Holy Trinity Catholic Media Arts College

Student Guide to staying safe online

With people posting and sharing every day, the digital world may appear to be a great way to share what you're doing with your friends. However, are they all really friends?

People can hold fake accounts, pretending to be someone they're not. This may seem scary but there are some things you can do. Safety on Facebook is very important, but do you really know how to stay safe using social networks?

First thing to do is **check your privacy settings** - making sure you know what you're showing to the general public. Some status updates and pictures could attract these 'fakers'. You can change this setting so only your friends can see, with just one click of your mouse.

Accounts can be hacked if you only have a weak password. **Make sure you have a strong password which contains numbers and letters**. If people get hold of your password, this can cause 'fakers' to pretend and write posts in your name. Changing your password often also helps.

Never agree to meet people that you've never met in real life. This could be dangerous, people are not always who they say they are. A 14 year-old boy could be somebody entirely different! To avoid this don't agree to meet up, no matter how good it may seem and always tell your parents!

Always protect your data. Criminals are most likely to hack websites when you enter a credit card number.

If you do buy a product online, then you should use a **'Single-Use' account** which is located on most websites. This is when your card details are deleted straight after payment. **Also avoid buying products from sites that you don't know**. Only buy products online from sites that you trust. Always remember that even if a site says 'secure' and starts with https: it means that it is harder to hack, but not impossible to hack.

Keep personal details safe! Details such as your full name, address, mobile number, email address, school name and friends full names secret. Otherwise people can use this information to contact you. Your passwords and nicknames should always be secret. If you have to give an online screen name or nickname, never use your real name, and try not to use things that are easy to guess like your parents name or the name of a pet.

When you send a text or photo message from your mobile, your phone number automatically goes with it. So think carefully, especially before sending photos of yourself or friends from your camera-phone. **It is best never to send photos at all** and remember – once any photo enters the digital world you cannot get it back! Remember- friends who are asking you to post ‘inappropriate pictures of yourself’ are not really friends at all.

Online gaming and technology has really moved on. You can send countless messages as you sit in your chair and play on your console. Also you can now download games so that they're ready to play as soon as you click 'download'. However not all downloads are completely safe - some may contain viruses, and not all messages will be friendly. Here's what to do if you receive a bad message or virus. Check the website that you have downloaded and research its history before you press 'download'. If it is the official webpage of the download, it should be ok, but you should always check. If unsure, avoid downloading.

Even on the internet bullying can occur. Posting an embarrassing or humiliating video of someone, harassing someone by sending messages or even setting up profiles on social networking sites can all examples of cyber bullying. Always let an adult know if you think you are being cyber bullied. No one especially children and teenagers should go through this. People seem so big over the internet. You don't really know who is out there or who is behind the profile or screen.

Talk to someone you trust. This could be a teacher, parent or friend. You may even have to change your email address if you're repeatedly bullied through email.

You can easily become a bully - stop and think before you write a message. If you receive a message, no matter how horrible the message - do not reply. That is what the bully wants. Instead block instant messages and emails. Ask a parent or teacher for help.

In terms of instant messaging, it is very easy to say something that you wouldn't say in real life. You can easily become a bully. Stop and think before you write a message. Think of the consequences.

PROCEDURE FOR STUDENTS

Remember if you are experiencing any form of Cyber bullying at School or know of anyone else who is, then please let your HOH or Form Tutor know.

Forms of Bullying

Verbal

Name-calling
Abuse e.g. racial, sexual
leasing/taunting Insults/blazing/
mocking
Offensive comments
Spreading rumours
Gossiping
Laughing
Threats
Criticising
Putdowns

Physical

Hitting/striking Kicking
Slapping
Taking/damaging
Belongings
Pushing
Tripping
Banging into people
Throwing things
Forced to do something
They do not want to e.g.
fight

Emotional or Relational

Encouraging others to ignore or avoid someone Ganging up on someone Isolating someone

Being unfriendly Giving dirty/nasty looks Body language, gestures Written notes/graffiti
Harassment or oppression
Abusive text messages or emails
Prank phone calls