Cybersmart Access

Upper Primary
Pic your friends
Creative Commons

These teaching resources are available to schools under Creative Commons licences. The licensing conditions enable schools and teachers to use, adapt and re-publish material from the resource, without seeking permission to republish from the Office. 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 2016

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 Office has taken reasonable care to ensure the information in this work is correct and accurate at the time of publication. However, the Office makes no warranties regarding the correctness of the information at later dates, and disclaims liability for damages resulting from its use. The Office 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 Office requests that if you republish this work, you notify the Office by email at: enquiries@esafety.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.

Before you start

This unit is designed for students with special education needs aged around 10-11 years-old. This unit may also be suitable for mainstream students aged 10-11 or slightly younger.

For some general information about what young Australians are doing online visit the ‘Aussie teens online snapshot’ section at https://esafety.gov.au/about-the-office/research-library/aussie-teens-and-kids-online.

Teacher background information

Online socialising has many benefits, however, it is important that children understand how to identify who true online friends are, and to restrict the information they share with people who aren’t trusted friends.

Students can practice using responding safely online with the Pic your friends game and other supporting activities. Pic your friends provides a social networking simulation where students receive communications from people claiming to be their friends. They are prompted to ask appropriate questions to identify whether the person is really a friend or a bully in disguise.

Unit overview and objectives

This unit aims to help students understand:

1. people can pretend to be someone else online;
2. learn strategies to identify true online friends;
3. what personal information is and how to protect it when online;
4. how to use user names and responsibly and safely; and
5. how to seek help when worried about something that has happened online.

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

1. identify safe and unsafe user names;
2. list safe strategies for making friends online; and
3. describe ways to keep their identity private online.

Unit duration

The time allocated to this unit will depend upon the prior knowledge and skill levels of your students.

It comprises four activities, each designed to take approximately one or two x 45-minute lessons.

Required resources

- Pic Your Friends Game from Cybersmart Access: https://www.esafety.gov.au/access/games_index.html. This online game models safe online 'friend checking' behaviour for children to use in social networking and gaming.

Cybersafety Traffic Lights Poster: Attachment A

Alison’s Story: Attachment B. This brief scenario developed by Strathclyde police in the UK describes a young girl’s online experience communicating with an online ‘friend’ who was in fact a male adult grooming her

Alison’s Story Rewrite the Story: Attachment C

Privacy Settings: Attachment D

Privacy Settings Circled: Attachment E

Further information

If students are worried or upset by something that has happened online they can contact Kids Helpline who provides free, confidential online counselling for children and young people, 24 hours a day, 7 days a week.

For more information, contact:
Office of the Children’s eSafety Commissioner
Tel: 1800 880 176
Email: enquiries@esafety.gov.au

Activity 1: Protecting your personal information

What you will need:

- Paper
- Pens
- Butchers Paper or whiteboard
- Alison’s Story: Attachment B. This brief scenario developed by Strathclyde police in the UK describes a young girl’s online experience communicating with an online ‘friend’ who was in fact a male adult grooming her. She finds out he is not who he says and reports him to her mum and the police.

Ask students to write down on a piece of paper “Yes” or “No” their answer to the following questions, or to stand up or sit down in response to the questions:

1. Do you have a social networking account?
2. Do you use a chat program to talk to people online?
3. Do you play online games that allow you to chat at the same time? If so, do you chat to people you haven’t seen in real life?
4. Do they have any online friends they have never met? How do they know they are friends?

Draw up a graph on butchers' paper or whiteboard (or you could use polling tools on the interactive whiteboard or web) to show the differences between real friends and those they only know online without using names. Focus on numbers of online friends they haven’t met and ask students to brainstorm why it might be risky to have an online ‘friend’ they haven’t met.

**Teacher notes**

Prompt students to consider:

- the risk that online ‘friends’ might be pretending to be someone else, might actually be mean, bully, seeking children for bad reasons (if appropriate for your group), seeking information about their home or parents to steal money, or possibly to hurt them.

Ask students to brainstorm ways they can keep safe when talking to online ‘friends’ they haven’t met.

Prompt students to consider:

- Keeping personal information private. Personal information is information that identifies people and where they live including, school name, address, full name, sports clubs, parents’ and siblings’ full names.

Reiterate that we can be safe when talking to online friends if we protect our personal information and never agree to meet an online friend without talking to a parent or carer, and, if they let them meet, taking the parent or carer to the meeting (you may not want to
mention meeting as an actual possibility…although some support groups for children with disabilities do end up meeting in real life with parental supervision).

**Alison’s Story**

View the Alison’s Story attachment on the interactive whiteboard or provide print-outs for students to follow. Read the story all the way through in the first instance. Discuss with students what happened in the story to ensure comprehension of important issues.

Read the story again, this time pausing strategically to tease out threats to safety and to discuss implications of Alison’s actions. What did Alison do that made her experience online very unsafe?

**Teacher notes**

Prompt students to consider the following unsafe actions and their positive alternatives:

1. providing her mobile number to someone she doesn’t know in real life; only give mobile numbers to people you have met. Check with an adult if you aren’t sure if you should share information or not.
2. agreeing to meet someone she doesn’t know in real life—people can pretend to be someone else online. Always tell your parent or carer if someone you haven’t met before asks to meet you.
3. not telling an adult she was going to meet someone she had met online. Never agree to meet someone you don’t know. Ask an adult to help decide. If they think it is safe to meet your parent or carer must go with you in daylight, and you must meet in a busy place with other people around.
4. meeting someone she didn’t know at a quiet place and by herself. Meeting in a busy place, with other people around makes meeting up safer. This should always be done with a trusted adult like a parent or carer.

**Pic Your Friends game**

Introduce the online game Pic Your Friends. On the Interactive White Board, show students a few basic features such as there are two windows, one is the Chat Window where the conversation appears and the window below contains the questions you should ask the people to ascertain their identity and where you decide whether they are telling the truth or a lie. Point out to students that they need to listen to or read both windows and then make a decision.

Give students a chance to explore the game in pairs or trios. High needs students may require targeted digital literacy support at times.

**After the game exploration**

Brainstorm and consolidate what students know about how to identify someone online:

- discuss how children can check they are really chatting to a friend
- find out from students how easy or difficult it was to find a bully.
- revise what they have learned about online safety from the videos.
- ask students one thing they can each do to protect their personal information.
Activity 2: Password privacy

What you will need

- Cybersafety Traffic Lights Poster: Attachment A. A large printout for class wall or individual printouts for each student.
- Paper and pens
- Cardboard or paper keys for each class member

Guess the password

Give each person a key and tell them this is the key to all of their private information and secrets. If time permits they can decorate the key to ensure they feel an attachment to it. Tell students they need to keep their key safe by making up a password that only they can guess. They must keep their password secret from the other students and it must be hard to guess. Ask the to write their name at the top of a sheet of paper and write their password on the piece of paper and pass it to you. Make sure they disclose any passwords they are actually using.

You can then read out passwords, with the class having two to three chances (depending on class size) to guess whose password it is. If a class member guesses the owner of a password, the student with that password must hand them their key. At the end of the game ask those without keys (because they had to give them away) to put their hand up.

Tell the class passwords are very important online because they protect personal and private information from strangers. They must think carefully about passwords and make sure it is something people can’t guess easily. Passwords should have a mix of numbers and letters and should be longer than 6 characters. They shouldn’t be a favourite food, pet name, their name, or the name of friends or family.

Ask students to return each other’s keys and in a circle take turns making up safe passwords (but not the ones they actually use). Remind students passwords must be at least six characters long, a mix of letters and numbers and not names of pets, friend, family or favourite foods.

Ask students to pledge not to share passwords with each other, even if they are best friends.
Hector’s World
Watch Hector’s World Story 1 at https://www.esafety.gov.au/education-resources/classroom-resources/hectors-world/your-personal-information-online for a demonstration of the dangers of sharing personal information online. If time permits, you might want students to watch additional episodes 2-5 which explore the issue in greater depth.

After video exploration
Ask students to consider what Ranjeet did that was risky and why his friends were worried.

Watch the episode again, prompting students to watch carefully to learn what information Ranjeet was going to give out and why his friends stopped him.

Teacher notes: prompt students to consider:

1. what personal or 'special' information is, e.g. address, full name, school etc.. Explore the fact that this information can be used to identify people and where they live. It can be used by mean people.
2. when to share personal information, who to share it with, and why they shouldn’t share it with everyone
3. the need to check with a trusted adult before typing in their personal information. Students should be prompted to identify a list of trusted adults – write this on the board or butcher’s paper and talk about why each adult chosen is a good option.
4. the need to talk to you or another trusted adult about any problems or worries especially if they think they have made a mistake or done the wrong thing on the computer

In pairs or trios ask students to list information that shouldn’t be shared with people they only know online. Ask them to present to another group or the class and discuss what can and can’t be shared with online friends.
Activity 3: Who r u talking to?

What you will need

- Cybersafety Traffic Lights Poster: Attachment A
- Alison’s Story: Attachment B. This brief scenario developed by Strathclyde police in the UK describes a young girl’s online experience communicating with an online ‘friend’ who was in fact a male adult grooming her. She finds out he is not who he says and reports him to her mum and the police.
- Alison’s Story Template: Attachment C. Blank template for children to re-write Alison’s story in a safer way.
- Paper and textas or online comic making and sharing program
- Who R U? Game

Cybersafety rules revision

Introduce students to the Cyber Traffic Lights principals.

Revise lessons learnt from Activity 1:

1. don’t share personal information with online ‘friends’ you haven’t met
2. never ever, meet anyone in real life that you only know online
3. always talk to a trusted adult if someone from online has asked to meet up in real life
4. always check with a trusted adult if someone online asks about something that makes you worried or makes you feel uncomfortable

Give students a chance to explore the game—individually in pairs or trios. High needs students may require targeted digital literacy support at times. Encourage students to try to improve their scores by helping each other with questions.

After the game exploration

Brainstorm and consolidate what students know about how to identify someone online.

- discuss how children can check they are really chatting to a friend
- ask children to put their hand up if they will use questions to check online ‘friends’ are really who they say they are
- encourage all children to try asking questions of people online to check who they are and to report back the next week about how they went.

Create a Digital Story

- Revisit Alison’s Story. Students discuss what Alison could have done differently to make her a safe surfer. (Alison’s Story: Attachment B)
- Students use comic making software or paper and textas to create their own safe surfing story.
- Alternatively students could use the modified storyboard template (Attachment C) to review the story and create new panels showing how Alison or another student could have changed his/her cyber behaviour for a more positive outcome. Prompt them to consider questions she could have asked and actions she could have taken to be safer.
· Share the different story board attempts
· Student reflection: What have you learnt about online friends? How could you ensure Alison’s Story isn’t your story? Discuss why you don’t meet people you only know online.
Activity 4: Privacy Settings

What you will need

- Privacy Settings: Attachment D
- Privacy Settings Circled: Attachment E

Activity preparation

Discuss with students the importance of not using full names or sexy usernames and not sharing rude photos. Discuss how to ensure information that might give away where you live or go to school is kept private. Brainstorm what other things might put students at risk and why.

Teacher notes: This discussion should be focussed on the positive uses of technology and social networking websites that students are happy and confident using. Ask students to consider their own online profiles, the information they share and what that might say to someone who doesn't really know them.

Prompt them to consider that publicly stating where they are going, where they live or go to school can put them at risk of stalkers. Real friends already know where they live and go to school. Remind them that sexy user names and flirty photos can attract the wrong kinds of people—creepy people.

Tell students it is important to check what information they are making public for everyone to see on their social networking sites. They need to check their ‘Privacy Settings’ and make personal information and photos Private or viewable by Friends Only not Public.

Identifying privacy problems

Print out Privacy Settings Original at Attachment C, providing one per pair or trio of students.

Tell students the profile they have is of a student named Josie from another school. Josie loves spending time on her social networking page. Her privacy settings are set to public access which means everyone can see her information.

Ask students to read the information Josie has posted on her page and find ten things she can do with her profile to:

1. keep her personal information private
2. help her avoid unwanted contact from creepy people or bullies
3. protect her digital reputation, or how others see her
4. show she is kind and nice online.

Students should circle 'problems' they find that might mean Josie could be found by strangers or that she isn’t sounding nice online.

Print out Privacy Settings Circled at Attachment D and hand to students. Discuss in class or in groups the ten items Josie needs to change. Use the following hints to guide the
cyber(Smart:)

discussion. Don't make your personal contact details such as email address and mobile phone number public.

1. Keep the list of your friends safe and manageable—only accept people you know in person.
2. Ask a friend’s permission before you post photographs of them or other personal information.
4. Be respectful of other people in the community—if you wouldn’t say it in person, don’t say it online!
5. Don’t reveal patterns or habits—this makes it easy for people to know where you will be and what you’ll be doing.
6. Take care with posting full photographs of yourself—especially when you have other identifying information on your page.
7. You don’t have to use your full name. Keep as much identifying information to yourself as you can.
8. The more details you give about where people can find information about you, the less protected you are.
9. Some information can invite contact you may not want for example, relationship status.
10. Be careful not to tell people your whereabouts.

Teacher Notes
Encourage students to check their own social networking profiles that night and to make sure their profiles are set to ‘Private’ and that they aren’t putting themselves at risk.
Attachment A: Cybersafety Traffic Lights Poster

Protect it

Protect your private information. Treat it like a toothbrush and don’t share it. Remember that people online may not be who they say they are. Online ‘friends’ are still strangers even if you have been talking to them for a long time.

Don’t post this stuff

Personal information includes:
- your full name
- rude or mean photos
- photos that show where you live, go to school or do sport
- addresses
- school information
- sports clubs or dance groups
- telephone numbers
- places you like to spend time

This is your special stuff – it is yours to keep.

Use settings

Get an adult to help you set Privacy Settings to Private so only your online Friends can see your stuff.

Use a nickname

When you use chat rooms in games or instant messenger, use a nickname instead of your real name.

Don’t share your passwords with any friends

Always keep your passwords secret. You can share them with your parents but that is all. Your parents can help you make a good password that is hard to guess.

Get help if people are mean to you

Stop or block people who send you nasty messages. Show a parent or teacher you like and they can help you block the person and report them online.

If they keep being mean they can get into big trouble with the Government as it is not okay to be mean online. Get a parent or teacher you like to look at this page: https://www.esafety.gov.au/complaints-and-reporting/cyberbullying-complaints/i-want-to-report-cyberbullying.

Don’t be mean to other people

You don’t want to hurt anybody’s feelings. Even if everybody else is being mean… it is better to stay out of it.

People can see what you don online and you can get into big trouble.

Don’t open attachments or click on links from people you don’t know in real life.

They might have viruses in them or be trying to trick you.

Get help if you feel sad or scared

If you see anything that makes you sad, scared or worried online show it to your parent or a teacher you like.

Check if somebody wants your photo

If somebody asks you for photos or asks you too much about yourself tell a – parent or teacher.

Check if somebody wants to meet you

If somebody asks to meet you in real life check with a parent or teacher.

Get help if something makes you feel yuck

If anything makes you feel yucky online show it to a parent or teacher. They can help.

Tell somebody if you see people being mean

If someone you know is being nasty to someone online, tell a parent or teacher. Don’t be mean back or you will get in trouble.
1. Alison loved the Internet. Every day, after school, she would go upstairs and surf the web. One of Alison’s favourite sites was a chat room. She would log on and talk to other kids about her favourite boy bands and TV shows.

2. One day, Carl logged on. He said he was 12 and he liked the same bands as Alison. Alison thought Carl was cool. She even gave him her mobile number so he could text her at school.

3. One day, Carl sent Alison a text, asking if she wanted to meet him in the park after school. Alison said ‘yes’ straight away. She couldn’t wait to see what Carl looked like.

4. When Alison got to the park, she couldn’t see Carl - just a man sitting by the swings. Alison phoned Carl to find out where he was. She got a fright when the man sitting by the swings answered the call.

5. Alison hung up. The man had been pretending to be Carl all along. Alison was in danger. Alison ran straight home and told her mum what had happened. Her mum called the police. Alison never heard from Carl again.

6. Alison didn’t tell her parents that she was going to meet someone she had met in a chat room. That was very dangerous. It was also a big mistake to give out her mobile number. Alison was lucky not to get hurt.
Attachment C  Alison’s Story: Rewrite the story
About Me

Basic Info
- Sex: Female
- Birthday: March 18, 1997
- Relationship Status: Single
- Looking For: Friendship
- Political Views: Sunshine and lollipops

Bio
My friends call me JosieJo because I am always smiling and laughing. I love to swim and do what makes me happy. I have so much fun and best of all I have the best friends in the world! I am in year 7 and am scared of Mrs Young!

Favorite Quotations
Well then, you see, a dog grins when it's angry, and wags its tail when it's pleased. Now I grin when I'm pleased, and wag my tail when I'm angry. Therefore I'm mad. [The Cat - Alice in Wonderland]

Work and Education

High School
- Cherry Creek High School

Contact Information

- Email: josiejo@hazemill.com
- Mobile Phone: 0447 654 321
- Other Phone: 
- Address: 37 Devon Way, Cherry Creek
- Twitter: @JosieJo
- Website: http://josieJO32164.blogspot.com
Attachment D: Privacy Settings Circled

My favourite thing to do is take my dog Walter to Cherry park after school. I love my BF Office but I don’t like farms. I like posting stories to my blog and want to be a famous writer so read my stuff!

Cherry Creek High School

Josie Mitchell

Email: josie@hotmail.com
Mobile Phone: 0412345678
Other Phone: 
Address: 123 Orion Way, Cherry Creek
Twitter: 
Website: http://josie.xx32344.bluespace.com