Social media – think before you post!

In recent years, the use of social networking has become the cornerstone of modern communication. But don't forget that what you post online could have real life consequences.

Most of us enjoy sharing personal news and views with friends, family and colleagues via platforms such as Facebook, Twitter, Instagram, LinkedIn, and more.

But while there are many benefits to using social media, it is important to **think before posting** – particularly in light of the ever increasing threat of identity theft.

Who else might be viewing your posts?

Social media allows us to publish to a potentially world-wide audience. Don't forget that such an audience includes spam bots and criminals, who will do just about anything to get their hands on our personal details. What you post online could have real life consequences.

It is important that we protect our personal information from potential misuse by others.

How to maintain your privacy online

Here are our top tips for using social media safely.

What have you agreed to?

Make sure you read and understand the **Terms, Conditions and legalities**.

- Remember that these will be updated change regularly. Have you checked them recently?
- How will the platform treat your intellectual property?

What can others find out about you?

Don't overshare. Make sure you understand the **Privacy Settings** and how they can be set to best protect you.

- Keep personal information about yourself (e.g. full name, address, date of birth) to yourself.

- Check your location settings. Turn them off if you don't want to share your location with everyone.
- Think twice about the images you post. For example, images of valuables, gifts or new acquisitions may advertise to criminals much more than your good fortune!

Are you aware of the risks of using public Wi-Fi?

- Eavesdropping internet traffic in public places has become commonplace. Criminals may listen in to everything you are doing online, including capturing your login credentials.
- Beware fake hotspots that appear to be legitimate. Avoid any whose name contains the word 'Free', or that are unencrypted.
- Always make sure you log out of a site when you are finished.
- Use two-factor authentication to protect yourself and set up login alerts where they are available.

Any other tips?

- Be wary of clicking links in posts, even if they have come from a friend. They may link to viruses or other malicious content.
- Avoid linking social media accounts. For example, an app might invite you to log in using another app, rather than create a new account. This may result in your information being shared without your knowledge.
- Stay away from online questionnaires. Many of these are designed to get you to divulge personal information.