Online Safety Advice for Parents and Students

Information for Parents and Students about online safety, with home learning activities can be accessed from ThinkUKnow by clicking Online Safety Home Learning Activities and from the Department for Digital, Culture, Media & Sport by clicking here.

Parent and Carer Helpsheet: keeping your child safe online while they are off school

Our Tips, advice, guides and resources to help keep your child safe online can be downloaded here.

Cyber Security Advice during Coronavirus can be found here

Safeguarding from harmful influences online advice can be found here

Parents: Supporting Young People Online (Childnet)
https://www.childnet.com/ufiles/Supporting-Young-People-Online.pdf

Leaflets available in a range of other languages here
https://www.childnet.com/resources/supporting-young-people-online

- Arabic
- Bengali
- English
- Farsi
- French
- Hindi
- Polish
- Punjabi
- Somali
- Spanish
- Turkish
- Urdu
- Vietnamese
- Welsh

Better Internet for Kids has sites for all European countries: https://www.betterinternetforkids.eu/sic

Online Safety Factsheets on the following can be found by clicking on the relevant name:

- **TikTok**
- **YouTube**
- **YouTube Kids**
- **Instagram**
- **Fortnite**
- **WhatsApp**
- **Snapchat**
- **Cyber-flashing**
- **Loot boxes and skins betting**

Online Safety Advice for Parents and Students

The internet is an amazing resource if used properly. If not, it can be a minefield. As a parent, it is very difficult to stay on top of social media, apps, online gaming, Facebook, Instagram, WhatsApp, Snap Chat and the latest online crazes. More importantly, do you know what your child is doing online? Do you know who they are talking to? Do you know what they are posting? Do you know how to take control and so ensure your child's online safety? The following tips will help you to keep your child safe online.

If you are concerned with your child's online safety please contact Mr É Casey, Assistant Headteacher/Designated Safeguarding Lead, or your child's Head of Year for support.

HeadofYear7@ecaterham.net

HeadofYear8@ecaterham.net

HeadofYear9@ecaterham.net

HeadofYear10@ecaterham.net

HeadofYear11@ecaterham.net

SixthForm@ecaterham.net

Alternatively, if you are worried about anything, you can email to get in touch with the Safeguarding Team on Safeguarding@ecaterham.net

10 Top Tips for ...

KEEPING CHILDREN SAFE FROM CYBER CRIME

We all want to continue being informed and inspired by the ever-expanding capabilities of the internet. But we also need to be able to safeguard ourselves against the growing amount of online hazards. Knowing what is fact, understanding what dangers exist and taking appropriate steps can go a long way towards protecting yourself and your family. National Online Safety has collaborated with the Yorkshire and Humber Regional Cyber Crime Unit to compile 10 pointers to help you keep your children safe from cyber crime.

1. Spot Phishing Bait

Phishing messages are untargeted mass emails asking for sensitive information (e.g. usernames, passwords, bank details) or encouraging recipients to visit a fake website. It's safest to learn the warning signs of phishing and increase your child's awareness. Too good to be true? Spelling or punctuation errors? Odd sense of urgency? These are all red flags. Don't click on links or follow demands: if you're unsure, contact the official company directly online to enquire further.

2. Don't Over-Share

Is your child sharing too much on social media? Do they post things about their private life, upload images of your home, or discuss their friendships and relationships online? Criminals will gather this information and may try to use it for identity theft or other offences such as fraud. To combat this, ensure your child's privacy settings mean they are only sharing information with family and close friends. Use parental controls where appropriate.

3. Encourage Strong Passwords

Weak passwords make it faster and easier for someone to gain access to your online accounts or get control of your device – giving them a route to your personal information. For a strong password, national guidance recommends using three random words (e.g. bottlegaragepylons). Consider paying for your child to access a password manager. Encourage them to have a separate password for their email account. Ensure the whole family uses two-factor authentication where possible.

4. Stay Updated

People often put off installing updates to apps or software because they don't feel it's necessary, it can be time consuming, or could cause problems with programmes they rely on. But updates help protect users from recently discovered vulnerabilities to malware. You can usually set them to run automatically – encourage your child to select this option. Ensure updates are installed as soon as possible after you're notified they're available.

5. Back up Your Data

Some cyber attacks can lead to the theft or deletion of important (and possibly sensitive) data or loss of files (like photos and videos) that can't be replaced. Backing up your data to the cloud – or to another device – will help prevent data loss if you ever became the victim of a cyber attack. Where possible, set your child's devices to back up automatically. Also encourage them to back up their data prior to installing any updates.

6. Be Wary of Public WiFi

Free public WiFi is commonplace – but it's often not secure and sends unencrypted data via the network. A hacker on the same network could access personal data (like financial information) without you even realising they'd done so. To avoid this, suggest to your child that they use their 3G or 4G mobile data when they're out and about, rather than free WiFi. Consider purchasing a VPN (Virtual Private Network) where possible.

7. Take Care When Chatting

Criminals may look to manipulate others online and coerce them into using their talents or cyber skills for unethical means. Try to get your child to be open about who they are talking to online. Communication tools such as Discord are popular among gamers – but be cautious of the other people using them, and ensure you know who your child is chatting with.

8. Recognise Warning Signs

Often, budding cyber experts will relish the challenge of testing themselves or earning recognition from peers for their exploits. Even principled 'white-hat' hackers will look to test their skills online. If you think your child is interested in hacking, try to understand what their motivation is. You could encourage their participation in ethical competitions such as bug bounties.

9. Understand Their Motivations

Those being influenced online to use their skills unethically may display certain key warning signs. Sudden evidence of new-found wealth (unexplained new clothes or devices, for example), secrecy around their online behaviour or boasting of new online friendships are all causes for concern. If in doubt, refer through to your regional cyber crime team.

10. Know the Consequences

Many young people may feel that hacking is essentially a light-hearted prank, and not especially serious. So make sure your child is aware of the implications of a conviction under the Computer Misuse Act – not only the possibility of a criminal record, but also lifelong travel restrictions and damage to their future career or educational prospects.

Home School Cyber Links

Cyber Discovery

Studying from home doesn't have to be a chore. Join our Virtual Cyber School, in partnership with HM Government, where you will gain access to CyberStart Game until 31st August 2020 - an interactive learning platform played and loved by over 200k students worldwide.

Our Virtual Cyber School is offering thousands of free licences to keep students occupied.

cyber-school.joincyberdiscovery.com

Weekly Webinar

As part of the Virtual Cyber School we are also offering you the chance to join our free weekly webinars. Join CyberStart creator and cyber security expert, James Lyne, as he uses CyberStart Game to teach security disciplines and digital forforensics.

"The challenges are interesting and satisfying. If I didn't know how to do something, I was encouraged to look through the manual and do extra research to learn how to do it; this gave me a sense of ownership over the solution, which was incredibly rewarding." **Previous Cyber Start student**

With your free CyberStart Game licence, you'll be able to explore and have a go at over 200 online cyber security challenges. Learn how to crack codes, find security flaws and dissect criminals' digital trails whilst playing as a cyber agent in our Cyber Protection Agency.

Students with no previous experience or interest have gone on to master techniques such as SQL injection and XXS.

Our training has taught them how to write their own programs and learn what it means to be an ethical hacker working in the industry.

NCA Cyber Security Challenge

Why not try your hand at navigating your way through a series of challenges? for example, a codebreaking exercise set in the historic Bletchley Park with **Codestrike** or defend several office buildings against a cyber attack with **Outbreak** and complete a series of cyber security related tasks in **Cyber Land**

The National Crime Agency & Cyber Security Challenge have developed a selection of interactive resources and games that aim to introduce you to different aspects of Cyber Security.

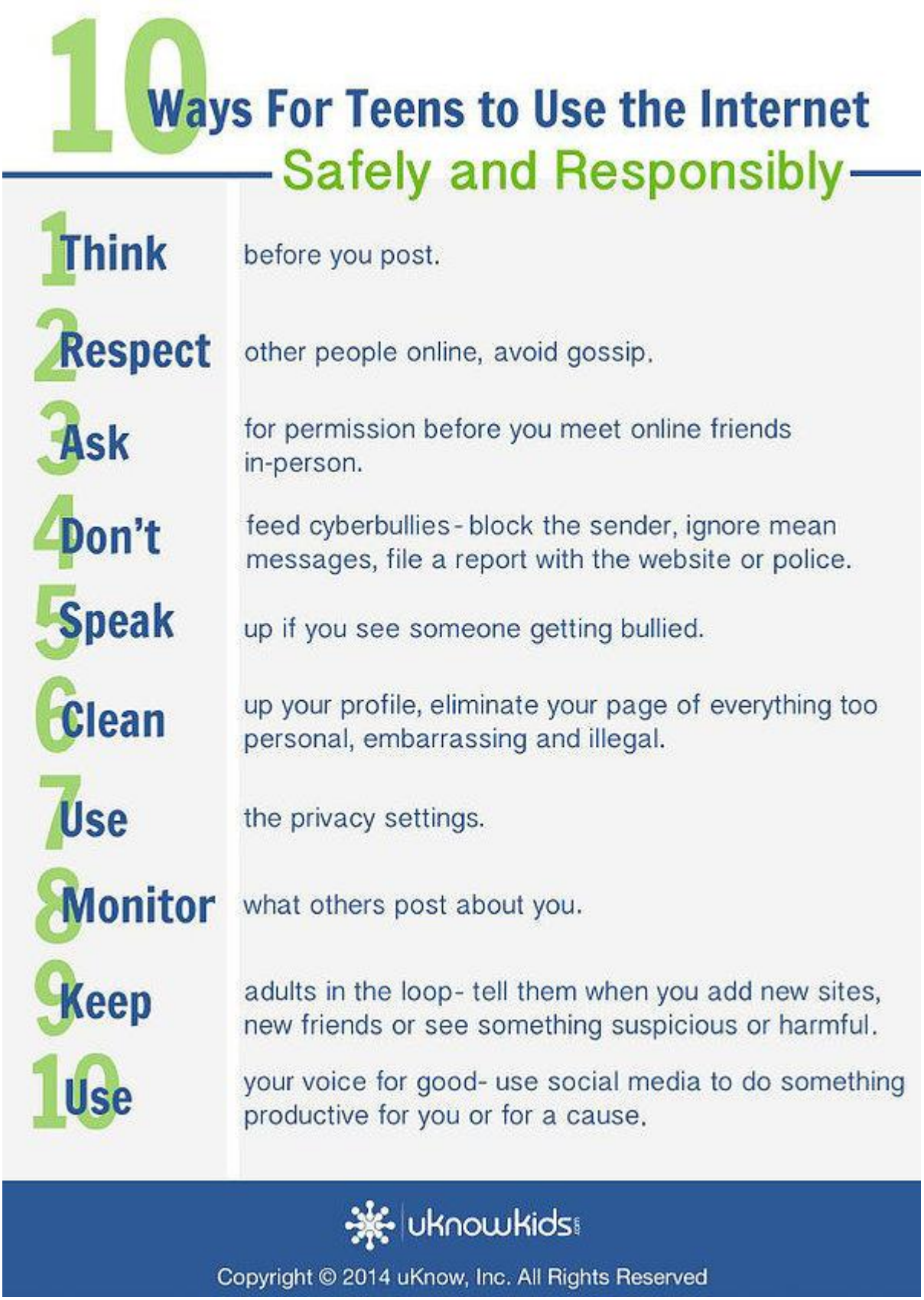
www.cybergamesuk.com

Cyber First

Cyber First was launched by the National Cyber Security Centre (NCSC), a part of GCHQ, as a programme of opportunities helping young people explore their passion for tech by introducing them to the world of cyber security.

So whatever your age, you could be anyone, from anywhere in the UK. We're not here just for the genius coders either; we're open to all sorts of tech and computing passions. **Livestreamers** with their own gaming vlogs or **Instagrammers** who could find the perfect angle in their sleep!

Click here to go to Cyber First



<iframe width="847" height="502" src="https://www.youtube.com/embed/bnl_gnRF3PE" title="YouTube video player" frameborder="0" allow="accelerometer; autoplay; clipboard-write; encrypted-media; gyroscope; picture-in-picture" allowfullscreen></iframe>

https://youtu.be/bnl_gnRF3PE

Childnet's mission is to work in partnership with others around the world to help make the internet a great and safe place for children. They work directly with children and young people from the ages of 3 to 18 on a weekly basis, as well as parents, carers, teachers and professionals, finding out about their real experiences online, and the positive things they are doing as well as sharing safety advice.

http://www.childnet.com/

Online Safety Tips for Parents:

1.If you are a parent of a Year 7 or Year 8 child under the age of 13 it is illegal for them to have a Facebook profile or be on Instagram as the minimum age is 13.The profiles must be deleted.

2.Make sure your child uses their online privacy settings at all times to keep their personal information private.

3.Make sure your child regularly changes their password and does not share this with friends.

4.Make sure your child knows not to share personal information like their name, address, mobile number, email address online.

5.Inform your child that they should not post anything online that they wouldn't want you to see. The Golden Rule is that if they wouldn't want their parents to see it, don't post it.

6.Monitor their selfies. Ask them to show you what they are posting.

7.Make your child aware that whatever they post online may come back to haunt them at a later date, whether it's college or university leaders checking them out before offering a place or employers checking them out before a job interview. Once it is posted, there is no going back.

8.Make sure your child only talks to real life friends or family on social media sites and in chatrooms.

9.If your child talks to a stranger online or games with them online, please make them aware that they could be talking to or playing with anyone pretending to be something else, such as pretending to be a member of the opposite sex, pretending to be younger or older than they say they are, pretending to have a different job to the one they have.

10.Ensure your child knows not to make arrangements to meet up with complete strangers online.

11.Make sure that your child is not sharing their geo-location when they are online. Ensure they have geo-location disabled to keep their whereabouts private.

12.Make sure your child knows that any messages and photos shared on Snap Chat no longer disappear but can now be saved. The sender is then informed that the recipient is saving what they have posted.

13.Monitor that your child uses secure and legal sites to download music and games.

14.Monitor that your child only uses online games, apps, films and social networks that are appropriate for their age. Age ratings come with all online games, apps, films and social networks.

15.Is your child an internet gaming addict? Do they play for hours at a time? Do they talk about online gaming non-stop? Do they get defensive or angry when asked to stop? Are their sleep and meal times disrupted because of online gaming? Do they have red eyes, headaches, sore fingers, back or neck? Discuss with your child how long they play for. Set rules on how long they play for. Ban tech in their rooms after lights out or remove all tech from their rooms so they can't play all night long when you think they are asleep. Arrange offline activities such as sports or clubs to get your child out of the house and away from the online games.

16.The best way to find out what your child is doing online is to talk to them about it and to ask them to tell you and show you what they do, what sites they access, what things they post online.

17.Ask your child how many followers do they have? Their followers should be only family and friends. Explain that some followers may not be who they say they are.

18.Ask your child if they are taking part in online streaming. Online streaming is the process of delivering continuous multimedia forms, such as music and films. Paedophiles can use this to contact your child and abuse them by asking them to do a variety of things.

19.Ask your child if they are being cyberbullied. Make sure they know how to block abusive comments and report content that worries them. This can be done on the CEOP website Child Exploitation Online Protection Centre (CEOP): www.thinkuknow.co.uk

20.Parents can gain a greater control of online safety at home by ensuring that parental controls are set on home broadband and any internet devices, including your child's mobile phone. Parents can find out how to do this at your broadband provider's website. Additionally, Google provide information and advice on how to set up online safety at home on : https://www.google.co.uk/safetycenter/

21.Talk to your child about the benefits and risks of social networking before they join any sites. Let them know that anything they upload, email or message could stay around forever.

22.Make your child aware that using public Wifi might not filter inappropriate content, so they should look for friendly Wifi symbols when they are out and about.

23.Inform your child that they should check attachments and pop ups for viruses before they click or download anything.

24.Have a family agreement about where your child accesses the internet. If they are accessing it in their bedroom, do you really know what they are doing? Would it be better to place devices in the living room only so you can monitor your child's online activity? Can your child use their mobile phone in your living room only?

25.Have a family agreement about how much time your child spends on the internet and stick to it or reduce it, especially if they are not completing all their school work.

26.Have a family agreement about the sites they can visit. Ask them to show you.

27. Have a family agreement about the type of information they can share online. Ask them to show you information before they post it. Ask them to show you recently posted information.

28.Make sure they know that they can come to you if they are upset by something they have seen online.

29.Talk to your child by explaining that if they are talked into bullying someone on line or send inappropriate images it may get reported to us at school and even to the police.

30.As we would say to our children in life, treat others as you would like to be treated, it is the same principle online. Talk to your child about not sharing anything online that can hurt others. Tell thin to THINK BEFORE THEY POST.

31.Parents can download free online safety resources at: Child Exploitation Online Protection Centre (CEOP): www.thinkuknow.co.uk

32.Internet Matters: www.internetmatters.org

33.Childnet: www.childnet.com

34.Parentzone: www.parentzone.org.uk

35. NSPCC: www.nspcc.org.uk

36.Talk Talk: https://help2.talktalk.co.uk/top-tips-staying-safe-online

37.Sky: https://www.sky.com/help/articles/safety-and-security-on-your-sky-products

38.Virgin Media: https://my.virginmedia.com/customer-news/articles/online- safety.html

39.BT: bt.custhelp.com/app/answers/detail/a_id/50602

40.Vodafone: https://www.vodafone.com/content/sustainabilityreport/2014/index/operating_

responsibly/child_safety_online.html

InternetMatters.org are a not-for-profit organisation with the aim of empowering parents and carers to keep children safe in the digital world.

Learn more about what they do by clicking on the image to the right.

Downloads

PAGE DOWNLOADS	DATE
STUDENT ACCEPTABLE USE POLICY.PDF	19TH JUN 2018
INSTAGRAM PARENTS GUIDE 2016.PDF	07TH FEB 2019
KEEPING CHILDREN SAFE IN EDUCATION	14TH SEP 2018
KIK MESSENGER PARENTS GUIDE.PDF	07TH FEB 2019
LIVESTREAMING PARENTS GUIDE V2 081118.PD...	07TH FEB 2019
OMEGLE PARENTS GUIDE.PDF	07TH FEB 2019
OOVOO PARENTS GUIDE.PDF	07TH FEB 2019
SNAPCHAT PARENTS GUIDE.PDF	07TH FEB 2019
WHAT PARENTS NEED TO KNOW ABOUT SNAPCHAT...	07TH FEB 2019

PAGE DOWNLOADS	DATE
WHATSAPPGUIDE.PDF	07TH FEB 2019
YOUTUBE PARENTS GUIDE.PDF	07TH FEB 2019
PRIVATE TUTOR AND TUITION SAFEGUARDING I...	30TH APR 2018