CRAVEN COLLEGE

E-SAFETY HANDBOOK

Craven college

CONTENTS

E-SAFETY INTRODUCTION

As we get used to staying home during the COVID-19 pandemic our devices and the internet are playing a big role in keeping us all connected and supporting our education, news, entertainment and distraction! The internet is an amazing resource which enables us all to connect, communicate and be creative in a number of different ways, on a range of devices.

There are lots of fun and interesting things you can do on the internet. And it can be a great way to stay in touch with friends. But it's important to understand how to stay safe online. Social media, cyberbullying, grooming, phishing and financial scams are an online reality. Craven College have put together this handbook to share our best online safety tips to keep you safe from risks online and where to go for support and advice.

What is e-safety?

E-safety, Online Safety or Internet Safety all means the same thing. It's about risk; it's about being aware of the possible threats that online activity can bring, and how to deal with them.

These risks are grouped into four categories:

CONDUCT

Personal online behaviour that may put you at risk of harm for example making, sending and receiving explicit images, or online bullying.

CONTENT

Being exposed to illegal, inappropriate or harmful material, for example pornography, fake news or radical and extremist views.

CONTACT

Being subject to harmful online interaction with unsuitable, unpleasant or dangerous people such as adults posing as children.

COMMERCIALISM

Use of platforms with hidden costs which may put you at risk.

YOUR DIGITAL FOOTPRINT

The things online that you have liked, shared and commented on, as well as what others have shared about you, may shape what other people think about you; this is your online reputation.

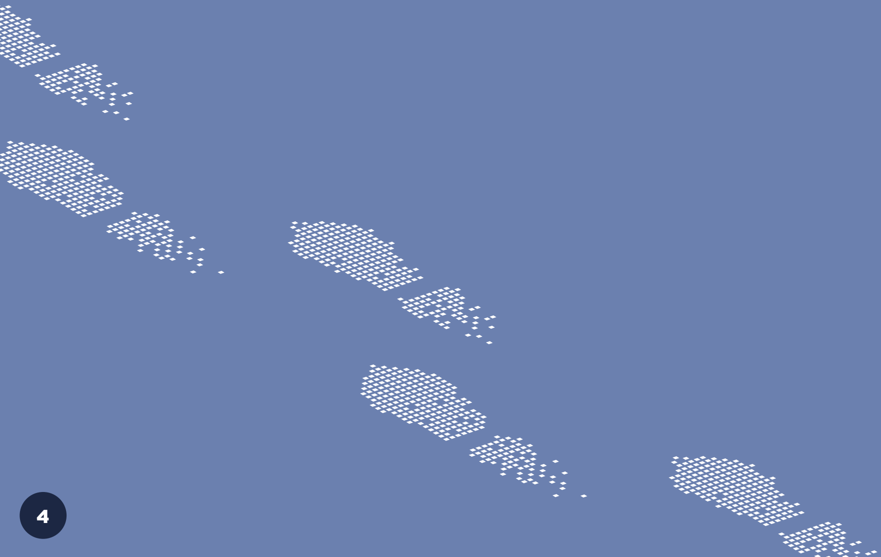
The internet plays a big part in or lives, we use it to connect, shop, work, play, buy and sell. Be aware of the trail you are leaving behind!

Your digital footprint is the mark that you leave behind when using the internet and can shape your online reputation. Your digital footprints can be positive or negative and shape how people see you now and in the future.

Most social networks allow you to manage your privacy settings so that your posts aren't public. Check your settings and aim to only post neutral or positive content. Once you post something it's not always in your control who saves or shares it.

Check out Childnet's Checklist below to help manage and maintain your online reputation or go to:

https://www.childnet.com/resources/online-reputation-checklist



MAKE A POSITIVE FOOTPRINT

The internet is a fantastic way to shout about all your achievements and to let everyone know about all the amazing things that you create and do online. The best way to keep your online reputation in check is to use your time online to get creative and leave a positive mark behind.

SEARCH YOURSELF ONLINE

Do you know what is online about you? Its recommended that you search your name online regularly. You might be aware of the content you post about yourself online, but are you aware of what others post about you? Set up Google Alerts – where you will receive an email every time your name appears in a Google search result. Remember: If your Instagram or Twitter pages appear you can change this by adjusting your privacy settings.

CHECK YOUR PRIVACY SETTINGS

Make sure that you know what information you are sharing on the platforms you use, in particular social networking sites. See our Social Media help with privacy settings or go to **www.saferinternet.org.uk/safety-tools** to learn about how to set up privacy settings on your account.

THINK BEFORE YOU POST

Be proud of everything you post online! Even if a service states that once you post a photo it will disappear after a certain time period of time, once something is online it could potentially be there forever!

DEACTIVATE & DELETE

If you stop using a social media account it's a good idea to deactivate or delete your account. Deactivating your account means that you can still access the content posted for a period of time. Deleting the account removes the account completely. Over time, this will prevent it appearing in search results on a site or through a search engine, and it will remove the risk of these accounts being hacked without you knowing.

STAYING SAFE ONLINE

The internet, apps and social media are a way of life for many, and they can be great for connecting and sharing. But becoming part of a network of millions of people you don't know does carry some risks.

Here are some things to think about:

Identifying information: Choose a profile picture that doesn't give away your personal information such as where you live or where you go to College. Keep your personal information safe, don't share your address, phone number or email anywhere on social media and never give any information to anyone you don't trust and know.

Friends: Be aware of who you "friend" online; not everyone is who they say they are. Never meet up with anyone you meet online if you don't know them in "real" life.

Bullying: Online bullying can be devastating. Respect others online and treat others how you would like to be treated. Remember, anything you post online is traceable. Before you post, THINK!

Blocking: If you are experiencing online bullying, speak with someone you trust. You can block the people who harass or abuse on most services without contacting anyone, as well as on chat services like WhatsApp. All social networks have policies about dealing with inappropriate messages – if you are receiving abusive messages you can take a screenshot and report the issue directly to the network or website you are receiving them on.

This page from Childnet **www.childnet.com/young-people/secondary/need-help** has links to the advice areas for specific networks

SOCIAL MEDIA GUIDES AND HELP WITH PRIVACY SETTINGS

Different social networking sites have different privacy settings, so make sure you've looked at each site you use to check you're not sharing your posts further than you think. Use strong passwords for all accounts, and always log out if the device could be used by someone else.

Password security starts with creating a strong password.

A strong password is:

- At least 12 characters long but 14 or more is better
- A combination of uppercase letters, lowercase letters, numbers, and symbols
- Not a word that can be found in a dictionary
- Not the name of a person or a popular entity such as a character, product, or organization
- Significantly different from your previous passwords
- Easy for you to remember but difficult for others to guess
- Consider using a memorable phrase like "6MonkeysLooking^"

Check how secure your password is at:
https://howsecureismypassword.net/

TREAT YOUR PASSWORD LIKE A TOOTHBRUSH — DON'T GIVE IT OUT AND CHANGE IT REGULARLY!

Safer Internet UK and SWGfi have collaborated with a number of social media providers to create safety checklists. These checklists provide tips and guidance on how to use safety and privacy features on a range of social media platforms including Facebook, Twitter, Instagram and Snapchat.

Who can find content I post?
How does my profile appear?
What is there about you on the web?
How do you use 'Friends' lists?

https://swgfl.org.uk/assets/documents/facebook-checklist.pdf?_=1553264115

How do I protect my privacy?
Who can follow me?
How do I report something?
How do I unfollow or delete content?

https://swgfl.org.uk/assets/documents/twitter-checklist-2020.pdf

Is my account private or public?
How to share with a select group of followers?
How do I block someone?
Do you know how to report a post?

https://swgfl.org.uk/assets/documents/instagram-checklist.pdf

How can I stay in control?
How do I find all my friends?
How do I block and delete?
How do I report a problem?

https://swgfl.org.uk/assets/documents/snapchat-checklist.pdf

What is TikTok
How to stay safe on TikTok?
How to block users on TikTok?
Where can I go for further support?

https://swgfl.org.uk/assets/documents/tiktok-checklist.pdf

CYBERBULLYING

Online bullying, sometimes called cyberbullying, is any behaviour that uses technology and devices to deliberately target or upset someone. Further information:

https://www.childnet.com/young-people/secondary/bullying

The internet is a tool, but how we use it is up to us. Some people choose to deliberately target or harass others, with the intention of upsetting or humiliating them. This is never okay and, for the victims, can be incredibly difficult and damaging.

TOP TIPS

1. Always be kind and respectful online. Remember that just because you're not saying it to someone's face, doesn't make it okay. Bullying online is unacceptable.

2. Report and block the bullies! Most social media sites and some games have reporting and blocking tools to supports users.

3. Don't retaliate. If someone is unkind online, being unkind back won't help. In fact, it could make the situation worse and you could end up getting in trouble.

4. Save the evidence using screenshots (or a picture of the screen, if a screenshot isn't possible) of offending messages, conversations or other situations online involving bullying.

5. Tell someone! Speak to an adult you trust like a parent, carer, tutor or one of our Safeguarding Team for support and advice on what to do next.

GAMING

Gaming involves playing 'video games' on a games console (such as a PlayStation 4, XBOX One or Nintendo Switch) a PC or mobile games on a smartphone or tablet. Further information:

https://www.childnet.com/young-people/secondary/gaming

Games can give you great experiences because of their exciting storylines or through puzzles that engage your brain. They can also be a good way to take a break from College work or things that are causing you stress. However, it is important to think about how playing video games makes you feel – if playing a game is causing you to worry, feel frustrated or stressed, then it might be time to take a break.

TOP TIPS

1. Balance gaming and 'screen time' with more physical activities away from the device so that it does not affect your studies, sleep, diet and health.
2. Be careful with what you share with other players and remember that not everyone will be who they say they are.
3. Report and block other players that try to bully or harass you when gaming online. Keep any evidence of the incident, and speak to someone you trust about what has happened.
4. Remember that many video games are designed to make money, so think carefully about any purchases and speak with a parent or carer about setting up spending limits.
5. If a game stops being enjoyable at any point, take a break, and return to it when you are ready.

NUDES

Sending nudes, sometimes referred to as 'sexting', means taking or sharing naked, partially dressed or sexually explicit images of yourself or others, using technology. Further information:

https://www.childnet.com/young-people/secondary/nudes

https://swgfl.org.uk/assets/documents/so-you-got-naked-online.pdf

TOP TIPS

1. If you see nudes being shared around, don't join in. Report the images instead and if you can, make sure the person shown in them gets support.
2. If somebody is pressuring you or a friend to send nudes, remember that is sexual harassment and not okay. Speak to an adult for support and remember: it's not your fault.
3. Try to ignore gossip and rumours about nude images, especially if it sounds like everyone is doing it.
4. If your nude gets leaked online, stay calm and speak to an adult you trust for support and help such as our Safeguarding Team or contact a helpline.
5. Remember that even as part of a healthy, consensual relationship, nudes showing under 18 year olds break the law.

ONLINE GROOMING

Online grooming is when someone builds a relationship with a young person online because they want to trick or pressure them into doing something that may hurt or harm them. Further information:

https://www.childnet.com/young-people/secondary/grooming

Online groomers use many different methods. They may use fake accounts and photos or say they enjoy the same hobbies and interests as the young person they are grooming. Others may pretend to be modelling scouts, sports coaches, celebrities or influencers. However, not all groomers will choose to hide who they really are and some may try to build a connection or develop a 'mentor' type relationship based on their true identity.

TOP TIPS

1. Where possible, limit contact online to people you know and trust and use privacy settings to protect your personal accounts and content.
2. If someone online is pressuring you or a friend, or making you feel uncomfortable, speak to an adult you trust straight away.
3. If you or a friend are in contact with someone online who you do not know offline, do not share personal information such as where you live, go to College or photos of yourself.
4. If someone who you only know online asks to meet up with you or a friend, speak to an adult you trust straight away.
5. Remember that you can report any suspected grooming to the police using the 'report abuse' button on the ThinkUKnow website.

LIVESTREAMING

Livestreaming is a way for people to broadcast themselves online. Apps such as Instagram, Facebook, TikTok, Twitch and YouTube all offer livestreaming services. Further information:

https://www.childnet.com/young-people/secondary/livestreaming

TOP TIPS

1. Decide who you share your livestream with. Think about who may be able to join and view your livestream and make use of privacy settings to manage this.

2. Protect your personal information when livestreaming– remember things can be easily given away by what you say or show on video or from clues in the background.

3. Think carefully before watching a livestream. Remember you can never know exactly what you will see or hear.

4. Report any inappropriate behaviour. Try to get a screenshot of the content before it expires and remember to speak to an adult you trust too.

5. Use livestreaming in a positive way. As well as your own digital footprint and online reputation, always think about how your livestream will affect your viewers or other people who are captured on the video.

FAKE NEWS

Fake news most often describes inaccurate or false information spread online by either news services or via social media. However, the phrase is sometimes used in other ways such as to describe anything thought to be false, misleading or inaccurate online. Further information:

https://www.childnet.com/young-people/secondary/fake-news

TOP TIPS

1. Read beyond the headline – when scrolling or searching online, remember that you won't always get the full story from a headline, title or photo.
2. Look for the original source – whatever content you are looking at, try to work out who created it or where it came from originally.
3. Question the things you see – think about its purpose, whether it matches what you already know or if there are any clues it might be suspicious.
4. Do further research – it's always best to check multiple sources, like several websites, different videos or even offline in a book.
5. Take action against fake news – use the report tool or speak up about fake or misleading content and never share it on without checking it's true.
6. Speak to an adult you know and trust for further help and support.

PHISHING & SCAMS

Phishing and online scams are ways that people try to trick you into giving up your personal information, login details or money. Further information:

https://www.childnet.com/young-people/secondary/phishing-and-scams

TOP TIPS

1. Make sure you only use your account login details (username and password) on the official website or app for the service you want to use and don't share these with anyone (even friends.)

2. Don't click on any links you receive in messages or comments.

3. Be careful of online surveys, giveaways and things that threaten or rush you as they are often scams trying to get information from you.

4. Question what you see online, even if it looks official or promises something exciting; if something seems too good to be true, it probably isn't true.

IDENTITY THEFT

Action Fraud: "Identity theft is when your personal details are stolen and identity fraud is when those details are used to commit fraud."

Cambridge English Dictionary: "Identity theft is the illegal use of someone else's personal details, for example in order to steal money from their bank account."

Identity theft is the UK's fastest growing method used to carry out crimes, and although it mainly affects adults, it can happen to young people. When people share so much about their lives online, it gives criminals opportunity to collect information and use it to find out other personal details (e.g. using information they know about you to answer the secret question and change your password to be able to access your account) or to use what they do know about you to sign up for new accounts, products or services in your name.

What can I do if it happens to me?

If you realise your bank account or your personal information is being used by someone else, you can report suspected fraud to Action Fraud on 03001 232 040.

They have more information on their site:

http://www.actionfraud.police.uk/fraud_protection/identity_fraud

DIGITAL WELLBEING

Going online and using technology can impact our emotions and mental health. Digital wellbeing is about recognising the way going online makes us feel and knowing how to manage this.

Digital wellbeing is a little different during the pandemic because spending time online has become a bigger part of our daily lives. Our increased use of tech has been a big change for everyone; and home learning, and video calls might feel hard to get used to.

You might find that you are seeing conflicting or worrying information online and this can feel really unsettling. If you feel tired, anxious, or upset about what's happening online, be sure to take a break and talk to someone about how you're feeling.

Sometimes, constant messages or intense social media use can feel overwhelming, so remember that you don't always have to reply to things straight away. It is important to be kind to yourself during this time and try to enjoy some offline activities too.

NEED HELP?

Has something upset or worried you online? There are lots of people who can help!

Try to talk to an adult you trust or our Safeguarding Team if anything has upset you or made you feel uncomfortable whilst online. If you don't want to speak to someone you know then you can always seek advice and support from a helpline. For the list of helplines for young people go to:

https://www.childnet.com/young-people/secondary/need-help

Craven college

USEFUL CONTACTS

SKIPTON, SCARBOROUGH & LEEDS BRADFORD AIRPORT:

Deputy Designated Safeguarding Lead & Student Services Manager

Catherine Jackson	**07921 214 115**

Safeguarding Officers:

Mandy Taylor	**07921 743 706**
Amanda Beck	**07769 165 523**
Julie Atkins	**07841 986 008**
Katie Fox	**07921 214 113**

Email: **staysafe@craven-college.ac.uk**

RIPON EVOLVE:

Deputy Designated Safeguarding Lead & Evolve Centre Manager

Bev Skaife	**01765 608 999**

Designated Safeguarding Lead & Vice Principal - Curriculum & Quality

Anita Lall	**07545 647 038**