Plymstock School

A parent guide to keeping a child safe online

Welcome to the digital world

Young people grow up in a technologically rich world. They are surrounded by ICT and use it extensively in school and out of school. ICT opens up a new world, a world that we should embrace and encourage. New technologies allow access to some of the most powerful communication, collaboration and research tools.

With the new opportunities that ICT brings there undoubtedly comes some risks. It is important that we make children aware of the risks and encourage them to adopt appropriate patterns of behaviour when using ICT.

Understanding the language used by your son/daughter online

One of the effects of Instant Messaging (IM), chatrooms and texting is that it has changed the way that people communicate with each other. A traditional text message has a maximum length of 160 characters and this led to a new generation of abbreviations and acronyms. Some of these are obvious, some are not so obvious.

Below are some of the most common examples:

NTHNG: Anything

RUOK: Are you OK?

R: Are

EZ: Easy

A?: Eh? (pardon)

XLNT: Excellent

THANQ: Thank you

LMAO: Laugh my ass off

ROFL: Rolling on the floor laughing

ASL: Age, Sex, Location

PMSL: Pee myself laughing

WTF: What the flip (or variations!)

POS: Parent over my shoulder

GR8: Great

L8R: Later

LOL: Laugh out loud

OMG: Oh my God!

SPK: Speak

BTW: By the way

KTHNX: OK thanks

Ten top tips for parents

1. Set up an account for each user on your PC at home and only give yourself administrator access. This will allow you to keep control of the settings and the installation of software. Each user account can be password protected.

2. Add a screensaver protected by a password to your account so that if you leave your pc for 5 minutes you will have to enter your password. You can do this in the 'Control Panel'.

3. Encourage your family to use technology in a public part of the

house and not in a bedroom. This applies not just to pcs but also to laptops, game consoles, Internet browsers on phones etc.

4. Remember that many consoles come with family settings. For example if you want to disable or limit 'Xbox Live' on an Xbox One you can do so by going to 'Settings, Parental controls'. There is also the option to add a mask to voices so that a youngster's voice sounds like that of an adult or even a robot.

5. Use a pop up blocker. Both Internet Explorer, Safari and Chrome come with their own pop-up blockers. If you are accessing a site that has a genuine pop up window that you need to access you should add it to the trusted sites rather than turn off the pop up blocker. The settings can be found in the 'Tools' menu of the browser.

6. Encourage your child not to open e-mails from unfamiliar e-mail addresses and to avoid opening suspicious attachments. As far as possible you should encourage your child to use the school's Learning Platform as this provides a safer environment.

7. Set your favourite search engine to do 'safe searches'. This will make sure that a search returns content suitable for all ages. For example, to set Google to do safe searches click on search settings on the homepage and then ensure that moderate or strict filtering is enabled.

8. Adjust the security settings of your browser and pc. For example, Apple Macs allow users to change settings in the parental control preference pane. Windows operating systems also have parental control sections.

9. Keep virus protection software up to date.

10. Add them as a friend on social networking (If they'll let you!)

Social networking safety

Social networking allows many of us to keep in contact with people and to share details and photos of what is happening in our lives.

Young people will have grown up surrounded by sites such as Facebook and Twitter. Social networking sites will undoubtedly play an important part in the lives of youngsters as they get older and we need to ensure that we give them simple guidance to ensure that they use them safely.

Five simple rules to discuss at home:

1. Adjust privacy settings – in Facebook you can select 'Settings, Privacy Settings, Profile'. This will allow you to restrict who sees information and prevents friends of friends seeing your posts and photos.

2. Think before you post – It is very easy to a post a comment or photo in anger or frustration. By the time you remove it many people will have seen it and the harm has been done.

3. Avoid posting images where possible – once posted, anyone can make a copy!

4. Only add people who you know in real life as friends. Remember that just because someone has a photo showing them as 15 year old in their profile they may be someone completely different (e.g. an adult).

5. Think carefully about how much personal information you put on your profile – you don't need to tell everyone your address, school, date of birth and mobile number.

6. Pay attention to age restrictions – for example Facebook is for people aged 13 and over.

7. If you suffer abusive comments online – don't retaliate! Save the conversation so action can be taken.