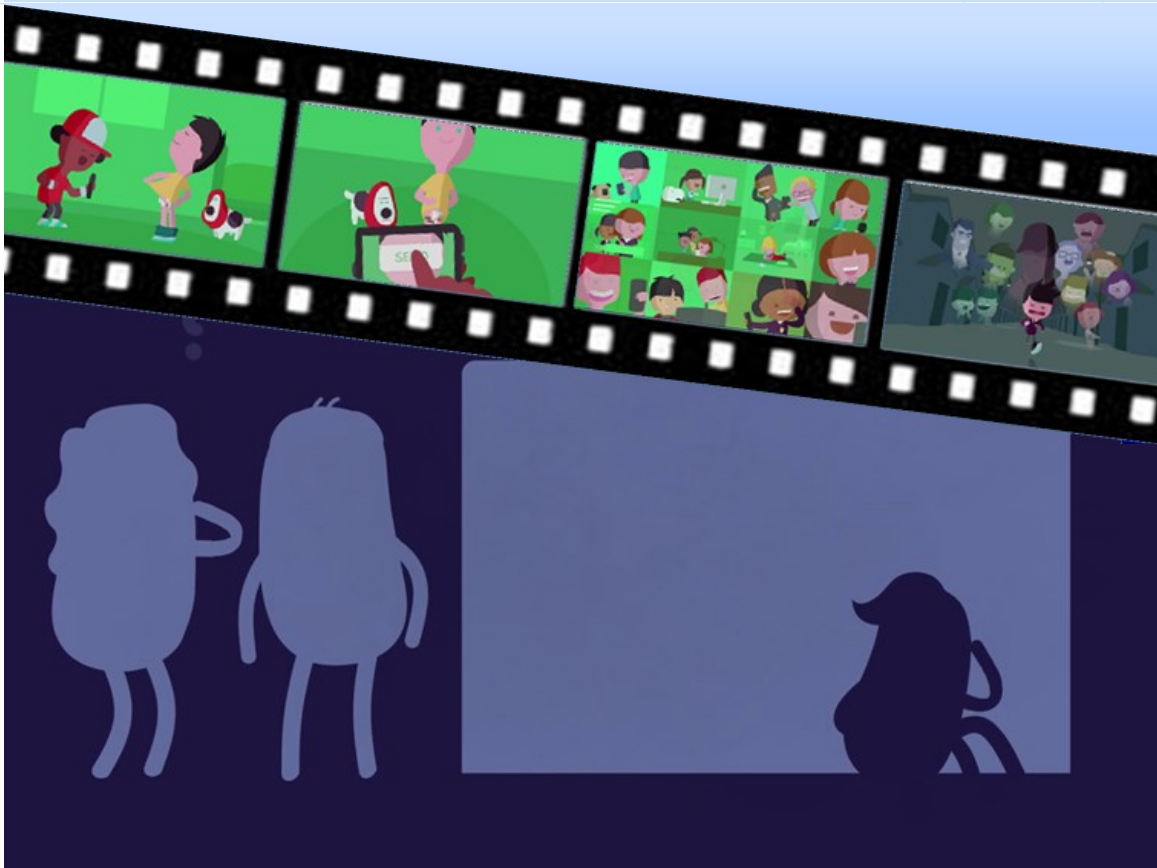
For further advice and information

Cleveland Police Cyber Crime
Online Child Safety



Cleveland Police are dedicated to promoting safer internet use and protecting people from becoming victims of cyber crime.

Technology is advancing at such a pace that many people feel left behind because they don't have the knowledge. Children are growing up in this technological world and from young ages they are using technology and social media which many parents feel they cannot begin to understand.

Parents may worry if they don't know what their child is doing online and they may not know where to look for help.

The good news is that parents don't need to be IT experts in order to help keep their children safe from cyber criminals, all you have to do is …

- Keep your computer software up to date
- Use antivirus software
- Set parental controls on devices
- Talk to your child about cyber crime including cyber bullying and sexting
- Be supportive and interested in your child's online activities
- Make sure your child knows their options if they are suffering any type of cyber crime

Cyber bullying is where the bully uses technology to communicate with the victim online by using their mobile phones, computers and tablets. Cyber bullying usually occurs via messages or social media.

Examples - The victim may be impersonated by the bully. The bully may develop a screen name similar to the victims, pretend to be them and then make posts. If the bully knows the passwords of the victims accounts, they can access the accounts and make posts pretending to be the victim. The bully could even change the password to something new meaning the victim cant access or have any control over their own accounts.

'Happy slapping' is the process of recording a bullying incident. Often where physical violence is used. The video may then be shared with others or posted online causing further embarrassment for the victim.

If the bully has access to personal photographs of the victim they may use these photos to blackmail the victim or share them with others to degrade or embarrass them.

Cyber bullying may be used to harass someone by threatening or embarrassing the victim or by posting rumours on a public forum about them.

Cyber clean

Unsafe Passwords

Your password is the first line of defence against hackers, fraudsters and cyber criminals.

- Create a strong password, at least eight characters, using letters, numbers and characters.
- Do not use the same password for different accounts.
- Do not share your password

Phishing

A common way for a cyber criminal to attack you is by using an email that's made to look like something official from somewhere like a bank, the police or a computer company.

- Ask yourself why that company is getting in touch with you
- Don't use links or phone numbers inside the email if you think they are suspicious
- If you suspect it's a scam, do not open, forward or reply to it.

Malware

Certain computer programs could allow cyber criminals to access your data. Prevent them getting in!

- Install antivirus software.
- Schedule the antivirus software to scan your computer regularly.
- Keep all your programs up to date by installing updates. These include security fixes.

Some simple steps to stay

Clickjacking

Cybercriminals may use something like funny videos or special offers to make you click on their links which download viruses onto your device.

- Think about what you're clicking on before you do.
- If it seems too good to be true, it probably is.
- If the phrase doesn't seem like that person made it, consider the possibility they didn't.

Identity Theft

Your personal information is big business to criminals. They could use this information to pretend to be you and make money from scams that could cost you!

- Never share passwords.
- Don't share information which might be used for security questions like mothers maiden name or first pets name.
- Try to use online nicknames that don't share any other information

Sexting - Sharing to shaming

Sexting is when someone shares sexual, naked or semi naked images of themselves or other people.

- 1 in 7 young people have taken a naked/semi naked image of themselves. Over half then shared that image with others (NSPCC).

Help and guidance resources:

- The Child Exploitation and Online Protection Centre's (CEOP) 'Play Like Share' and 'Nude Selfie' YouTube videos.
- The National Society for the Prevention of Cruelty to Children (NSPCC) 'I Saw Your Willy' YouTube video.

- Talk to your child regularly about the potential consequences of sharing sexual images and make sure they know they can turn to you if anything worries them.
- Ask them if they'd want something private shown to the world. Talk about the Granny rule - would you want your Granny to see the image you're sharing?
- If children are sending images to people they trust, they may not think there's much risk involved. Use examples of when friends or partners have had a falling-out and what might happen to the images if this happens.

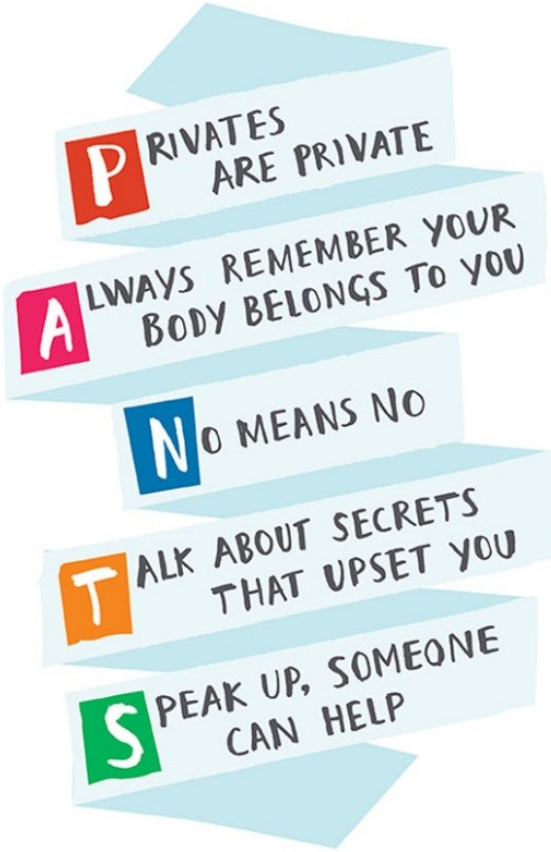
If your child is a victim of cyber harassment…

- Thank them for coming to you to talk about it. Try to stay calm and reassure your child.
- Ask your child what they want to happen, don't assume they have the same objective as you.
- Engage with the school if the bullying stems from there.
- Encourage your child not to react to bullying behaviour, to remove themselves from the situation and to report the situation to an adult.
- Regularly seek updates from your child but try not to be too overbearing. Be supportive and positive to empower your child to cope with it.
- Focus on your child's strengths and achievements in order to maintain their self belief and confidence. Bullying, whether online or not, could damage their self esteem.
- Keep a record of incidents in case you need to take the matter further at a later date.
- Remember police will take the report seriously

Remember online risks are the same as real world risks.

Use the parenting skills you already use everyday to speak to your child about situations they may face online. Listen to what they do and then learn what you can do to help.

The NSPCC 'PANTS' scheme is there to help keep children safe from abuse ...



Tell your child, remind your child that everything under their underwear is private.

Their body is theirs, don't do anything which makes them feel uncomfortable.

They have the right to say no.

They can talk about any secrets and reassure them they wont get into trouble for sharing with you.

An adult your child trusts can help them understand what's right or wrong.

The NSPCC can also be there for you if you have concerns over your child and they can be contacted on: 0808 800 5000.

Online safety rules

Always use privacy settings (most social media sites will provide you with guidelines)

Always think about what you're posting

Keep your account information secure

Keep your personal information secure

Do not post any abusive threats or bully or harass people

Do not post nude or sexual images

Do not break the law or support others doing so

Do not pretend to be someone you're not

Respect other people you're talking to

I will talk to my parents about posting pictures of myself or others online

I will be a good person and not do anything to hurt others

I will tell my parents straight away if I see something which makes me uncomfortable

I will not give out my passwords to anyone except my parents

I will never agree to get together with someone I 'meet' online without checking with my parents.

I will help my parents to understand how to do things online and to teach them about computers, the internet and other technology!!