The Dangers of Social Media when Applying for Jobs.

Social Media is a huge and growing phenomenon, with people of all age groups accessing Facebook, Twitter, LinkedIn, Youtube etc. With this brings some potential dangers which are important to consider when using social media.

Social Profile – LinkedIn, Facebook and Twitter are extremely popular networking sites that are used by professionals in employment and job seekers alike. While they are great avenues to use when job searching, one important thing to remember is what is posted on any social media site whether it be Facebook, Twitter or LinkedIn **can be seen by any potential employer**. Social Profiles can help you land or lose that job! 92% of companies use social media for recruiting and to conduct their own background checks to verify a candidates' suitability as a "fit" for their company. Therefore your profile matters more than ever. Companies hiring react most negatively to references in posts to drugs and alcohol, posts of a sexual nature, profanities and spelling and grammar errors. Content that recruiters want to see include memberships in professional organisations and volunteering with charities. Content to post/tweet with caution include items of a political or religious nature. A key point to remember before posting items online is not to leave yourself open to professional scrutiny with questionable content. Always make sure your privacy settings protect sensitive content so that recruiters see only the public information you want them to see. **When in doubt, leave it out!**

Security – there are some "phishing" scammers on social media sites who may attempt to acquire personal information such as usernames, passwords and credit card details by masquerading as a trustworthy entity. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. These websites can be set up to appear like your legitimate social media website in order to steal your password and social media identity. It often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Once someone has your password, they can use it to destroy your profile or send out spam messages and viruses which could do irreparable damage to your online reputation.

Privacy – Many people upload photos or video clips to social networking sites like Facebook or Youtube, however it is a grey area as to who owns the copyright to the material uploaded. There

is potential for private information to be shared with third parties who could have access to your information.