

Middle secondary unit

Managing online safety



Creative Commons

These teaching resources on the Cybersmart website's Schools Gateway are now available to schools under Creative Commons licences.

The new licensing conditions are more flexible than existing copyright, enabling schools and teachers to use, adapt and re-publish material from the resource, without seeking permission to republish from the ACMA.

These materials have been licensed under an attribution non-commercial share alike licences (BY-NC-SA). Under these licences, the materials are available for free use and adaptation so teachers can change, translate and share new creations with other teachers and students.

Copyright Notice

Source: © Commonwealth of Australia 2011



This work is based on materials that constitute copyright of the Commonwealth of Australia and is licensed under a Creative Commons Attribution Non-Commercial Share Alike 2.5 Australia Licence.

Disclaimer: The ACMA has taken reasonable care to ensure the information in this work is correct and accurate at the time of publication. However, the ACMA makes no warranties regarding the correctness of the information at later dates, and disclaims liability for damages resulting from its use. The ACMA recommends that users exercise their own independent skill and judgment when using this work and carefully evaluate the accuracy, currency, completeness and relevance of the material for their purposes.

The ACMA requests that if you republish this work, you notify the ACMA by email at: cybersafety@acma.gov.au including a link to the republished work. This is to assist us in tracking the uptake of our works and the innovative uses that our licensees are making of our works.

See: <http://www.cybersmart.gov.au/Legal/Copyright.aspx> for more information.

Before you start

This unit is designed for students aged 14–15 years.

Before you start this unit it is important that you are aware of what your students, and others in this age group, are doing online and how they use online technologies. For some general information visit the 'What are students doing online?' section at www.cybersmart.gov.au/schools.aspx.

This section provides information on children and technology, including cybercitizen profiles, videos of students discussing their online activities and links to ACMA research regarding online behaviour.

Teacher background information

When engaging in online activities, young people can share information with friends and strangers from all over the world. While there are many benefits in online communication, there are also risks. If young people are to have positive Internet experiences, it is important that they develop protective behaviours to safeguard themselves, their friends and their families while engaging with others online. These behaviours include protecting personal information, identifying when they feel unsafe, identifying risky online behaviour and recognising and reporting grooming tactics.

This unit covers the following separate, but related topics:

- Understanding digital reputations (activities 1 to 3)
- Online privacy (activities 4 and 5)
- Keeping yourself safe (activities 6 to 8)
- Managing unwanted contact (activities 9 to 11)
- Responsible cybercitizenship (activity 12)

Each topic can be taught individually or the five topics can be taught as a complete unit.

This unit contains several videos which may be disturbing or unsuitable for some students. It is important to view all videos before allowing your students to watch them.

Unit overview and objectives

This unit aims to help students to:

- increase their understanding of the risks to personal safety when interacting online
- learn how to manage the risks of interacting with others online
- increase their understanding of how to implement the protective behaviours required to interact safely online.

By the end of this unit, students will be able to:

- list the risks involved with social networking, and detail strategies to better manage those risks
- acknowledge that it is difficult to remove or retract content once it is posted online
- recognise that others may use 'grooming' strategies to build relationships with young people
- identify the indicators of grooming behaviour
- apply strategies to help protect themselves and their peers online

Unit duration

This unit comprises five separate topics with a total of 12 activities. Each activity is designed to take approximately one or two 45 minute lessons.

Required resources

- Worksheets 1–3
- www.privacy.gov.au
- Interactive whiteboard and computers with Internet access
- ‘Profile Penalty’ video at www.nsteens.org
- ‘Offline Consequences’ video at www.nsteens.org
- Access to students’ social networking profiles
- ‘Your Privacy is Important. Think before you upload!’ animation at www.privacy.gov.au
- ‘private i – Your ultimate privacy survival guide’ magazine at www.privacy.gov.au (may require several printed copies of this magazine)
- ‘Tracking Teresa’ video at www.netsmartz.org
- ‘Stalking Sarah’ video at www.cybersmart.gov.au/wiseuptoit
- ‘Jeremy’s Friend’ video at www.cybersmart.gov.au/wiseuptoit
- ‘Clare thought she knew’ or ‘Matt thought he knew’ videos at www.youtube.com

Further information

For more information, contact:

Australian Communications and Media Authority
Cybersafety Contact Centre

Tel: 1800 880 176

Email: cybersafety@acma.gov.au

www.cybersmart.gov.au

Activity 1: Understanding digital reputations—part 1

What you will need:

- Worksheet 1: Social networking—what do I know?
- www.privacy.gov.au
- Interactive whiteboard and computers with Internet access

Ask students what they already know about online social networking.

Students to work individually to answer the questions on worksheet 1. When the students are finished discuss their responses. To find the answers go to:

www.privacy.gov.au > FAQs > Your Privacy Rights
FAQs > Social Networking.

Activity 2: Understanding digital reputations—part 2

What you will need:

- Interactive whiteboard and computers with Internet access
- ‘Profile Penalty’ video at www.nsteens.org
- ‘Offline Consequences’ video at www.nsteens.org
- Access to students’ social networking profiles

Ask students what they think is meant by the term ‘digital reputation’? Share or record ideas.

Watch ‘Profile Penalty’. This video demonstrates the importance of considering what sort of information is posted on social networking profiles and how that information impacts on digital and real-life reputations.

It can be found at www.nsteens.org > Videos > Profile Penalty.

After watching discuss the following:

- What did Tad’s original profile say about him?
- Why do you think Tad changed his profile?
- Do you think recruiters would look at a student’s social networking page?
- Who can see the information you post on your profile or page?
- Can you guarantee complete privacy when you post things online? Why or why not?
- When Tad removes the items from his profile and page are they really gone? Why or why not?

Watch and discuss ‘Offline Consequences’ at www.nsteens.org > Videos > Teens Talkback > Offline Consequences.

Ask students to think about their own digital reputation. Do they have a social networking profile? What does it say about them? Students to critically analyse their own page (or a friend’s page if they feel comfortable doing so) and write down what someone who doesn’t know them might think they are like after reading/viewing the information on the page.

Discuss: ‘If you applied for a job and the potential employer had access to your site, do you think they would hire you’? Why or why not?

Alternative activity

Students who do not have a social networking page could create a mock page, taking into consideration what it says about them to friends, acquaintances and potential employers.

Activity 3: Understanding digital reputations—part 3

Students, individually or in small groups, assume one of the following roles:

- an up-and-coming garage band
- an author with a new novel to promote
- an artist
- an aspiring singer or actor
- a young independent politician

Students to consider what information they would include on a social networking profile/page to promote themselves to the general public.

Students to create a mock social networking profile/page for their assumed role. While doing so they need to consider:

- the target audience (i.e. who do they want to see the profile/page)
- the information they want the target audience to have
- how they will ensure that the information provided doesn't give away their personal information (this may include setting up a separate email address for promotion purposes only)
- how to protect themselves from unwanted contacts such as stalkers and scammers.

Students can use computer software to design their page.

Students to present their profile/page to the class to enable fellow students to openly discuss the pros and cons of each proposed social networking profile/page. Students should focus on the potential risks to safety. Students should formulate strategies to address any identified risks.

Activity 4: Online privacy— part 1

What you will need:

- ‘Your Privacy is Important. Think before you upload!’ animation at www.privacy.gov.au
- Interactive whiteboard (or several computers) with Internet access

Watch ‘Your Privacy is Important. Think before you upload!’ at www.privacy.gov.au > Privacy topics > Youth > Your Privacy is Important. Think before you upload!

Ask students to list the key messages the video contains. Ask students to think about a photo they have taken and posted, but now think should not have been shared. Discuss whether they can do anything about it once it has been posted.

Students to work in small groups to write a script for a television commercial designed to educate younger students about the potential dangers of posting photos online. Students can record the commercials and/or perform them to the class or at an assembly.

Activity 5: Online privacy— part 2

What you will need:

- ‘private i – Your ultimate privacy survival guide’ magazine at www.privacy.gov.au
- Several computers with Internet access or printed copies of ‘private i – Your ultimate privacy survival guide’ magazine

Separate students into pairs or small groups. Provide each group with access to (or a copy of) ‘private i – Your ultimate privacy survival guide’ magazine. This can be found at www.privacy.gov.au > Privacy topics > Youth.

Allocate each pair (or group) specific articles from the magazine to read. Students will provide a summary of the article/s to the rest of the class.

Activity 6: Keeping yourself safe—part 1

What you will need:

- Worksheet 2: Profile audit
- ‘Tracking Teresa’ video at www.netsmartz.org
- Interactive whiteboard (or several computers) with Internet access

Students to complete worksheet 2 and then share their audits with the class. Do students think that the level of information they are currently posting is ok?

As a class watch ‘Tracking Teresa’ found at www.netsmartz.org > teens > Real-Life stories watch online > Tracking Teresa.

This video demonstrates how easy it can be to find out information about someone, even though they think they are being careful about what they post.

Discuss the following:

- What clues does Teresa leave?
- Do you think Teresa meant to leave clues that would expose her to danger?
- Who has access to these types of clues?
- How do the clues expose Teresa to danger?
- This video is set in the U.S. and is aimed at helping parents to protect their children. Do you think the same clues could be used to track a young person in Australia? What about on social networking sites?

Watch the video a second time and ask students to highlight, on their completed copy of worksheet 2, the types of information that Teresa posted online (e.g. email address, likes etc.). Ask students if they are sharing more or less information than Teresa. Discuss how students are feeling about the information they are sharing, after viewing the video.

Have students work with a partner to assess the level of risk their social networking profile poses to their safety, including the posting of party details, details of holidays (advertising a vacant house to thieves), details of where they will be spending their day (advertising whereabouts to stalkers). Students to report back to the class about their identified level of risk and any changes in behaviour they are likely to make when posting information online.

Activity 7: Keeping yourself safe—part 2

What you will need:

- ‘Stalking Sarah’ video at www.cybersmart.gov.au/wisepuptoit
- ‘Jeremy’s Friend’ video at www.cybersmart.gov.au/wisepuptoit
- Interactive whiteboard (or several computers) with Internet access

Reflect on the video from activity 6. Ask students to share what consequences they think might arise from sharing too much personal information online. If students feel comfortable about doing so, they can share personal stories.

Ask students who uses online chat forums. Discuss which ones and whom they chat to (e.g. family, friends and/or strangers). Explain that you will be watching two videos that present real-life examples of what can happen when someone is not cautious enough when chatting with strangers, or sharing their personal information.

Watch ‘Stalking Sarah’ at www.cybersmart.gov.au/wisepuptoit > Resources > Stalking Sarah.

Then watch ‘Jeremy’s Friend’ at www.cybersmart.gov.au/wisepuptoit > Resources > Jeremy’s Friend.

After watching the videos students form small groups to discuss the following:

- How do you think Sarah felt when the man she met online began harassing her?
- What did Sarah do to try to stop the man from contacting her?
- Why do you think Jeremy spent so much time playing games online?
- What strategies did their online ‘friends’ use to gain Sarah and Jeremy’s trust?
- What mistakes did Sarah and Jeremy make in the use of online games and chat rooms?
- What positive strategies did the videos provide for dealing with unwanted contact?
- What information can people find out about you online?
- Would it be easy for a stranger to contact you?

- What information do you need to remove or modify to improve your online safety?
- What will you do in the future to ensure that this sort of situation does not happen to you?

Share responses with the class.

Introduce the term ‘grooming’ to students. Ask students what they think it means.

Online grooming is what occurs when an adult takes deliberate actions to befriend and establish an emotional connection with a child or teenager in order to lower the child’s inhibitions, with the intent of later having closer contact with that child/teenager. It may include situations in which adults pose as children in chat rooms or social networking sites, or where adults provide emotional comfort or support to vulnerable children/teenagers.

As a class list the ‘grooming’ techniques that were used in ‘Stalking Sarah’ and ‘Jeremy’s Friend’. Ask students what other techniques they think people might use to befriend children or teenagers. Ask students to think about what strategies would work on them.

Important

The videos used in this activity contain themes that may be disturbing or unsuitable for some students. It may be necessary to seek the permission of a parent/guardian before viewing them.

Activity 8: Keeping yourself safe—part 3 (assessment opportunity)

Revisit the term ‘grooming’. What does it mean and what are some examples of ‘grooming’ techniques that might be used to build relationships with young people?

Examples include:

- telling the young person they are special, attractive and intelligent
- making the young person feel ‘grown-up’ and respected
- suggesting they can get the young person a job in modelling or acting
- telling the young person they are in love with them
- seeking to isolate the young person from supports by suggesting that they are the only ones who truly understand and care for the young person
- providing virtual or real gifts to the young person
- encouraging the young person to have private conversations
- escalating contact by phone and potentially requesting a meeting in person
- encouraging the young person to provide images of themselves or to communicate using a webcam
- as the relationship progresses, they may use more forceful coercion to encourage the young person to provide images or to meet in person.

Students to work in small groups to come up with some concepts to promote messages about grooming, including the risks, identifying the warning signs, and defining and implementing strategies to protect teenagers from grooming (for further information see ‘Tips for dealing with unwanted contact’).

Students to develop a creative advertising ‘pitch’ to promote messages about grooming, the signs, how to avoid it and how to protect friends.

The advertising pitch could be presented as short video advertisements or plays, but must include the development of a script with the key messages integrated and explanations about why their advertisement would appeal to teenagers. Alternatively they might develop a song, poster or webpage promoting the key messages.

A panel of three students will debate the merits of each ‘pitch’, considering how effectively key messages are delivered and the likely impact on the target audience of teenagers. One student should be the panel moderator to ensure that comments remain constructive.

Tips for dealing with unwanted contact:

- tell the person you feel uncomfortable and ask them to stop (they may not have realised their behaviour was upsetting you)
- save the person’s details, including their username, the messages they have sent and the date and time they were sent
- block them if they continue
- report the unwanted contact to a teacher, parent/guardian, older sibling or other trusted adult
- changing email address or other contact details
- report the contact to agencies such as the Australian Communications and Media Authority (ACMA) or the Australian Federal Police
- contact your Internet Service Provider (ISP).

Activity 9: Managing unwanted contact—part 1

What you will need:

- ‘Clare thought she knew’ or ‘Matt thought he knew’ videos at www.youtube.com
- Interactive whiteboard (or several computers) with Internet access

Explain that you will be watching a video about a young person who forms an online relationship with someone they don't know. The online relationship quickly develops into a real-life relationship and puts the young person at risk.

Depending on the knowledge of your students, it might be necessary to explore the topic of grooming (in activities 6, 7 and 8) before beginning this activity.

Watch ‘Clare thought she knew’ or ‘Matt thought he knew’. These videos can be found by searching for ‘Clare thought she knew’ or ‘Matt thought he knew’ on www.youtube.com

‘Clare thought she knew’ and ‘Matt thought he knew’ essentially cover the same topics, but one has a young girl as the main character and the other a young boy. Select the video that is most suitable for your students.

After viewing the video discuss the following:

- How old do you think Clare/Matt is?
- What sort of person do you think she/he is? Why?
- How do you think Clare/Matt was feeling about her/his life before this incident? Why?
- What danger signs were there that should have alerted Clare/Matt to the fact that the online relationship could be dangerous?
- What grooming strategies did the online ‘friend’ use to build his/her relationship with Clare/Matt?
- Do you think anyone is vulnerable to grooming tactics, or only a certain type of person? Why?
- Does the danger of grooming affect girls and boys equally?
- If a person feels vulnerable, sad, frightened or lonely who are some real-life people who might be able to help?
- What can young people do to avoid being deceived in this way? List some strategies. (See activity 11 for some suggestions.)

Important

The videos used in this activity contain themes that may be disturbing or unsuitable for some students. It may be necessary to seek the permission of a parent/guardian before viewing them.

Activity 10: Managing unwanted contact—part 2

What you will need:

- ‘Clare thought she knew’ or ‘Matt thought he knew’ videos at www.youtube.com
- Interactive whiteboard (or several computers) with Internet access

View ‘Clare thought she knew’ or ‘Matt thought he knew’ a second time and list the steps that Clare took to regain control of her life. The videos can be found by searching for ‘Clare thought she knew’ or ‘Matt thought he knew’ on www.youtube.com

After viewing the video use the ‘fishbowl’ technique to discuss the following:

- How were Clare/Matt supported by family or friends?
- What did Clare/Matt do to manage the situation?
- How could you support a friend in this situation?
- Who are the people available to help us should something like this occur?
- Would you involve adults if you needed help?
- Would you involve adults if you thought a friend needed help? Why or why not? If yes, then who?
- Do you think reporting concerns about the behaviour of strangers online is a good idea?
- Whom would you report concerns to (see activity 11 for some suggestions)? What would prevent you from reporting concerns to parents or another trusted adult?

The ‘fishbowl’ technique involves selecting a group of (four to five) students to be seated in a small circle in the centre of the classroom. All the other students sit in a larger circle around the fishbowl group. The fishbowl group starts the discussion and is observed in silence by the outer group. Once a participant has made two or three contributions to the discussion they can select a classmate from the outer circle to take their place in the fishbowl.

Activity 11: Managing unwanted contact—part 3 (assessment opportunity)

Students to work in small groups to use the knowledge they have gained through watching and discussing the videos to formulate a list of strategies that could be used to avoid, manage or deal with unwanted contact.

Students develop a presentation about managing unwanted contact, which will be presented to a group of younger students. The presentation must include a hard copy resource for the younger students to keep that lists the strategies they can use and the contact details of agencies that can help them manage unwanted contact. The resource could take the form of a poster, brochure, mouse mat, or booklet—be creative.

Tips for dealing with unwanted contact:

- tell the person you feel uncomfortable and ask them to stop (they may not have realised their behaviour was upsetting you)
- save the person's details, including their username, the messages they have sent and the date and time they were sent
- block them if they continue
- report the unwanted contact to a teacher, parent/guardian, older sibling or other trusted adult
- changing email address or other contact details
- report the contact to agencies such as the Australian Communications and Media Authority (ACMA) or the Australian Federal Police
- contact your Internet Service Provider (ISP).

Activity 12: Responsible cybercitizenship

What you will need:

- Worksheet 3: Internet use contract

Provide each student with a copy of worksheet 3. Explain that students will need to sign this contract if they wish to continue using the Internet during school hours and at home. Read the contract and ask students how they feel about signing it.

Do students think the contract is realistic? Are the guidelines achievable? What would need to be changed for them to feel comfortable about signing it?

Students to work in small groups to write a contract that they think young people would be happy to sign. Worksheet 3 provides some guidelines for students to follow. Once the contract is written, the groups are to create a website/page that promotes responsible cybercitizenship. The websites/pages could be uploaded to the school's intranet.



Worksheet 1: Social networking—what do I know?

Name: _____

Use your current knowledge about online social networking to answer the following questions:

1. What are social networking sites?

2. Are there any privacy risks associated with using social networking sites?

3. Do I have rights under the Privacy Act when I use social networking sites?

4. I have a privacy-related complaint about a social networking site. Who can I complain to?

5. Are organisations allowed to use the personal information I post on social networking sites?



Worksheet 1: Social networking—what do I know?

Name: _____

6. How long does my information stay on social networking sites?

7. What can I do to protect my privacy when using social networking sites?

8. What can I do if someone posts information about me on a social networking site that I want removed?

9. What can I do if I'm being threatened, harassed or defamed online?

10. Where can I go for more help?

Worksheet 2: Profile audit

Name: _____

Think about all the online sites that have your personal information. Consider social networking sites, sites where you have registered or have membership, banking sites, mobile phone accounts etc. Below are listed many different pieces of personal information. Tick the box if you have shared the piece of information somewhere on the Internet.

- | | |
|--|--|
| <input type="checkbox"/> First name | <input type="checkbox"/> Likes/dislikes |
| <input type="checkbox"/> Last name | <input type="checkbox"/> Names of family members |
| <input type="checkbox"/> Age | <input type="checkbox"/> 'Handle' (online name) |
| <input type="checkbox"/> Location | <input type="checkbox"/> Sports/hobbies |
| <input type="checkbox"/> Gender | <input type="checkbox"/> Home phone number |
| <input type="checkbox"/> Address | <input type="checkbox"/> Mobile phone number |
| <input type="checkbox"/> Email | <input type="checkbox"/> Name of school |
| <input type="checkbox"/> Date of birth | <input type="checkbox"/> Photos |

List any other information that you have posted online:

_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

Worksheet 3: Internet use contract

I _____ understand that in order to continue using the Internet at school and at home, I must agree to the following terms and conditions.

(Please initial each one to show that you have read and understood it):

- I will agree with parents/guardians or teachers about when I can go online, how often and for how long.
- I will be a responsible user who uses the Internet in ways that I know my parents/guardians or teachers would approve of.
- I will moderate my online activities and only visit safe, secure websites.
- I will download content only if I know it is safe.
- I will use a handle or avatar when using online chat services, and only use my real name for communicating with real-life friends.
- I will keep personal identifying information, such as last name, home address, email address, telephone number, parents/guardians' names, or the name or location of my school, private. I will not give it out without permission from my parents/guardians or teachers, to avoid being 'tricked' into allowing people to engage in cyberbullying, identity theft or to send viruses or spyware to my computer.
- I will not send photos or descriptions of myself, my family members or my friends to anyone without permission from my parents/guardians or teachers.
- I will not respond to content that makes me feel uncomfortable, or that is rude, obscene, offensive or threatening and I will tell my parents/guardians or teachers immediately if I read or see such content.
- I will not agree to meet someone I know only via the Internet without permission from my parents/guardians. If my parents/guardians agree to a face-to-face meeting, I will only meet in a public place with a parent/guardian nearby.

Signed: _____

Date: _____