends' list some of whom they don't know in real life. Facebook is the most visited website in the world it has become one of the biggest influences on the lives of girls in particular.

Tips for carers

Be positive

Take a look at some of the main social networking websites e.g. Facebook, Twitter and, Instagram, and set up your own profile

Talk to the child about social networking to understand what they do and ask to see their profile if possible to discuss, but be aware they might have more than one

Explain they must be honest about their age when they register and why it is important

Stay positive about social networking sites, try to balance between educating young people to behave safely and also trust them to use their profile responsibly

Explain privacy

Most social network providers have tools for user protection including privacy tools and it is important to make sure that children know how to use these tools

It is important to discuss what is meant by privacy and for them to check privacy settings

Encourage children to set their settings to private and remind them friends known only online are still strangers

Photos

Help children think about the implications of posting photos and think about what is suitable:

- What type of picture
- What type of attention it may attract
- Information it could divulge, who could see it
- Photos can be easily copied, changed, shared, used elsewhere, and potentially stay online forever
- "would you want a relative or future employer to see this photo?"

Postings

Help children to think first before they post any information. Think about what is and isn't appropriate to say.

Also about the effect on other people which may start as a joke but could cause embarrassment and a lot of pain and unhappiness and cannot be taken back.

Sharing Information

It is important children tell adults about anything they are worried about or any bullying. Adults need to take information seriously. It is vital they keep any evidence and report it via the Child Exploitation and Online Protection Centre website

Remember: Information can become public very quickly and children can be at risk by:

- Creating and posting offensive or illegal content on their own or other people's web pages. Any content can be copied, changed and reposted by anyone and this can be damaging and targeted later and cannot be rectified

- Putting too much personal information on these sites. Chatting about personal information may encourage someone to contact the child online or in person or encourage cyber-bullying

Many children see social networking sites as a private space like a diary, so it is important they understand the risks and how to keep themselves safe

Reminder for young people

Click Clever, Click Safe

Zip it, Block it, Flag it:

- Zip it – keep personal information private and think what you say and do online
- Block it – block people who send nasty messages, don't open unknown links and attachments
- Flag it – flag up with someone you trust if anything upsets you, or if someone asks you to meet offline

Do's and Don'ts

Don'ts

Don't give out your personal details online - age, address, mobile number, school etc

Don't arrange to meet strangers that you have met online

Don't give out your user name and passwords

Don't download unknown files – music, videos, photos, or games

Don't go on adult, racist, or hate websites

Don't do anything that makes you feel uncomfortable or that you believe is not right

Don't open unknown links or attachments

Do's

Do get information for your homework online

Do chat and hang out with your friends online. Use a nick name instead of your real name when using chat rooms or instant messenger

Do visit and surf safe websites

Do share your music with your friends online

Do set privacy settings to restrict access to personal information

Do leave a chat room if someone or something worries or upsets you. Report it to your carer immediately

Do have fun

Do be considerate to others – share the time online

Do keep passwords secret, change them regularly

Do block people who send nasty messages

Useful websites

Thinkuknow website

Childnet International website

Get Safe Online website

getnetwise website

UK Council for Child Internet Safety (UKCCIS)