The Internet is a valuable resource of information and excellent tool for communicating with friends and family. However, the Internet can potentially be an unsafe place to be if you're not careful. Poultec Training Limited takes internet safety and security seriously and has produced the following guidance to help you stay safe on the internet:

Website Browsing

Search Engines - There's a lot of useful information on the Internet and locating it would be impossible without the use of search engines such as Google and Bing. As there's also a lot of harmful and inappropriate information on the Internet, here's how to not stumble across something you don't want.

> Be careful what you ask for - think what you could get from what you asked for, try to use specific search terms - searching for 'free images' can provide all kind of results including pornography.
>
> Always use search filtering - like Google's SafeSearch which remove results that are inappropriate - be aware however they are not always perfect.

Social Networking – Sites such as Facebook, Twitter, MySpace, Bebo and YouTube allow you to share online what you do in your everyday life. These sites allow you to add photos, videos and give people an insight to your life.

> Be Careful who you share with! Do you really know who you are sharing your online presence with? Have you made sure that you have only shared with known friends and family and not the whole world!

Online Banking - Accessing your bank accounts online is a great way to actively manage your money. Banks have many features to keep your details and money secure, however it is always important to remember that these are only as secure as the password that you use! Do not make passwords easy to guess, by using predictable words or phrases (see below for more information on password security).

If you're using a computer in a public place who's looking over your shoulder? If you're using a public or shared computer make sure you trust the owner of the computer and only ever connect to websites securely (look for that closed padlock).

Password Safety - Avoid using the same password across multiple websites - if someone knows your password they could access all of your online accounts.

> Do not use 'guessable' passwords - simple words, phrases or personal information can be easily guessed. Don't use passwords like 'password', '1234456' or 'letmein' – it is best practice to ensure passwords have a mix of uppercase and lowercase characters and numbers.
>
> Never write down your password - if you have to write it down make sure they are kept very securely so no one can easily access it.

Make sure you keep your password recovery details are up-to-date, so if you do need to reset your password you can be contacted easily. Generally these features e-mail a new randomly generated password to your defined e-mail address.

E-mail and Instant Messaging

Phishing - Phishing is when you receive an e-mail message claiming to be from your bank, PayPal, eBay or similar and you are asked to go to the website and sign in. These e-mails are not from your bank but someone else trying to steal your log-in details by directing you to a fake website that looks like the website of the organisation where the e-mail appeared to have originated from. Here are some steps to avoid being caught by phishing scams:

Your bank will not send you e-mails asking you to log-in - they may offer you a special offer, or tell you about new products, but they will not ask you to sign in.

Never use the link in the e-mail - the phishers make the link look legitimate but it goes to their fake site: always type the web address into your web browser to ensure you're going to the legitimate website.

Chatting - Whether you're using a forum, chat room or instant messaging software, such as Windows Messenger or Google Talk, make sure you know who you're talking to and remember:

Never agree to meet someone you met online - you have no idea who they really are.

Never give out any personal details – you may not be talking to the person you thought you were.

Avoid using your real name - so you can protect your real identity by using a nickname.

Viruses - You can get viruses by opening infected e-mail attachments - here's how to know which ones to open:

Never open an e-mail attachment from someone you don't know - you have no idea what it contains.

Never open an attachment from someone you know but weren't expecting - viruses can pretend to be someone you know and send e-mails from them.

Ensure that you have installed Antivirus software and that it is up-to-date. Updates are normally automatically downloaded and installed, but you should also check periodically.

Other Sources of Help

Think U Know

Child Exploitation and Online Protection Centre

Official Google Blog Security Series