

SAFER SOCIAL NETWORKING

1. KEEP PERSONAL INFORMATION TO A MINIMUM

- Don't put your full date of birth (you can leave out the year).
- Don't include your home/work/school address – your friends already know these details.
- Think before publicly accepting invitations to events – it can let people you might want to avoid know where you will be.

2. NO MOBILE PHONE DETAILS

- Don't put your mobile phone number on your profile, your friends and family already have it.

3. NO IDENTIFYING INFORMATION

- Keep information about your private life including school, work place, club memberships and your location to a minimum.

4. KEEP YOUR PASSWORDS PRIVATE

- Your best friend does not need to know your passwords to anything.
- If you share your password others can pretend to be you online.
- Make your password hard to guess – use a mixture of letters, numbers and symbols.

5. USE A GENERIC AND NON IDENTIFYING EMAIL ADDRESS

- Your friends and family already know your full name.
- Using your name in your email address give online 'friends' and 'contacts' access to more information about you than you may want.



6. CHECK YOUR PROFILES REGULARLY

- Check what others have posted or written on your profile, inappropriate or content you think is offensive may be posted on your profile.
- Check you are happy with everything on your profile and delete anything you don't like.
- Block anyone who posts inappropriate or offensive content.

7. LOCK YOUR PROFILE AND PHOTO ALBUMS

- Don't let people you don't know or trust have access to your photos – remember everything posted on any website can be copied, emailed and saved.

8. THINK BEFORE POSTING PHOTOS

- Think about what and who are in any photos you post.
- Try and have no identifying information in photos such as school uniforms or sporting team uniforms.
- Remember what you post today may haunt you tomorrow - potential employers often check social networking profiles.

9. ALWAYS GET PERMISSION BEFORE PUTTING A PERSON'S PHOTO ONLINE

- Never post a photo of a person anywhere online without their permission, it is an invasion of their privacy.
- If a person asks you to remove a photo make sure you do.

Digital Footprint

Evidence of a computer user's activity online and offline

Cyberstalking

Repeated, intense harassment and/or abuse that may include threats and can create fear

Harassment

The repeated sending of abusive, threatening and insulting messages

Impersonation

Posting or sending material online, whilst pretending to be someone else

USEFUL WEBSITES

Stay Smart Online

www.staysmartonline.gov.au

Net Alert

www.netalert.gov.au

Net Safe

www.netsafe.org.nz

Bullying No Way

www.bullyingnoway.com.au

Virtual Global Taskforce

www.virtualglobaltaskforce.com

Australian Communication & Media Authority

www.acma.gov.au

Internet Industry Association

Security Patrol

www.security.iaa.net.au

Centre for Safe and Responsible Internet Use

www.cyberbully.org

10. REPORT ABUSE

- Report and abuse, harassment, bullying or inappropriate content to the website, and if necessary your school and the police.
- If you become aware of any friends or relatives who are having problems with harassment, bullying or inappropriate content being placed online, report it.
- Schools and the Police take online abuse, bullying and harassment very seriously.

