TIPS FOR PROFESSIONALS

- Remember the billboard test, if you wouldn't put the content on a huge billboard next to your name, face and the company name don't let it exist in digital format.
- In the digital age you are a representative of your company 24 hours a day, 7 days a week.
- The tattoo effect of the digital content.
- Don't air grievances regarding your company, your boss, other employees or clients online.
- Don't violate the privacy of clients or colleagues on social media.
- Remember that all the confidentiality obligations in your contract apply to social media too.
- Do not use the company name or logo on your personal social media accounts, webpages and blogs or as your handle or username.
- Don't talk on behalf of your company- there are people in your company authorised to do this.
- Beware the work WhatsApp group – use the group for work-related content only and be respectful of your colleagues' time by not messaging around the clock.
- Remember that you are responsible not only for the content that you post, but also the content that you share, retweet, like and are tagged in.
- Turn on two-factor authentication for all accounts
- Download your Instagram history and activity data – Tap on your profile – access 'settings' at the bottom right of your screen – go to 'security' and tap 'download data'.

GUIDELINES FOR WORK WHATSAPP GROUPS

The Company recognises that many Employees are part of WhatsApp groups which have been established for the sole purpose of providing a communication channel amongst employees and contractors of The Company (the "Groups"). The following guidelines are to be followed when engaging in any communication on the Groups.

1.1 **Relevant content only**: Try to keep the content relevant to your colleagues. In certain cases, it will be relevant to discuss current affairs or social issues on these groups, it be careful not to waste your colleagues' time. Advertising, political endorsements, and other non-related topics are prohibited on these groups, unless otherwise approved in advance by the Group administrator.

1.2 **Only respond if necessary**: Do not reply for the sake of replying. If a message does not require a response, please do not respond. The volume of messages on the Groups can become overwhelming. You do not need to acknowledge receipt unless specifically asked to do so. Comment only when your information adds value.

1.3 **Long conversations, especially if only involving a few members of the Group, are to be taken off the Group**, unless it is the purpose of the group.

1.4 **Membership on these Groups is part of your job.** You have been made a member of these Groups/this Group for the purpose of information sharing. As the

information shared may be relevant to your job deliverables, you may not leave these Groups/this Group without specific approval from your manager.

1.5 **The content shared on these Groups is for the members of these Groups only and shall not be shared with any third party**. These chats are confidential, may be legally privileged and are solely for the intended addressees. Disclosure, copying (e.g. by screenshot) or distribution of these chats to unintended recipients is prohibited.

1.6 **Try to avoid "after hours" communication on the Groups** - Appreciate that everyone needs some down time from social media. Please try to be respectful of your colleagues and refrain from communicating on the Groups before 6am and after 8pm, [confirm or alter as appropriate], save for cases of extreme emergency.

1.7 **Practise good digital hygiene on any device on which the Groups are used -** The Groups are often used to discuss confidential client or business information. Any member of a Group must take the following measures to ensure that this content remains secure:

1.7.1 Ensure that all devices on which the Groups are accessed are password-protected; and

1.7.2 Periodically deleting content on the request of the Group administrator.

PARENT TIPS:

- Childhood 2.0 on YouTube: https://youtu.be/He3IJJhFy-I
- The Social Dilemma on Netflix
- ALL devices out of the bedroom at a fixed time every night
- No social media until high school
- Agree on a time budget with your children – how many hours a day on your device is reasonable. Set those time limits on the device
- Learn more about the websites, games and apps that your children are using. Have a look at the ultimate parent guides released by Common Sense Media here https://www.commonsensemedia.org/parents-ultimate-guides or Bark here https://www.bark.us/blog/streaming-sites-safety-kids/
- Open discussion – benefits and risks, what are your friends doing online, why do you want it, what would you do on it
- Remember the Billboard test
- Have a Smartphone contract with your child https://www.thedigitallawco.com/parents/smartphone-contract-teenagers/
- Turn off location services on social media apps
- Install parental control software – for high risk children have a look at Bark, Qustodio or Our Pact – otherwise Google Family Link on Android

https://www.thedigitallawco.com/smartphones/googles-family-link-app-everything-parents-need-to-know/ or Screentime on Apple https://www.thedigitallawco.com/parents/apples-screen-time-app-everything-parents-need-to-know/ are free and comprehensive
- Set up some ground rules for the sharing of personal information
- Children must beware of anyone they don't know trying to join their network of friends – presume everyone they meet online is dodgy until proven otherwise
- Consider your child's privacy when posting photos
- Work with your child in setting up their social media accounts. Make sure that they have activated all privacy settings and do not include their date of birth
- Install filtering software on the WiFi at home. Turn off WiFi at night.
- Install tracking software (Life 360 or free on most smartphones)
- Model good phone behavior
- Media-free times and locations at home
- **Regular check-ins and conversations**

TIPS FOR SPOTTING FAKE NEWS

Presume everything you receive is fake until you can prove that it is true
Interrogate content before you share it:
- What is the source? If there is no source, don't share it. If a voice note – does the person identify themselves? Have you googled the person?
- Is the source credible? Have you been to the social media pages of the alleged source?
- Does the link look legit? eg. ccn instead of cnn
- Does this content make you very happy, scared or angry? Red flag! Think about why the information might have been created and shared. Political forces are at work!
- Compare info against info from trusted and official sources - Are the main news sites covering the story?

ZOOM TIPS

- Never use your personal meeting ID
- Each Zoom user has a personal meeting ID—think of it as your Zoom phone number. When creating a meeting, you can use your personal ID or generate a random one, and you should always generate a random meeting ID.
- Always use a meeting password
- Use Zoom's waiting room feature
- Mute audio and disable video for meeting attendees
- Turn off screen sharing for everyone but the meeting host/co host