

# Stay Safe Online



**Cleveland Police** are dedicated to promoting safer and more responsible use of online technology and mobile phones. While the internet and the technology used to access it is rapidly evolving, providing exciting new experiences and methods of communicating, it is important that children and professionals alike do not forget the risks that are associated with it.

As a result of cultural developments like cyber bullying being a relatively recent phenomenon, ethics are still being established by both those who create legislation based on this concept and how to regulate it. Nevertheless, the law currently views any sexual pictures of anyone under the age of 18 years as illegal due to the inherent risks to children being exploited and their pictures being distributed.

This booklet is an opportunity to provide children and professionals with the knowledge and awareness of how to utilise the technology available to them in an informed way to keep themselves and each other from exploitation and harm.



**CLEVELAND  
POLICE**

## **Cyber Bullying**

Cyber bullying is bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as mobile phones, computers, and tablets as well as communication tools including social media sites, text messages, chat, and websites.

## **5 Types of Cyber bullying**

### **Harassing Someone**

- Using text messaging, instant messaging and email to harass, threaten or embarrass the target.
- Posting rumours, threats or embarrassing information on social networking sites such as Facebook, Twitter, and Instagram.
- Engaging in “warning wars.” Many Internet Service Providers offer a way to report a user who is saying something inappropriate. Kids use the “warn” button as a way to get the victim in trouble or kicked offline.
- Participating in text wars or text attacks, which occur when bullies gang up on the victim and send thousands of texts. These attacks not only cause emotional distress but create a large mobile phone bill.

## Impersonating Someone

- Developing a screen name that is similar to the victim's screen name and then posting rude or hurtful remarks while pretending to be the victim.
- Stealing the victim's password and chatting with other people while pretending to be the victim. The bully will say mean things that offend and anger the victim's friends or acquaintances.
- Changing the target's online profile to include sexual, racist or other inappropriate things.
- Setting up an account on a social networking site and posting as the victim while saying mean, hurtful or offensive things online. Actual photos of the victim may be used to make the account look authentic.
- Posing as the victim and posting in chat rooms of known child molesters or hate groups. The bully may even provide the victim's personal information encouraging the groups to contact the victim.

### Participating in “Happy-Slapping”

- Using a camera phone to videotape a bullying incident, this may include one or more kids slapping, hitting, kicking or punching the victim.
- Downloading the videotaped bullying incident and posting it to YouTube in order to allow a larger audience to view the incident.
- Sharing a videotaped bullying incident via mass e-mail or text messaging to humiliate and embarrass the victim.

## Creating Websites, Blogs, Polls and More

- Developing a website with information that is humiliating, embarrassing or insulting for the victim.
- Spreading rumours, lies or gossip about the victim online through websites or blogs.
- Posting the victim's personal information and pictures on a website, which puts the victim in danger of being contacted by predators.
- Creating a blog about the victim that is embarrassing, insulting or humiliating.
- Using the information that was shared in confidence and making it public.
- Conducting an Internet poll about the victim. Questions in the poll may vary including everything from who is ugly and who smells to who is dumb and who is fat.
- Posting rude, mean or insulting comments about the victim via the chat option of online gaming sites.
- Sending viruses, spyware or hacking programs to the victim in order to spy on the victim or control his or her computer remotely.



## Using Photographs

- Taking nude or degrading pictures of the victim in a changing room, a bathroom or dressing room without his or her permission.
- Threatening to share embarrassing photos as a way of controlling or blackmailing the victim.
- Sending mass emails or text messages that include nude or degrading photos of the victim. This behaviour is often called "sexting," and once the photos are sent, there is no way to control it. The photos can be distributed to hundreds of people within just a few hours.
- Posting nude pictures on photo sharing sites for anyone on the Internet to view and download.



Vine is a short-form video sharing service where users can share six-second-long looping video clips. The service was founded in June 2012, and American microblogging website Twitter acquired it in October 2012, just before its official launch. Users' videos are published through Vine's social network and can be shared on other services such as Facebook and Twitter. Vine's app can also be used to browse through videos posted by other users, along with groups of videos by theme, and trending, or popular, videos. While Vine enjoys the support of Twitter, it competes with others such as Instagram and Mobli. As of December 2015 Vine has 200 million active users.

A BBC review described collections of Vine videos to be "mesmerising", like "[watching a] bewildering carousel of six-second slices of ordinary life [roll] past."

Soon after its launch, Vine faced criticism for how it handled pornography; while porn is not forbidden by Twitter's guidelines, one sexually explicit clip was accidentally featured as an "Editor's Pick" in the Vine app as a result of "human error". Because pornographic content violates Apple's terms of service, the app's rating was changed to 17+ in February 2013 following a request by Apple.

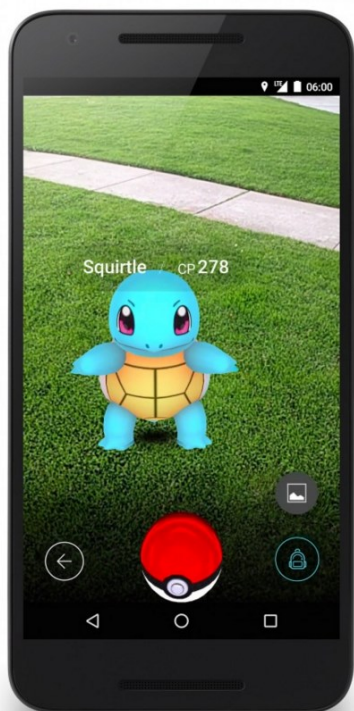




Pokémon Go is a free-to-play, location-based augmented reality game developed by Niantic for iOS and Android devices. It was initially released in selected countries in July 2016. In the game, players use a mobile device's GPS capability to locate, capture, battle, and train virtual creatures, called Pokémon, who appear on the screen as if they were in the same real-world location as the player. The game supports in-app purchases for additional in-game items.

The application can place users at risk of being targeted by criminals or injury due to being unaware of one's surroundings.

Since the launch of Pokémon Go in the United Kingdom, 290 police incidents have been reported to occur in England and Wales.



# Yik Yak

Yik Yak is a social media smartphone application. It is available for iOS and Android and it allows people pseudo-anonymously to create and view discussion threads within a 5-mile radius. It is similar to other anonymous sharing apps such as Nearby, but differs from others such as Whisper in that it is intended for sharing primarily with those in proximity to the user, potentially making it more intimate and relevant for people reading the posts. All users have the ability to contribute to the stream by writing, responding, and "voting up" or "voting down" yaks.

Yik Yak works by combining the technologies of GPS and instant messaging, allowing users to microblog to other nearby users. Before loading messages, the Yik Yak app determines the user's location and groups them into pockets of 1.5 mile (2.4 kilometre) radius zones. Within these zones, anyone inside the radius can post and read other people's "yaks". Yik Yak is effectively an online bulletin board.

One of the biggest criticisms of social media sites and applications is their inherent potential to feed the growing amount of cyber bullying. Due to the widespread bullying and harassment committed through Yik Yak, many schools have taken action to ban the app.

# What parents and carers need to know

CEOP have launched 'Nude Selfies: What Parents and Carers Need to Know'. It is a series of four short animated films for parents and carers offering advice on how to help keep their children safe from the risks associated with sharing nude and nearly nude images. The films can be seen at [www.youtube.com/ceop](http://www.youtube.com/ceop)



The films aim to help parents and carers:

- Understand young people's motivations for sending nude selfies.
- Plan to respond positively and constructively to an incident in which their child has shared a nude selfie.
- Gain confidence and skills in initiating preventative conversations.
- Identify risky behaviours or situations and know where to seek help.
- Know how to get help if a child is at risk after sharing an image.



The Nude Selfies films are accompanied by a guidance pack including a suggested session plan and practitioner guidance for delivering an effective workshop.

Further resources can be found at [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

# Information for parents

**Set boundaries for your child before they get their first 'connected device' (mobile, tablet, laptop or games console). Once they have it, it can be more difficult to change the way they use it or the settings.**

**You may be starting to think your child knows more about using technology than you do, and you may be right. Make it your business to keep up to date and discuss what you know with your child.**

**Review the settings on parental controls in line with your child's age and maturity and adjust them if appropriate. They may ask you to trust them sufficiently to turn them off completely, but think carefully before you do and agree in advance what is acceptable online behaviour.**

**Discuss with your child what is safe and appropriate to post and share online. Written comments, photos and videos all form part of their 'digital footprint' and could be seen by anyone and available on the internet forever, even if it is subsequently deleted.**

**Explain to your child that being online doesn't give them anonymity or protection, and that they shouldn't do anything online that they wouldn't do face-to-face.**

**Here are some questions you could discuss with your children:**

- Do you really know everybody on your 'friends' list?
- Do you know how to use and set privacy and security settings? Can you show me how?
- Do you ever get messages from strangers? If so, how do you handle them?
- Do you know anyone who has made plans to meet someone offline that they've only ever spoken to online?
- Has anyone at your school, or anyone else you know, taken naked or sexy photos and sent them to other people, or received photos like that?

# Tips for children

## Online Safety Plan

I will not give out personal information such as my address, telephone number, parents' work address/telephone number without my parents' permission.

I will tell my parents right away if I come across something that makes me feel uncomfortable.

I will never agree to get together with someone I "meet" online without first checking with my parents. If my parents agree to the meeting, I will be sure that it is in a public place and bring them along.

I will talk with my parents about posting pictures of myself or others online and not post any pictures that my parents consider to be inappropriate.

I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell my parents right away.

I will talk with my parents to set up rules for going online and using a mobile phone. We will decide on the time of day and length of time I can be online and appropriate areas for me to visit. I will not access other areas or break these rules without their permission.

I will not give out my passwords to anyone (even my best friends) other than my parents.

I will check with my parents before downloading or installing software or doing anything that could possibly hurt our computer or mobile device or jeopardize my family's privacy.

I will be a good online citizen and not do anything that hurts other people or is against the law.

I will help my parents understand how to have fun and learn things online and teach them things about the Internet, computers and other technology.

### Helpful Sites

CEOP, Think You Know – [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

Net Smartz Kids—[www.netsmartzkids.org](http://www.netsmartzkids.org)

NSPCC—[www.nspcc.org.uk](http://www.nspcc.org.uk)



**NSPCC**