

Cybercrime and the Law

Lesson Ideas Pack



CRIME
STOPPERS
com.au
1800 333 000

Introduction

We support the view that schooling should develop a sense of community engagement in students by increasing their potential to be informed, responsible, ethical and active participants in society.

Through practical tasks relating to real life experiences, these *free* resources help students develop a positive attitude towards their role in society. They enable teachers to select lesson ideas within a theme in any order, to best suit **curriculum requirements** and the **interest** of students. Digital resources embedded in these resources comply with the [Social Media Minimum Age obligation](#) (SMMA obligation) and have been chosen with careful consideration to support learning and wellbeing. Some resources feature YouTube videos that can be seen without logging into an account. These should be viewed by students with teacher support.

We developed these to make the content of the Australian Humanities and Social Sciences (HASS) Civics and Citizenship syllabus for Years 7-10 *more engaging*.

To make things easy, lesson ideas link directly to the Australian and Victorian Curriculum codes and key concepts, namely; *Democratic Values, The Westminster System, Justice, Participation, and Rights and Responsibilities*. The activities provided are just suggestions and should be adjusted to suit the student cohort.

Specific lessons in this theme can also be used to support the teaching of lower secondary Digital Technologies, The Arts (Media Arts), Health & Physical Education and English content.

A number of the activities in this resource link to the [eSafety Commissioner's website](#). Crime Stoppers Australia would like to acknowledge the important work carried out by the eSafety Commissioner to empower Australians to have a more positive and safe online experience.

HASS Year Level Description and Required Content

Year 7

An understanding of the Civics and Citizenship concepts is developed through a focus on Australia's democracy and legal system. The teaching ideas in this resource assist students to gain knowledge and understanding of how Australia's legal system aims to provide justice, through the rule of law. *Links to curriculum codes:* [AC9HC7K03](#) / [VC2HC8K05](#)

Year 8

An understanding of the Civics and Citizenship concepts is developed through a focus on how citizens can participate in Australia's democracy, including use of the electoral system, contact with their elected representatives, use of lobby groups, and direct action.

Links to curriculum codes: [AC9HC8K01](#) / [VC2HC8K06](#)

Year 9

An understanding of the Civics and Citizenship concepts is developed through a focus on how Australia's legal system works to support a democratic and just society. The teaching ideas in this resource assist students to gain knowledge and understanding regarding the key principles of Australia's justice system, including equity before the law, independent judiciary, right to appeal and the factors that can undermine the application of the principles of justice.

Links to curriculum codes: [AC9HC9K04](#) / [VC2HC10K05](#)

Year 10

An understanding of the Civics and Citizenship concepts is developed through a focus on what are the features of a resilient democracy. The teaching ideas in this resource assist students to gain knowledge and understanding regarding the challenges to and ways of sustaining a resilient democracy and cohesive society. *Links to curriculum codes:* [AC9HC10K05](#) / [VC2HC10K10](#)

The Australian Curriculum alignment statement is based on the Australian Curriculum, Assessment and Reporting Authority (ACARA) materials which are licensed under a [Creative Commons Attribution 4.0 International \(CC BY\) licence](#).

Learning Intentions

Resource Focus

Community safety and wellbeing is enhanced when individuals understand the law and take action to prevent crime.

This resource provides students in years 7-10 with the opportunity to explore what a digital citizen is and how Australia's democracy, and other democracies, may be undermined by cybercrime. It explores the safeguards that individuals and governments can put into place to protect Australia's and individual's democratic online rights.

Please note that some students may have experienced negative themes explored in this resource. It is important that the teacher, prior to teaching the resource, knows where student support is within the school and community, and provides this information to students prior to teaching the themes.

If teachers wish to access professional learning to support teaching online safety, eSafety provides a free [professional learning program](#) which covers the latest online safety research, case studies and teaching strategies to help educators integrate online safety into their programs and student wellbeing planning.

Students Understand:

- What it means to be a digital citizen
 - That technology can facilitate criminal activity
 - How to interpret cybercrime statistics
 - How to be cyber safe
 - How to recognise fake news
 - Cybercrime and the law
-

Lesson Ideas

Tuning In

Australians love technology and have one of the highest take-up rates in the world. In fact, technology has become an integral part of our daily life. Today, billions of people all over the planet interact using various technologies. This has created a digital society with citizens that can connect through many avenues such as, education, commerce, employment, entertainment and social interaction. So, what is a digital citizen, are there rules, laws and behaviours that should be followed in a digital society and what happens when these are not adhered to?

A digital citizen can be defined as:

‘a person with the skills and knowledge to effectively use digital technologies to participate in society, communicate with others and create and consume digital content’ ([Best Practice Framework for Online Safety Education](#), eSafety Commission, 2021)

Within any society, it is expected that digital citizens act in a certain way according to accepted behaviours, rules, and laws. Each of these will be covered in this resource. (This information can be written somewhere in the classroom to remind students about appropriate online behaviour.)

- Ask students to watch [Commit to Digital Citizenship!](#) and conduct a class callout identifying the video's key messages as a citizen and then as a digital citizen. Discuss whether these messages pertain to behaviours, rules, or laws? (Mainly behaviours). It is important to emphasise that being online makes you no less responsible for your behaviour or calling out the behaviour of others. Online behaviour is pervasive, permanent and the impacts can multiply beyond the first action.
- Download the [I'm a Digital Citizen](#) poster and display it in the classroom so that you can refer to it throughout this theme.
- Mike Ribble, internationally renowned author of *Digital Citizenship in Schools*, suggests [nine themes of digital citizenship](#) that guide a S3 (Safe, Savvy and Social) Framework. Ask students to research the [S3 Framework](#) (found underneath the nine elements of digital citizenship). They can then complete the second column of the [nine themes of digital citizenship work sheet](#). Share student's responses as a class and discuss whether the school has or should have a digital citizenship policy, and what it does/could encompass. Conclude the activity by asking students to complete the third column of the table considering their class discussion.

Lesson Idea 1: You as a Digital Citizen

In the theme, *Democratic Values*, students explored the values that underpin being an Australian citizen. This lesson explores how these values underpin being a digital citizen, digital citizens' rights, and how their digital footprint can 'brand' them into the future.

- Remind students that we all make sense of each other by the way we react when we meet/interact, whether this is face-to-face or online. What you do and say online is how people decide what kind of person you are.
- Provide each student with a copy of the [Australian Values and Digital Citizenship](#) worksheet and conduct an 'experts' strategy to determine how each of our Australian values underpins being a digital citizen.
 - Divide the class into seven groups and allocate one value to each group.
 - Ask each group to appoint a facilitator and discuss what that value means as an Australian citizen and as an Australian digital citizen. They record their responses on their sheets.
 - Form new groups with one student from each 'expert' group. All the 'experts' share what they have discussed, and students enter the information into their sheets.
 - Ask students to draw a two circle Venn diagram to identify similarities and differences between being an Australian citizen and a digital citizen.
 - Discuss as a class their responses and conclude the activity by asking students to write a paragraph explaining 'the importance of not only being an Australian citizen but being an Australian digital citizen'.

- Explain that the UN Conventions of the Rights of the Child (UNCRC) was introduced over 30 years ago to determine the conditions in which children under 18 could flourish. The *Convention on the Rights of the Child* set out the freedoms and protections that countries must give children and young people under 18 years old. That was the same year the world wide web was invented and at that time people were not aware of the impact online access would have on young people. Recently the Committee on the Rights of the Child, have detailed how children should be treated in the digital world. Display the shorter version, [In our own words – children’s rights in the digital world](#) written by 11–17 year olds, on an interactive whiteboard and conduct a shared reading of the document. Ask students to identify their rights as a digital citizen and use this information to create a Digital Citizen’s rights poster. (Students may wish to use an app such as *Canva* to create their poster.) The most effective could be displayed around the school.
- Discuss as a class what is meant by the term ‘digital footprint’ and create a collaborative definition. (For example, the information about a particular person that exists on the internet because of their online activity.) Write it on the whiteboard. Watch [What’s in your Digital Footprint](#). Refine the definition if required. Ask students to pair and share what they think their current digital footprint says about them as digital citizens.

Explain that the class is going to engage in the eSafety Commissioner activity, ‘*What’s your brand?*’. This activity explores the key elements of a positive digital reputation (footprint) and how a personal brand can be reinvented. Lesson guidelines can be accessed [here](#) and the PowerPoint [here](#).

View the PowerPoint as a class via an interactive whiteboard and discuss the questions as they appear on the PowerPoint.

Conclude the activity by discussing and writing on the board next to the digital footprint definition, the appropriate digital behaviours that create a positive digital footprint.

- Play the online game [Digital Compass](#). The game explores appropriate online behaviour and can only be played on laptops or desktops. This activity can be conducted as a class using an interactive whiteboard.
- If you wish to explore this theme in more depth, additional lesson plans and activities can be accessed via the eSafety Commissioner’s [Young and eSafe](#) resource.
- Explain that on December 10, 2025, a new [Social Media Minimum Age law](#) was implemented in Australia. This law states that Australian children have to be 16 years or older to have a social media account. The change is designed to protect young people from the risks of harm from social media and to support their wellbeing. Australia is the first country in the world to implement this type of law and other countries are keen to see its impact. Explore as a class how various groups in Australian society may respond to this new law. Ask students to watch the eSafety Commissioner ‘[For the good of...](#)’ [Social media minimum age TV advertisement](#). Ask students if they have any questions about the Social Media Minimum Age Law and clarify possible misconceptions. Give each student two copies

of the [Compass Points worksheet](#) and read through each of the questions below. After each question allow time for students to think about and write their response:

- What Excites you about this law?
- What Worries you about this law? What are your concerns? What are the downsides?
- What do you Need to know to better understand the law and its consequences?
- What are the possible Stances, Steps or actions that could be taken (legal action?)

Invite the class to share their thoughts and identify common themes that emerge from the exercise. Ask students to repeat the exercise considering the questions as a parent. Discuss their answers and compare and contrast common themes.

Lesson Idea 2: Fake News and You

Fake news is making news, and it is a problem. The volume and pace of information we now receive can make it difficult to spot fake news. An inability to differentiate between fake and accurate, reliable news isn't something we should overlook. It can lead to uninformed decisions, sow distrust in public institutions, support criminal activity and even directly harm a person's well-being since many potentially dangerous fake health news articles are shared on social media. This lesson supports students to identify examples of fake news and how it can impact on their decision making and strategies to spot fake news. It is important to emphasise with students that if they are in any doubt about what they are reading, they should go back to trusted sources.

- Explain that news articles and advertising can often be biased. That is, facts are distorted to support a particular view. Examples of this can be election campaigns, action campaigns, marketing campaigns for rival products and newspaper reporting. Conduct a class brain dump for one minute of current examples of biased news or advertising students are aware of.
- Discuss that fake news is not the same as biased media or advertising. Show students the ABC video [Fake news](#). Discuss the examples of fake news highlighted in the video, identifying those that could impact on the democratic process and those that could lead to criminal activity. Ask students to complete the [Text to Text, Text to Self, Text to World handout](#) and pair and share their answers.
- Ask students to predict strategies that can be used to identify fake news. Write these on the whiteboard. Show the video [Basic verification tips](#). Discuss the verification tips presented in the video and add any additional strategies to those listed on the board. Ask students how they can use these strategies to become an active and informed digital citizen. Conclude the activity by asking students to create a poster that encourages and assists teenagers to spot fake news. Conduct a class vote and post the top ten posters around the school.
- Explain that students will now face a *Fake News Challenge*. (Individual iPads or computers will be needed for this activity.) Students may use either of the following sites to work their

way through a *Fake News Challenge*. Once completed, discuss students' results and whether they found it difficult or easy to spot the fake news.

- [Real, LOLZ, oops or fake](#)
- [Fakey](#) (play Anonymously)

Lesson Idea 3: Cybercrime

Just as the internet and other new technologies are opening tremendous possibilities, they also provide opportunities for criminals to commit new crimes and to carry out old crimes in new ways.

What is Cybercrime?

In Australia, the term 'cybercrime' is used to describe both:

- crimes directed at computers or other information communications technologies (ICTs) such as computer intrusions and denial of service attacks; and
- crimes where computers or ICTs are an integral part of an offence (such as online fraud).

Statistics show that cybercrimes continue to grow in Australia and pose a serious threat to individuals, businesses, and governments. Cybercriminals constantly evolve their operations against Australian organisations, fuelled by a global industry of access brokers and extortionists (Australian Signals Directorate (ASD) [\(ASD\) Cyber Threat Report 2024-2025](#))

The Australian Signals Directorate (ASD) and Australian Cyber Security Centre (ACSC) provide a list of common online threats that can occur.

- Account compromise
 - Business or personal email compromise
 - Cryptomining
 - Data breaches
 - Hacking
 - Identity theft
 - Malicious insiders
 - Malware
 - Phishing
 - Quishing
 - Ransomware
 - Scams
- Instruct students to access the [ASD/ ACSC website](#) or [Scamwatch](#) and research each of the online threats. Using the [Cyber threats: Note taking template](#) they are to describe

the threats and what they can do to protect themselves and their families. (This information will be used in the concluding presentation activity.)

- If students finish their research before the rest of the class, they may like to attempt the quiz, [Think you can spot a scam?](#)

Cybercrime Statistics

The Australian government's Australian Cyber Security Centre (ACSC) is responsible for strengthening the nation's cyber resilience. It identifies and responds to cyber threats against Australian interests. The ACSC also manages *ReportCyber* on behalf of federal, state and territory law enforcement agencies. This is a single online portal for individuals and businesses to report cybercrime. (Australian Signals Directorate and Australian Cyber Security Centre [\(ASD\) Cyber Threat Report 2024-2025](#).)

- Conduct this activity as a class. Display the year in review section of the Australian Signals Directorate and Australian Cyber Security Centre [\(ASD\) Cyber Threat Report 2024-2025](#) on an interactive whiteboard or provide students with a copy of the pages and ask the following questions.
 - Describe the key cyber incidents that occurred in 2024-2025 and the groups affected?
 - Which cyber incident was the most prevalent across all sectors? Suggest why this may be the case?
 - Discuss which Australian infrastructure sectors would be deemed critical to everyday life in Australia? Suggest reasons why these sectors may be the target of cyber incidents?
 - Look at Figure 5 on page 23 of the report and identify the cyber security incident. Use the diagram to describe how the cyber security incident occurred. Can you give examples of this criminal activity featuring in the media recently?
- Conclude the lesson by asking students to use their notes from the previous activity and the information on the Australian Signals Directorate and Australian Cyber Security Centre [\(ASD\) Cyber Threat Report 2024-2025](#) website to write a summary focusing on the statement 'The downside of digital technology.' Once completed, groups present their findings to the class.

Lesson Idea 4: Our Cyber Safety

In a recent research report, [The digital lives of Aussie teens](#) compiled by the eSafety Commissioner in February 2021, 44% of teens had a negative online experience in the six months to September 2020 and three quarters of teens wanted more online safety information delivered through trusted channels. The eSafety Commissioner is the only government agency in Australia solely committed to keeping citizens safer online. Their

website provides a range of excellent resources to guide students, educators and families through the major online issues impacting on Australians today.

- Explore the [eSafetyyoungpeople](#) website with your students explaining the purpose of the eSafety Commissioner and discussing the key online issues impacting on teenagers today. Issues that may currently impact on secondary students include:
 - Using digital devices safely
 - Cyberbullying
 - Image-based abuse
 - Online abuse related to family violence
 - Removing images, posts, and other material
 - Online scams and identity theft
 - Balancing online time
 - Gaming
 - Social media and online chatting
 - Online child sexual exploitation/online grooming
 - Collecting evidence for legal proceedings.
- Ask students to read [Being Safe Online](#). If online access is not available, provide a copy of the PDF. Discuss as a class, the key strategies to keep safe online. Ask students to use this information to create a poster using an app such as *Canva*. Explain that some apps allow users to invite others to assist with the creation of a product and the importance of only allowing friends they know and trust to work with them. Display the completed posters and conduct a class vote on the most effective posters. These could be displayed around the school.
- Write the online issues listed above on the whiteboard. Play to the class the following Australian Broadcasting Commission radio interview [Cyber safety](#) and ask them to use this information to predict which of these issues would be classed as criminal offences. Place a tick next to them. (For example, cyberbullying, image-based abuse, online abuse related to family violence, online scams and identity theft, gaming, and online child sexual exploitation/online grooming.)

Divide the class into six expert groups and allocate one of the ticked issues per group. Each group is to research their issue, identifying the key information using the following websites:

- [eSafety](#)
- [Netsmartzkids](#)
- [ThinkUKnow – online abuse](#)
- [Digital technologies hub](#)

After the groups have conducted their research, form new numbered groups, which will contain one “Expert” from each of the original groups. During this time, “Experts” will present their information to the other members of the group. Conclude the activity by asking for one interesting fact about each of the issues. Explain that the information they have gathered will be used in Lesson 5.

- Teachers wishing to explore this theme in more depth with their students can engage with [The YeS Project](#). This is a workshop-based digital and social health program that encourages young people to act as positive leaders and supportive friends in all their social spaces, especially online.

Lesson Idea 5: Cybercrime and the Law

As mentioned in Lesson Idea 3, the internet and other new technologies are providing opportunities for criminals to commit new crimes and to carry out old crimes in new ways. These crimes can be committed across multiple borders and target many victims simultaneously. Tools that a lot of us use, such as, high-speed broadband, peer-to-peer file-sharing and sophisticated encryption methods, can also assist criminals to carry out and conceal their activities. Ask students to watch the video on the [Australian Federal Police \(AFP\) website](#) and identify the latest technology used to commit cybercrime. Discuss how individuals can protect themselves from this form of malware.

Cybercrime law

The Australian Commonwealth has passed legislation to cover cybercrime offences. These laws are found in parts 10.7 and 10.8 of [the Criminal Code Act 1995](#). Each State and Territory also has its own legislated computer-related offences. Many are similar to Commonwealth legislation, but they have also passed legislation that covers online fraud and other technology enabled crimes.

- Discuss the information above with your students and direct them to the [AFP Cybercrime website](#). Ask them to identify and write down the cybercrime offences that are covered by Commonwealth legislation. Discuss their findings as a class. Direct students to research their own State or Territory cybercrime legislation using the [eSafety Commissioner website](#). Once completed students create a Venn diagram using an app such as *Canva* to compare and contrast the two levels of legislation. Conclude the activity by discussing students’ findings and suggest why there maybe similarities and differences.

The eSafety Commissioner

- The eSafety Commissioner has various functions and powers under Australian Government legislation to foster online safety. Ask students to research these [powers](#) and conduct a circle talk to enable them to share what they have learnt with others.

- Place students in two concentric circles (one circle within the other). This structure facilitates dialogue between students. Students in the inner circle face outwards, directly facing the student in the outer circle.
- Students stand facing each other to encourage active listening between partners.
- Ask students standing in the inside circle to start the sharing process by outlining one of the organisation's functions or powers.
- Remind the class to listen attentively to their partner and take turns.
- After sharing, ask the students standing in the outside circle to stand and move on two or three positions to meet a new partner. Use the same question again and repeat this process until all functions and powers have been listed.

Finish the activity by discussing as a class why they think these functions and powers were granted to the eSafety Commissioner.

- Cyberbullying can occur over the Internet, in instant messaging (IM) applications, chat rooms, social networking sites, blogs or gaming sites. It can also occur over the phone, by SMS or MMS, or other technologies. One in five young people have been bullied online. Show the [Cyber Bullying](#) page from the eSafety Commissioner site on an interactive whiteboard and conduct a shared reading of the forms of cyberbullying. Discuss as a class why people cyberbully and what the impacts can be. (Be prepared to intervene if the discussion proves disturbing for any of your students.) Explain that serious cases of cyberbullying can be a crime. Ask students to read [Youth Law Australia's Cyberbullying site](#) and make notes of the possible laws that cyberbullying can breach. Conduct a class brain dump of collected information. Write the information on the board. Explain to students that there are a range of options to report cyberbullying which will be discussed in the next lesson.

Lesson Idea 6: How You Can Report Cybercrime

This lesson will assist students to explore some of Australia's cybercrime reporting agencies and strategies for gathering evidence to prevent and/or report a cybercrime.

- Inform students that cybercrime has surpassed drug trafficking as the number one global crime. It has therefore become more important than ever to report these crimes to the appropriate authorities, whether it be a parent, a teacher, the local police, the Federal police, dedicated government agencies or non-government agencies. Emphasise the following information to your students.

If you are in Australia and in immediate danger or at risk of harm, call triple zero (000). This will link you immediately to the local police. Staying safe is your number one priority.

Display the [Australian Cyber Centre's Help page](#) on an interactive whiteboard and explain that there are a range of agencies to assist individuals, families and businesses if they are suffering a form of cybercrime. As you work through the information on the board, ask students to note down the agencies that handle reports of specific cybercrime activities. Explain that they are going to look at two of the agencies in more detail. The eSafety Commissioner and Crime Stoppers.

The eSafety Commissioner

- Explain that if students are suffering forms of online abuse and they are unable to resolve the issue with assistance from a parent, teacher or school administration, eSafety gives the following advice:
 - report cyberbullying to the platform on which it occurred; and
 - if the content is not removed within 48 hours you can make a [cyberbullying complaint](#) to eSafety.
- Most social media services have rules prohibiting cyberbullying and offer a complaints or reporting tool where you can ask for cyberbullying material to be removed. With other sites, services and platforms, you can report using the reporting links in [the eSafety Guide](#).
- The eSafety Commissioner has a platform where you can report cyberbullying, image-based abuse, and illegal and harmful content.

Divide the class into groups of three. Explain that each member of the group is to research the key facts pertaining to one of these issues using the eSafety Commissioner [Report](#). Once completed, each member of the group shares their findings to the others in the group. Conclude the activity by discussing the importance of collecting appropriate evidence if reporting online abuse. Students explore the eSafety Commissioner link [Collect evidence](#) and create a poster that summarises ways to collect evidence if suffering online abuse on popular apps such as Snapchat or Instagram.

Crime Stoppers

- [Crime Stoppers](#) is Australia's most trusted information receiving service for people wanting to share what they know about unsolved crimes and suspicious activity without saying who they are. They were first established in 1987 as an independent not-for-profit registered charity representing the collective eight Crime Stopper organisations operating in every state and territory in Australia. They work closely with police, media, and the community to help solve, reduce, and prevent crime by collecting information and passing on those details to police and other law enforcement agencies to help keep communities and families safe. As well as offering the community a way to actively to help solve and prevent crime, Crime Stoppers Australia also runs a number of crime awareness campaigns throughout the year.

(Teachers need to ensure that the following activity is supported by the creation of a safe learning environment such as noting if a student is feeling distressed by what they are

reading and needs to leave the classroom with appropriate support; and any discussion that occurs must include a 'no name' proviso and be respectful of others' feelings.)

- Explain that incidences of online child exploitation and online grooming have increased world-wide. Display and conduct a shared reading of [Unsafe or unwanted contact – signs to look out for](#) on an interactive whiteboard. Ask the following questions:
 - What are the warning signs that you may be receiving unsafe contact?
 - How can you protect yourself from unsafe or unwanted contact online?
 - What actions can you take if you are receiving unsafe or unwanted contact?
- Explain that in response to increased incidences of online grooming, Crime Stoppers Australia supported an e-safety campaign. Ask students to explore this [e-safety campaign](#) and discuss as a class the purpose of the campaign. Conduct a 3-2-1 Bridge strategy. This thinking routine unveils words, questions, and connections that students may associate with e-safety, and in particular online abuse. Ask students to write down three thoughts or ideas the e-safety campaign triggered for them and pair and share these with another student close to them. Ask if there are any general comments that students would like to share with the whole class. Now ask students to write down two questions they may have. If these questions cannot be answered at the time, make time at a later stage to provide responses. (This maybe a good opportunity to invite a member of the local police force technology team to speak to students.)

Conclude the activity by asking students to use the campaign material to create a check list of safety online practices and warning signs that students could leave by their computer. Share these as a class and post the most effective lists around the classroom.

Resources

Lesson Idea – Tuning In

- [Best Practice Framework for Online Safety Education](#) - website
- [Commit to Digital Citizenship!](#) – video
- [I'm a Digital Citizen](#) - poster
- [Nine themes of digital citizenship](#) – website
- [S3 Framework](#) – website
- [Nine themes of digital citizenship](#) – worksheet

Lesson Idea 1 – You as a Digital Citizen

- [Australian Values and Digital Citizenship](#) – worksheet
- [In our own words – children's rights in the digital world](#) – website (PDF)
- [What's in your Digital Footprint?](#) – video

- [‘What’s your brand?’](#) – lesson guidelines
- [‘What’s your brand?’](#) – presentation slides
- [Digital Compass](#) – online game
- [Young and eSafe](#) – website
- [Social Media Minimum Age law](#) – website
- [‘For the good of…’ Social media minimum age TV advertisement](#) – website
- [Compass Points](#) - worksheet

Lesson Idea 2 –Fake News and You

- [Fake news](#) – video
- [Text to Text, Text to Self, Text to World](#) – worksheet
- [Basic verification tips](#) – video
- [Real, LOLZ, oops or fake](#) – online game
- [Fakey](#) – online game

Lesson Idea 3 – Cybercrime

- [Annual Cyber Threat Report 2024 to 2025](#) – report
- [ASD / ACSC website](#) – website
- [Scamwatch](#) – website
- [Cyber threats: Note taking](#) – worksheet
- [Think you can spot a scam?](#) – online quiz

Lesson Idea 4 – Our Cyber Safety

- [The digital lives of Aussie teens](#) – research report
- [eSafetyyoungpeople](#) – website
- [Being Safe Online](#) – PDF
- [Cyber safety](#) – radio interview
- [eSafety](#) – website
- [Netsmartzkids](#) – website
- [ThinkUKnow – online abuse](#) – website
- [Digital technologies hub](#) – website
- [The YeS Project](#) – website and online workshop

Lesson Idea 5 – Cybercrime and the Law

- [Criminal Code Act 1995](#) – website
- [AFP Cybercrime](#) – website
- [eSafety Commissioner website – image based abuse laws](#) – website
- [eSafety Commissioner powers](#) - website
- [eSafety Commissioner cyber bullying](#) – website
- [Youth Law Australia’s Cyber Bullying](#) – website

Lesson Idea 6 – How You Can Report Cybercrime

- [Australian Cyber Centre's Help page](#) – website
- [Cyberbullying complaint](#) – website
- [The eSafety Guide](#) – website
- [eSafety Commissioner Report](#) – website
- [eSafety Commissioner Collect Evidence](#) – website
- [Crime Stoppers](#) - website
- [Unsafe or unwanted contact – signs to look out for](#) – website
- [e-safety campaign](#) – website

Further student enquiry

- [Fake news](#) – website
- [Internet and the Law](#) – online lesson
- [ThinkUKnow](#) – website

Assessment

- [Marking Key](#)
-

Further Student Enquiry

- Students explore more strategies for identifying [fake news](#) and use this information to create a toolkit poster to assist others to identify fake news.
 - Students explore The Internet and the Law in more depth using the following eSafety Commissioner [activity](#).
 - Students explore and discuss current e-safety campaigns and resources on State and Territory Crime Stoppers websites.
 - The [ThinkUKnow](#) website provides a range of parent, carer, teacher and student resources focusing on the prevention of online child sexual exploitation. Select a topic relevant to your student group and request a presentation.
-

Assessment

Formative

- Students write their own digital citizenship classroom manifesto.
- Students write their own definition and give examples of cybercrime.
- Conduct a class discussion about whether cybercrime legislation will need to change as technology improves and why this will be required?
- Conduct a class discussion about the role media can play to highlight the importance of e-safety.
- Students explain why, as good citizens, people should report cybercrimes through Crime Stoppers and/or the eSafety Commissioner.
- Students complete the Compass Points activity to explore their understanding and impact of the Social Media Minimum Age Law.

Summative

- Many of the activities in the lesson ideas can be used for summative assessment.
- Students present, in an appropriate format, their responsibilities as a digital citizen and how these reflect agreed Australian values.
- Students present, in an appropriate format, their understanding of the impacts of cybercrime on Australians and what action is being taken to protect Australian's democratic online rights.
- Students present, in an appropriate format, their understanding of how to be cyber safe.
- Students present, in an appropriate format, their views on how our legal system both protects citizens against technology crime and requires them to be active digital citizens.

This material can also be [accessed online](#)

© Unless otherwise indicated, this material may be used, reproduced and communicated free of charge for non-commercial educational purposes within Australian and overseas schools where the Australian Curriculum is taught, provided all acknowledgements are retained.