

Be **WISE**

Always ask yourself, **Why** a website or someone you make friends with on the Internet would need your personal information. Remember our safeguarding cautions are about your personal safety, online identity and exposure to extremist views and opinions.

Be **Inspired**. The Internet offers great tools for research, learning, discovering and creating.

Be **Secure**. There are constantly new scams, hoaxes, viruses and spyware on the Internet. Install security software to keep your computer and data safe.

Evaluate the stuff you read, see or receive through the Internet. Just because it's on the Internet does not make it true, reliable or genuine.

BE **SMART**

Keep **Safe** by being careful not to give out your personal information - such as your name, email, phone number, address, College name, any Bank details, PIN numbers or passwords - to people online.

Meeting someone you have only been in touch with online can be dangerous – Tell an adult and **Don't** do it alone!

Accepting emails, messages on IM or opening files, pictures or texts from people you don't know or trust can lead to problems.

Reliable? Someone online may be lying to you about who they are.

Tell your parent or trainer immediately, if someone or something on-line makes you feel uncomfortable or worried.

Staying Safe on Social Networks and Instant Messenger

Do you know everyone on your buddy or contacts list? Think carefully about who is on your list, people on Instant Messenger and chat like Apps, may not be who they say they are, so a friend of a friend is not necessarily a friend!

Keep your personal information private when talking to someone you don't know in the real world. Also think about what visible information you have in your Profile or Member directory, for example.

Learn how to keep an archive/save a copy of your conversation, and don't be afraid to tell someone you are saving your conversation with them.

Learn how to block, ignore and report people. Report anything that makes you feel uncomfortable; if it doesn't feel right, it probably isn't.

Check you know how, to report something you feel uncomfortable about to the Messenger or Social Networking provider or use the CEOP 'Report Abuse' button on tpm's website pages.

Use a nickname, not your real name, and a nickname that is not going to attract the wrong type of attention.

Keep your username and password private, and change your password on a regular basis.

Don't reply to abusive messages. Don't send abusive messages either. It's best not to say anything on IM or a Social Network that you wouldn't say to someone's face.

Don't accept messages from people you don't know.

Meeting someone you have only been in touch with online can be very dangerous. If you feel that you 'have to' meet, then for your own safety you **must tell your parent or carer** and take them with you – at least on the first visit – and meet in a public place in daytime.

Don't pass the buck - if someone you have accepted on your buddy or contacts list is acting weird; don't pass them on to a friend. You could be putting your friend at risk. Just block them and report them to an adult, Parent or carer.

IMPORTANT NOTICE:

In relation to the General Data Protection Regulations it is imperative that any personal data should not be disclosed to anyone who does not have the appropriate authority to receive such information, irrespective of their seniority or relationship to you.