E-Safety The Heath School

Whilst the online world is a fantastic place for research and creativity, and can be a great arena for children to develop future job skills, introducing them to the world of commerce and business, it can also introduce them to a number of risks;

- Cyber bullying and the lack of appropriate rules
- Online privacy and personal information and the increasing
- Likelihood of being hacked
- Reputation management and 'digital footprint'
- Sexting, grooming, pornography and inappropriate material
- Illegal downloads and copyright infringement
- Spam, phishing, viruses and malware
- Children lying about their age to get onto social networking
- Platforms with a 13+ age limit
- Pressure to respond to comments 24/7

As a parent, these risks may make the internet feel daunting and overwhelming. Understanding what children do online and the risks they face will help you keep your child safe online. Creating a positive environment where your child can be open and inquisitive and feel confident discussing their online experiences, whether positive or negative is essential.

Top tips to stay safe online

1. Do not post or give out any personal information that could identify you.

- This includes your name, your address and pictures or links to your school
- Don't post details of where you're going to be at particular time
- Make sure you use the security and privacy features on your social networks, so you only share what you want with who you want.

2. Don't arrange to meet anyone you have only ever met online.

- You can:
  - Say – No
  - Tell – Tell your trusted adult
  - If your trusted adult says you may go, take them with you and meet in a public place

3. Learn how to block and report people on every chat app. you use.

- You should:
  - Only add people you know in the real world
  - Don't get involved in online arguments. Once it's said online it can be there forever

- Don't join in with online bullying just because others do it, be the better person
- Use an avatar as your profile pic, rather than a photo of you
- Only post comments and photos/videos you'd be happy for your parents to see

4. Don't open emails from people / places you don't know.

- Remember:
  - Only give out your email address to people you know or on official forms
  - If you're not sure have a second disposable email address for spam, you can always change it to your 'personal' address later
  - Many viruses, malware and ransomware and other and similar files are spread by emails
  - Phishing and scam emails are extremely common, if it sounds too good to be true it probably is

5. Keep your device secure with the latest security updates and virus protection.

- The latest anti-virus software with the latest virus definitions is essential. This includes everything that connects to the internet like your computer, tablet or phone.

6. Suspicious or abusive activity on the internet can be reported by the following methods:

www.IWF.org (Illegal websites)

www.ceop.police.uk/Ceop-Report (advice and make a report)

www.beatbullying.org (anti bullying)

7. Advice for parents and children is available from the following:

www.ceop.police.uk/safety-centre

www.getsafeonline.org

www.commonsensemedia.org (what's good/safe to see and do)

www.vodafone.com/content/parents.html (for parents)

Police – Non Emergency phone 101 (advice and to report a non-urgent incident).

Police – Emergency 999 (someone or their property at immediate risk).

E-Safety The Heath School

Further advice and support can be sought from:

https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

https://www.net-aware.org.uk/

https://www.thinkuknow.co.uk/

http://www.childnet.com/

At The Heath all of our student computers are monitored using eSafe Education's Forensic Monitoring Service.

"At e-Safe, we understand that keeping children and young people safe, when they're using the school's ICT system, is all about identifying these risks early, and then putting the necessary intervention strategies in place to stop them from escalating.

That's why we offer a unique, comprehensive monitoring solution, providing not one, but three, vital components for detecting early safeguarding risks."

1. *Advanced detection software - with the capability to monitor words and phrases, in any language, as well as images that are moving and static.*
2. *Expert interpretation & assessment - Working behind the scenes a dedicated team of behavioural experts work diligently to identify the early warning indicators of inappropriate and harmful behaviour.*
3. *Dynamic threat libraries - updated daily to maintain detection accuracy - Working in collaboration with external partners and schools, our experts update and refine threat libraries on a daily basis to detect emerging behavioural trends at an international, national and local level.*

Transgressions and breaches of our ICT Acceptable Use Protocol (AUP) are dealt with in line with our Behaviour Policy.

<u>Sexting (Youth Produced Sexual Imagery)</u>

Sexting is when someone shares sexual, naked or semi-naked images or videos of themselves or others, or sends sexually explicit messages.

They can be sent using mobiles, tablets, smartphones, laptops - any device that allows you to share media and messages.

Sexting may also be called:

- Trading nudes
- Dirties
- Pic for pic.

Help or advice can be found here:

https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting/

http://kidshealth.org/en/parents/2011-sexting.html