(38) Internet Safety and Social Media

Using computers and similar devices to go online has made everyday activities such as shopping, banking, paying bills and keeping in touch fast and easy … anytime, anywhere. There are, however, several risks associated with going online, some general and some specific to the respective activities that you carry out.

There are a number of sensible and simple measures which you need to take in order to protect yourself against these risks, which include identity theft, criminals stealing your personal and financial data to defraud you or empty your bank account. The precautions are as simple as choosing safe passwords and ensuring you have adequate antivirus/antispyware installed, to learning how to distinguish between genuine and fraudulent websites and emails.

Privacy settings

- Hosts should ensure that all devices with internet access are safe and secure, including privacy and password settings.
- Hosts should encourage and support Individuals to also consider safe and secure access to the internet with privacy settings and passwords.
- Social media sites should be set to private to ensure only those they choose can view their account.
- When supporting an Individual with capacity to set up an account, they should be encouraged to make their account private and advised not to share their passwords or personal information with others. Internet safety should be discussed with them and their vulnerability around this.
- Privacy settings should be reviewed at least annually to ensure the correct privacy is in place.

General Data Protection Regulations (GDPR)

- GDPR needs to be considered when using the internet or social media platforms.
- As described in the Host agreement, Hosts are responsible for keeping personal data safe for the people they support.
- As controllers and processors of information, should they breach these regulations they are liable to fines or prosecution.
- Here is Kent Shared Lives Privacy Notice

Mobile phones and Apps

- Privacy settings also require consideration on mobile devices, these should be checked at least annually.
- People should be encouraged to have locks or passwords to access their phones and report any lost or stolen devices. This should also be reported

to the Shared Lives team via an incident form indicating any potential data breaches.

Photographs

- Any photographs of the people Hosts support need to be used only with informed consent from them, if they are unable to agree to the use of the photograph due to capacity, they should not be shared with others.
- Consent can be provided by filling in the KCC consent form or via a written confirmation that this can be used.
- People can choose at any time to withdraw their consent by putting this in writing to the Shared Lives service.
- When giving consent, Individuals need to demonstrate that they understand who may be able to see/access/comment on these photographs. If they are unable to demonstrate this then the host must consider whether informed consent has actually been given.

Online Gaming is a popular pastime for both young people and adults across the world. Many games have adopted an interactive online element - whether it's playing against other users, chatting or making purchases.

- Chatting within gaming
  - many games have functions allowing users to chat with one another. Gamers will usually communicate within the game to coordinate game tactics, although it can just be to chat as they play. Depending on the game and its chat functions, they may be able to type messages or talk to one another through a headset. Some consoles also allow them to leave voice messages and chat when a game is not in play.
- Depending on their privacy settings, gamers can be contacted by people they may or may not know or play against 'bots' (a computer-controlled character that may send messages to gamers).
- Bots can be hard to spot as their messages can seem very realistic. These messages often contain links to external websites which are inappropriate for young/vulnerable people, showing violent or sexual content.
- If your placement receives a message from an unknown user, ask them to not respond or click on any links contained within the message. Report these users directly to the site.
- Gifts within gaming
  - Some games and apps allow users to make purchases. Gamers can buy tools that can be used in the game to give them an advantage such as weapons, coins or cheats.
  - Offenders use gifts in gaming to encourage a person to trust them. They may offer gifts asking for nothing in return, this can be part of the grooming process and can help to build a close relationship with a person. Others may try to use gifts as 'leverage' to persuade young people to do something such as moving to a different online platform, going on webcam or taking a photo of themselves.

  - If you are worried that a person is being groomed in a game, or on any other online platform you should seek support. You can contact your local police or report to the social care safeguarding team. If you believe a person is in immediate danger call the police on 999.

Social Media
Are interactive computer-mediated technologies that facilitate the creation or sharing of information, ideas, career interests and other forms of expression via virtual communities and networks.

- Examples include:
  - Facebook (and its associated Facebook Messenger), YouTube, WeChat, Instagram, QQ, QZone, Weibo, Twitter, Tumblr, Telegram, Baidu Tieba, LinkedIn, WhatsApp, LINE, Snapchat, Pinterest, Viber, VK, Reddit, and more.

Social Media checks

- When a new Host application is received, Shared Lives will carry out a social media check for all those listed on the application form (over 18 years).
- This check will ensure the application is of good character and any social media posts not inappropriate (For example, posts that show aggressive, illegal or discriminatory content).

Safeguarding
A key part of the care and support you provide to the Individuals using the Shared Lives service is around keeping people safe.
The world wide web is a risky place and there are many vulnerabilities to us and the people we support.

- Hosts should report to the Shared Lives service and/or social care funding teams when they become aware of any concerns relating to internet safety and risk.
- A safeguarding alert may be required to be completed with the potential for police involvement and investigation.
- There are many dangers on the internet including chat rooms, harassment on social media, hate crimes and trolling.

Reporting
Any concerns regarding internet safety or data concerns and breaches should be reported to the Shared Lives service as soon as possible. An accident/incident report should be submitted.

Helpful resources
Some helpful information and resources can be found on Kent County Councils webpage: Kent County Council online safety resources
Cyber Security course - Delta

This policy to be read alongside:

- Confidentiality policy
- Code of conduct and Practice policy
- Consent policy
- Host Agreement
- Safeguarding