LHA
LOSTOCK HALL ACADEMY

Online Safety

What is internet safety?

Internet safety is the act of staying safer online. This includes being aware of the risks associated with your child's online activity and employing a few strategies to prevent or avoid these risks. Internet safety is also sometimes referred to as online safety, cyber safety, or e-safety.

The internet and children: the risks

The Internet offers many positive educational and social benefits to young people, but unfortunately, there are risks too. As in any other area of life, children and young people are vulnerable and may expose themselves to danger, knowingly or unknowingly, when using the internet and other digital technologies. Indeed, some young people may find themselves involved in activities that are inappropriate or possibly illegal.

Inappropriate Material

One of the key risks of using the internet, email or chatrooms is that young people may be exposed to inappropriate material. This may be material that is pornographic, hateful or violent in nature; that encourages activities that are dangerous or illegal; or that is just age-inappropriate or biased. One of the key benefits of the web is that it is open to all, but unfortunately, this also means that those with extreme political, racist or sexual views, for example, are able to spread their distorted version of the world.
In the case of pornography and child abuse images, there is no doubt that the internet plays host to a large amount of legal and illegal material.

Physical Danger

The threat of physical danger is perhaps the most worrying and extreme risk associated with the use of the internet and other technologies, and is probably the risk most reported by the media.
A criminal minority make use of the internet and chatrooms to make contact with young people with the intention of developing relationships which they can progress to sexual activity. Paedophiles will often target a child, posing as a young person with similar interests and hobbies in order to establish an online 'friendship'. These relationships may develop to a point where the paedophile has gained the trust in order to meet in person. These techniques are often known as 'online enticement', 'grooming' or 'child procurement'.

Bullying

Cyber Bullying – whether by internet, mobile phone or any other method – is another aspect of the use of new technologies that provide an anonymous method by which bullies can torment their victims. While a young person may or may not be in physical danger, they may receive email, chat or text messages that make them feel embarrassed, upset, depressed or afraid. This can damage their self-esteem and pose a threat to their psychological wellbeing.

Illegal Behaviour

Some young people may get involved in inappropriate, antisocial or illegal behaviour while using digital technologies. Just as in the real world, groups or cliques can form online, and activities that start out as harmless fun, such as voicing an opposing opinion to another member of a chatroom, can quickly escalate to something much more serious.

Illegal Activity

Some children and young people may become involved in other equally serious activities. Possible risks include involvement in identity theft or participation in hate or cult websites, or in the buying and selling of stolen goods. The ease of access to online gambling, suicide sites, sites selling weapons, hacking sites, and sites providing recipes for making drugs or bombs are also of great concern. There is some evidence to suggest that young people have become involved in the viewing, possession, making and distribution of indecent and/or child abuse/pornographic images.

Divulging Personal Information

Most parents do not allow their children to give out personal information online and around 50% of children acknowledge this. Just under half of 9-19 year old children who go online once a week say that they have given out personal information, such as their full name, age, address, email address, phone number, hobbies, name of their school etc., to someone they met on the internet.

Top parenting tips for keeping your child safe online

Steps to increase internet safety for kids:

- Set parental controls.

- Install family security apps.
- Use internet safety filters.
- Use safety features on social media sites.
- Install antivirus software.
- Keep the computer in a common space.
- Password-protect all accounts.
- Update your operating systems regularly.
- Balance safety with independence.

Set parental controls on devices and apps

Parent controls are built-in features included on devices and apps. With these features, you can customize your child's online experience. What parental controls are available on each device or app varies, but in general, they limit screen time, restrict content, and enhance user privacy.

Features of parental controls:

- Limit screen time.
- Turn off in-app purchasing.
- Prevent inappropriate or mature content.
- Limit website access.
- Play, message, or send/receive content with approved contacts only.
- Monitor device location through GPS.
- Take time to look at what parental controls are available on your child's commonly used apps. Then, set them to reflect the type of experience you think is best for your teen's online safety.

Install family security apps

Use safety filters through your internet providers (ISPs)

Internet service providers (ISPs) like AT&T and Verizon offer parental controls as part of their internet security suite of services. Usually, these are free with your service or come with a small monthly fee.

Use safety features on websites

Safe Search in Google filters out most mature and inappropriate content and YouTube has "Restricted Mode." Some apps or software does this for you. Spend a few minutes making sure that sites your child uses have the appropriate settings ticked so that it is less likely your child will stumble upon inappropriate content.

You can also install adblockers on your web browsers. Ads can often contain intrusive or inappropriate content. Safety settings and internet filters can help but consider taking the extra step of adding an add-blocker to remove the risk of harmful pop-ups.

Install security or antivirus software programs and a VPN on your computer

Cybersecurity or antivirus software programs prevent spyware or viruses that may harm your computer if your child visits a malicious site. Using these programs, parents can also set up regular virus checks and deep system scans to make sure there is no harmful activity happening.
A VPN hides users' internet activity from snoops and spoofs your location. This protects your kids by making sure hackers or predators cannot detect their actual location. You can install a VPN on your router so that the location is spoofed on all connected devices.

Keep the computer in a common space

If possible, experts suggest keeping computers and devices in a common space so you can keep an eye on activity. It prevents children from doing things that might be risky. In addition, if inappropriate or harmful content appears through messages or popups, you can address it with your child right away.

Password-protect all accounts and devices

From phones to computers to apps, put a password on it. That way, no one without the password can access you or your child's device. Keep track of passwords by using a password manager.

Update your operating system regularly

All your devices from mobile phones or tablets to computers and smartwatches receive important updates in response to security issues on a regular basis. Be sure to install them regularly so you have the most up-to-date security fixes and remain safe online. Our recommendation is to set updates to install automatically so your device is less vulnerable to known attacks. Usually, you can find this feature in Settings, then select Automatic Updates, but it varies between devices.

Balance cyber safety controls with independence

Tips to balance safety with independence:

- *Explain why.* Tell your teen why you put safety controls on the family's devices. It is not because you do not trust them, but because there are other people on the internet that you do not trust.
- *Empower them.* Make sure your teen knows how to report inappropriate content or behaviour online themselves. If they want to download a new app, do the research together so they can decide for themselves if it is safe.
- *Allow them to have privacy*. Whether that is with or without a device, do not assume they are hiding something simply because they want privacy. If there are apps or games that you feel comfortable with them playing in their room, consider that option.
- *Make sure boundaries are clear.*

Useful Links

https://www.internetmatters.org/
https://www.parentsprotect.co.uk/
https://saferinternet.org.uk/
https://www.thinkuknow.co.uk/parents/

Reporting Concerns

https://www.thinkuknow.co.uk/parents/Get-help/Reporting-an-incident/
https://www.ceop.police.uk/safety-centre
https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/remove-nude-image-shared-online/

Social Media Checklists

https://saferinternet.org.uk/guide-and-resource/social-media-checklists
https://swgfl.org.uk/resources/checklists/snapchat/
https://swgfl.org.uk/resources/checklists/tiktok/
https://swgfl.org.uk/resources/checklists/instagram/
https://swgfl.org.uk/resources/checklists/twitter/
https://swgfl.org.uk/assets/documents/facebook-checklist.pdf