Cyber Safety in Action – Teacher's resource

These scenarios are designed to help to create conversation starters during class after Internet Safe Education has presented.

Key Messages

- The internet is PUBLIC and PERMANENT
- My identity is paramount
- Online contacts remain strangers
- Online rules and laws are real
- I take action when things go wrong online

1 –When you apply for a job, they will look at your social media accounts. What do you think they are looking for?

- Discussion points
  - They are looking for anything that makes you a risk in the workplace such as violence, bias, harassment, poor language, sexism, racism, overtly sexual etc.
    - Australian employers have an obligation to the health and safety of their staff under Australian law. Inappropriate comments in a workplace may lead to harm of co-workers who feel offended or threatened.
    - Discriminatory behaviour is unlawful, and an employer will not risk a new hire becoming a workplace problem.
  - They are looking to see who you follow, your influences, and any windows into your character. They are making an assessment of your cultural fit in the organisation.
- **Can you stop a potential employer from seeing your social media/online activity?**
  - Settings can be used to secure an account and improve privacy settings however there are things an individual can't control. For example, where they are tagged by someone else or a comment is made on another person's account that has poor privacy settings. Often people use settings well in one app but poorly in others. Consistent poor online behaviour will usually appear.
  - Once a potential employer knows your school and year, they can look into other accounts that are not well secured to see images or information about you.

2 – Carmen has experienced bullying at school and online. The school and parents worked together to address it and Carmen's school life had been better until about a month ago. A new person is saying cruel things online. The person says Carmen should hurt herself. Carmen and her friend suspect it is the same person using a new online name. What can they do?

- They don't know for sure who is doing it.
- Use the school and family rules and supports rather than react with anger or threats.
- Do not respond. Take control. Gather evidence. Screen shot. Keep a file. See if the identity links to any other accounts that are identifiable to a student.
- Carmen should go back to her privacy and security settings and lock them down as much as possible. Block that identity.
- Seek support from parents, school, and friends.

3 – Josh has been gaming with some guys for months. They have never met. One of the players invites Josh to catch up on the weekend. Josh organises to meet the player and doesn't tell anyone about the meetup. What could go wrong?

- Discussion points
  - The player may not be who they said – older. Poor intentions. More than one person – intending to cause harm (bash) or rob. People are not always who they say they are online.
- **What protective actions could Josh take?**
  - Get the player to video chat before they meet up so that they know what each other looks like. Be suspicious of a broken camera. Take a friend to the meetup. Tell his parents where he's going, who with and when he's likely to be back.

4 – Terry and Grace have been dating. Terry sends Grace a sexually explicit picture and asks Grace to do the same. What should Grace do and how does consent factor into this situation?

- Discussion points
  - Remember that images are for ever and today's relationships are tomorrow's potential problem. Images are permanent and people can use images to extort further action or embarrass or shame in the future.
  - Grace did not consent to receiving an image. Sending the image is disrespectful and possibly causes harm, distress and/or fear. Sending the image is equivalent to indecent exposure.
  - Grace is the ONLY one who can decide to say no. Any further pressure indicates Terry's lack of respect and care.
  - **Research indicates about 1/3 of girls who are asked eventually send the picture, and most instantly regret it. Don't be one of the 1/3. Don't believe 'everyone' is.**[1]
- **What does the law say about taking inappropriate pictures of children that may be considered child exploitation materials?**
  - It is against the law to take, store or share them. The age of 'child' differs between states.

This may feel uncomfortable to teach however it is happening and it's best to get in front of the conversation. Give them the tools to not do it or stop doing it. Seeing the parallel to the physical world example can shock and refocus the perception of 'everyone is doing it' and what 'it' really is. When it's digital, it is potentially accessible everywhere.
Forever.

[1] Biddul