Online Safety Basics - eSecurity

Topic: eSecurity

Target age group: Years 2-4

Lesson/activity duration: 5 x 10min

Activity purpose

The activities included in this lesson plan are designed for young people setting up their first device or signing up to a social media account for the first time. Students will develop skills in using device and app security settings to prevent unwanted contact and protect their information.

RECOMMENDED TEACHING APPROACH

Watch the Act eSafe video and discuss students' knowledge of the online safety concepts covered. Depending on the current level of student knowledge, use the resources as an online safety refresher or tackle one concept per lesson and allow time for discussion and device practice. Use the activities to reflect on the key concepts covered in the video. Depending on the age of the students work through the different aspects of the 'Personal online safety plan' as class or have older students complete the worksheet independently.

RESOURCES REQUIRED

- Act eSafe video esafety.gov.au/education-resources/classroom-resources/act-esafe
- Class set of the student ‘Personal online safety plan’ worksheet
- Tablet or computer

KEY WORDS

- eSecurity
- Personal information
- Privacy
- Help and support

Uses technology | Class discussion | Requires handouts or signs | In pairs | Activity length

Activity 1: Watch the Act eSafe video and discuss the role of critical thinking in online safety

10 mins

Learning intention

- For students to reflect on the critical literacy skills required to stay safe online.

Resources: None required

Instructions

1. Ask the students to discuss what they think is the most important skill that will help them to stay safe online.
2. Explain to students that the people who are the safest online, are the ones that ask the most questions.
3. Use the acronym Ask-Check-Think (ACT) to help students think of some of the ways they can use critical thinking to help them stay safe online. Use the following ideas to guide the discussion:
   - **ask** - others what they do when they're online to stay safe
   - **ask** - people about their experiences and mistakes
   - **check** - settings and passwords
   - **check** - author information and website security
   - **think** - about the benefits and risks of sharing personal information
   - **think** - about how the situation makes you feel.
4. Guide the class through activities 2-5 of the lesson plan and complete the corresponding areas of the 'Personal online safety plan'.

Activity 2: Keeping personal Information private

10 mins

Learning intention

- For students to identify class and personal guidelines to protect personal information and identity when communicating with unknown audiences.

Resources: Paper, highlighter, tablet or computer (teacher and/or students)

Instructions

1. Ask students to work in pairs to list the types of information (e.g. photos of pets, photos in a school uniform, name, full name, suburb) they have seen posted on a website, game or app.
2. Ask the students to highlight any content that is private or not safe to share.
3. Demonstrate how to use privacy settings on a game, app or website. Optional: In pairs, ask students to log in to a game or app account that is recommended for under 13 year olds and check their privacy settings to see if any private information is shared.
4. Ask students to complete the 'Keeping personal information private' section of the 'Personal online safety plan'.

Activity 3: Keeping location information private

10 mins

Learning intention

- For students to develop personal protocols to protect location information and privacy when using location services.

Resources: Tablet or computer (teacher and/or students)

Instructions

1. As a class, review and discuss the scenario in the video (1:24) where Anna's brother could see her location because she hadn't turned off 'location sharing' for the app she was using.
   a) Who else might be able to see her location?
   b) What are the risks of Anna sharing her location?
2. Ask students to discuss how they can minimise the number of people who can see their location when they're online e.g. turning off automatic location settings, not tagging their location when sharing images.
3. Demonstrate how to turn off automatic location sharing. See our eSafety Women resources for tips on how to do this esafety.gov.au/women/lifestyle/using-your-device/gps. Optional: In pairs, ask students to login to their personal device and turn off automatic location sharing.
4. Ask students to complete the 'Keeping your location private' section of the 'Personal online safety plan'.

Activity 4: Keeping your device safe

10 mins

Learning intention

- For students to share knowledge and practice skills for setting up and managing a device to protect data and photos.

Resources: Tablet or computer (teacher and/or students)

Instructions

1. As a class, review and discuss the scenario in the video where Harvey accidentally clicked on a link and installed a virus on his computer (2:28).
   a) What was the consequence of downloading a virus for Harvey?
2. In pairs or small groups, have the students discuss the advice they would give someone to help them avoid downloading a virus or malware e.g. not clicking on pop-ups.
3. Ask students to share other ways to protect devices such as keeping them in a safe place or using a passcode to lock the device when not in use.
4. Ask students to complete the 'Keeping your device safe' section of the 'Personal online safety plan'.

Activity 5: Getting help and support

10 mins

Learning intention

- For students to explore where to get help and support when online issues impact on their identity, privacy or emotional safety.

Resources: Tablet or computer (teacher and/or students)

Instructions

1. Ask students to share different types of negative experiences they might have encountered online. Use the following questions to guide the discussion:
   a) Has anyone seen a picture or video online that made them feel worried?
   b) Has anyone ever had someone they don't know contact them in a game?
   c) Has anyone ever said mean things about them or someone they know?

2. Ask students to describe how they have dealt with these experiences in the past. Students to work in pairs or small groups to come up with other suggestions for dealing with situations that make them feel uncomfortable e.g. talking to trusted adults or reporting issues to the game/app/social media service.

3. As a class, visit each of the following sites and discuss the online support available:

   - visit the esafety.gov.au website and discuss the cyberbullying reporting functions
   - visit scamwatch.gov.au and discuss the latest scams and how to report a scam to them
   - visit kidshelpline.com.au and discuss how they can access anonymous 24hr online counselling if they are worried about something they have seen or experienced online.

4. Ask students to complete the 'Getting help and support' section of the 'Personal online safety plan'.

Australian Curriculum links

Learning areas	General capabilitiies
Digital Technologies Year 1 & 2 Create and organise ideas and information using information systems independently and with others, and share these with known people in safe online environments. (ACTDIP006) Year 3 & 4 Plan, create and communicate ideas and information independently and with others, applying agreed ethical and social protocols. (ACTDIP013)	**Information and Communication Technologies (ICT) Capability** Year 1 & 2 • Apply digital information security practices - follow class rules about applying selected standard guidelines and techniques to secure digital information. • Apply personal security protocols - follow class guidelines when sharing personal information and apply basic social protocols when using ICT to communicate with known audiences. Year 3 & 4 • Apply digital information security practices - independently apply standard guidelines and techniques for particular digital systems to secure digital information. • Apply personal security protocols - apply standard guidelines and take action to avoid the common dangers to personal security when using ICT and apply appropriate basic social protocols when using ICT to communicate with unknown audiences.

Online Safety Basics - eSecurity

Student Worksheet

When you are playing games, researching for school, watching videos and chatting to people online, it is important to be aware of eSecurity risks. eSecurity risks can include losing your information, spending money that you didn't intend to spend, damaging your device or having someone contact you in a way that doesn't feel safe. It's a good idea to prepare yourself and to build skills to face eSecurity risks.

Complete the worksheet below to come up with your own 'Personal online safety plan'.

Keeping my personal information safe	
What is my safe username?	
Which types of information do I like to keep private?	
How do I protect the privacy of others when I'm online?	
How can I make a strong password?	
Keeping my location information private	
When can I share my location publically on a game or app?	
Who can I ask to help me update my settings?	
Keeping my device safe	
Who's in charge of keeping my device and anti-virus software up to date?	
How do I back up my data and photos?	
How can I avoid downloading a virus to my device?	
Getting help and support	
Who can I trust if I need to talk about something that I've seen online has made me feel bad or uncomfortable	
Where can I go for information about staying safe online?	
Where can I get 24hr support or advice if I feel upset about something I've experienced online?	
Where can I keep up to date on the latest scams?	