Cybersmart Access

Upper Primary
Crowd surfing
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 10-11 years-old 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

This unit explores private and personal spaces and the types of information that should be kept private online. It introduces the concept of online and offline friends.

There is an interactive online game to help students can practice deciding whether a message is safe or there is a good reason to pass it on and to consider who can be trusted to share messages with online.

Unit overview and objectives

This unit aims to help students understand:

1. that personal information can be used to identify or locate them
2. personal information must only be shared with trusted people and for a good reason.

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

3. recognise the difference between public and private online spaces
4. understand what type of information should and should not be shared online.

Unit duration

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

There are four activities, each designed to take approximately one or two 45-minute lessons. There are also extension activities for further consolidation.

Required resources

- Cybersafety Traffic Lights Poster: Attachment A
- Rules for Cyber Binning: Attachment B
- Cybersafe T Chart: Attachment C

Further information

If students are worried or upset by something that has happened online they can contact Kids Helpline which provides free, confidential online and phone 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: Sharing Online Information

What you will need:

- Computers with web access. One per two to three students.
- Whiteboard or butchers paper to record student responses to focus questions

Warm up activity - The Pulse

- Ask students to stand in a circle with hands joined. One student is selected to be the observer and stands in the centre of the circle.
- Secretly select a student to be first to send the pulse. Students pass around a pulse by squeezing a hand (once they have received a hand squeeze). They can pass back to the student they received the squeeze from or on pass to another student.
- The observer student in the middle must try to catch a student in the act of squeezing.

Focus questions

1. How quickly did the squeeze move?
2. How often did it go backwards?
3. Did anyone squeeze too hard and hurt someone? (Can that happen with words or with things we do on our phones and computers?)
4. If so, what did the student do? (Perhaps shouted out, or broke the circle. Then use this information to show that real life is no different to online. If something online is hurtful then students should ‘shout out’)
5. How might this be compared to online communication and behaviour?
6. How quickly do digital messages move online?
7. Should we always pass on digital messages? What if the message might hurt someone?

Teacher notes

Prompt students to consider:

- the passing on of online messages is silent. Once they send a message it is hard to know what others are doing with it
- messages can be shared very quickly and can reach people outside the group. Demonstrate this by having some students break the chain or joining your own hand in and starting a new chain
- only share with people they have met and trust offline. If it is an online contact they need to check with their parent or carer.
- only share messages that won’t hurt them or others if somebody else reads the message – nothing mean or nasty or private.
Activity 2: Avoiding viruses tag game

What you will need:

- Safe running space such as a gym or a grassed playing field

Pre-game discussion

Explain to students:

- Viruses are bad files made by mean people to steal information and break computers
- Viruses can get into computers and break them
- They can keep viruses out of computers and devices by not clicking on links on ads or emails asking for money
- They need to check with an adult before signing up to a website or sharing their email address online.
- They should tell a trusted adult if they think they have made a mistake and clicked on something bad.
- They can help keep viruses out by not sharing files with friends and not opening files from friends unless an adult has checked them for viruses.
- They should not download files unless an adult has checked them for viruses. Downloading is when you click on a link or file and it starts loading onto your computer or device so you can use it.
- They should get an adult to load “anti-virus” software on computers and devices. Villains and Viruses Tag Game

This tag game is based loosely on Octopus Tag. It explores the concept of viruses, identifying that ‘clicking on’ some online things may expose computers to viruses which can break computers.

Game rules

The cyber villain is the main tagger. The computer users are trying to be safe online (across the gym). If the villain tags you then you become a virus. The virus must stay where they were tagged, they can move one leg and both of their arms to help the cyber villain capture more users.

Instructions

1. Set up a rectangular space as described in the Teacher Notes section below, and mark the boundaries.
2. The computer users line up at one end and the cyber villain stands in the middle and cries out, ‘I am the villain of the online space. See if you can cross my place.’
3. The computer users try to run or sneak across the online space as the cyber villain tries to tag them. If tagged, they become viruses. Keeping one foot planted, viruses try to reach out and tag the computer users running by, thus turning those players into viruses as well.
4. Once the computer users reach the other side, the cyber villain and the viruses say the chant and the crossing contest starts again. The game continues until all the
computer users are caught. The last computer user caught becomes the next cyber villain.

**Teacher Notes**

Make sure your space isn't too wide. To determine the right width, have everyone hold hands and spread out across the field. Indicate the two sidelines with clothing or other markers. Since the game tends to produce fast cybervillains (meaning the slower students rarely get a chance to be "It"), consider teaming a slower student with a faster player to create a two-person cybervillain.

You can replay the game and introduce a trusted adult who helps clean up the viruses, ‘freeing’ the computer users to emphasise the need to report any issues to a trusted adult.
Activity 3: Cyber sharing games

What you will need:

- Student computers with web access. One per two to three students.
- Whiteboard
- Projector or interactive whiteboard.
- Rules for Cyber Binning: Attachment A

Crowd Surfing game

Introduce the rules of the game to students:

- In this game you get messages from others. You need to decide whether to Bin them, Check with an adult or Pass them on.
- Ask students to think about what messages they might ‘Bin’ or ‘Check with an adult’
  - E.g. rude stuff, mean messages, ads and money offers, people they don’t know (that they haven’t met for real) asking for information
- You may like to demonstrate the game for students.
- Pairing students up might help them work through the messages and what to do with them.
- Offer students the chance to replay the Crowd Surfing game. Did students improve on their score from last time?
- The game can be played multiple times to improve the score and also to test the consequences of choices.
- Have a quick chat about which messages people Binned, Checked or felt were Okay to pass to recap key messages.
Activity 4: To Share or Not to Share...

What you will need:

- T Chart templates: Attachment C
- Digital cameras or access to computers to search for digital photos
- Glue
- Large poster paper, Coloured card
- Texta pens
- Boardmaker symbols if required
- Activity cards
- ‘Share’ or ‘Keep private’ cards

*Alternative: This activity could be done by using a word processor or desktop publishing program*

Students complete the T Chart to record the information that is private and should not be shared and information that is acceptable to share.

**Public and private montage**

Ask students to create a photo montage of public and private spaces in their lives. They should stick the name of the activity on the ‘public’ or ‘private’ sheet to represent how they would manage activities.

**Teachers:** for if visual support will help, you could print off activities on cards, such as:

- Get dressed.
- Go the toilet.
- Go to school.
- Play at playground.
- Eating ice cream in school uniform.
- Playing sport.

Students could stick these onto the appropriate photos in the montage.

Teachers could also write simple action statements such as (or use visual representations):

- Share with the world/show everyone
- Keep private/not show to anyone

The above statements could be accompanied by thumbs up and thumbs down to give students visual cues.

**Teacher notes**

Prompt students to consider:

- the types of activities and whether they are giving away too much information about themselves.
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.
Rules for Cyber binning

C - Do I feel comfortable?

H - Could it hurt me or someone else?

E - Am I embarrassed?

S - Is it safe?

S - Am I sure it’s legal and secure?
## Attachment C: Cybersafe T-Chart

Name: ____________________________________________

<table>
<thead>
<tr>
<th>Cyber Safe Practice</th>
<th>How Safe?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

C-Comfortable  
H-Hurtful or not?  
E-Embarrassing or not?  
S- Safe  
S-Secure