DTiF
Digital Technologies in focus
Initiative of and funded by the Australian Government Department of Education, Skills and Employment

acara AUSTRALIAN CURRICULUM, ASSESSMENT AND REPORTING AUTHORITY

# CLASSROOM IDEAS: Years 7–8

## Privacy and security


*Image source: Pixabay*


*Image source: Pixabay*

Students should explore the automated and non-automated processes through which data is collected, generated, stored and secured in digital systems.

Students need to consider how their behaviour online can provide access to their personal data, including breaching social and ethical protocols and jeopardising their safety. Also, as students engage in social media and online gaming, they need an awareness of the impacts that supplied data can have on their current and future lives, including social relationships and professional opportunities. By exploring this, students identify and explain how to protect against cyber security threats, manage the risks of sharing and curate their digital footprint.

Contents:

Years 7 and 8 students will learn:

- how to use multi-factor authentication to protect an account
- ways to password-protect data so it does not become compromised
- how to identify phishing and malware threats
- what data that existing systems and student solutions collect contributes to a digital footprint
- how to manage their personal data and reduce their digital footprint
- to assess if the data collected via websites and apps is essential to their purpose.

The following activities could be used in isolation or as part of a unit.

## Prior learning

### Is it authentic and credible?

Students should understand that although the internet might house millions of useful sources it can also contain misleading and unreliable information. The Credibility, Accuracy, Reasonableness, Support (CARS) checklist can be used by students to check the authenticity of information and determine whether it might be fake or outdated. See useful links for further information. There are some great websites for students to explore. Provide students with a mix of real and fake websites and have them answer questions such as:

1. University of Antarctica: antarcticaedu.com
    a. If you could go to this university, what would you study?
    b. Would you recommend this university to your friends? Why or why not?
2. Australian Museum – drop bears: australian.museum/learn/animals/mammals/drop-bear
    a. Where are drop bears likely to be located?
    b. What is your best defence against a drop bear?
3. Snowboarder chased by bear: www.youtube.com/watch?v=vT_PNKg3v7s (1.25 min)
    a. What would you do in this situation?
    b. Describe your thoughts on this video and justify your opinion.
4. Banksy currency: numismatics.org/pocketchange/banksy
    a. Explain how Banksy achieved the stunt.
    b. What advice would you give to a person in the crowd who caught one of the notes on how to detect it was a fake?

Activity: Students present their findings to others and explain how the CARS checklist could help them to determine authenticity of information.

## Lesson 1 – Multi-factor authentication

### Review

There are many ways that a person can protect their privacy and identity when they go online. Ask students:

- How well do you think you protect your identity?

Explain that a person's digital footprint is valuable and should be protected at all costs. If at any time a student feels that their identity is compromised online then they should immediately change their password and seek guidance from a trusted adult.

Ask students to consider how some large corporations try to protect users and their privacy.

- Why is it so important that you protect your identity and your password?
- What is multi-factor authentication and how does it work?
- How does it help protect your online identity and data?

### Teacher notes: Multi-factor authentication. What is it and why is important?

Multi-factor authentication (MFA) is a security technology that requires multiple methods of authentication from independent categories of credentials to verify a user's identity for a login or other transaction. MFA combines 2 or more independent credentials: what the user knows, such as a password; what the user has, such as a security token; and what the user is, by using biometric verification methods, for example, a fingerprint.

In short, there are 3 factors that can be used for MFA. They are:

*Image source: Pixabay*

- what you know
- who you have
- what you are.

Sometimes another 2 factors are used:

- where you are
- what you do.

If you think of items that explore what you know, these include a password that only you know or a personal identification number (PIN) for your bank or for entering a building. But if your password or PIN is compromised then it would be easy for someone to access your bank account or website. This is why it is important to consider a secure password along with a multi-factor solution. For example, a bank will send you a numbered code after you have correctly entered your password to confirm it is you.

The smartphone is an example of 'what you have'; it proves it is you – unless, of course, your phone is stolen or compromised. View the following video that explains how MFA works: www.youtube.com/watch?v=STI6vtKtHpU (5 min)

#### Creating a password

There are several secure methods you should consider when creating a password. The Computer Science Field Guide has some resources on creating a secure password that with MFA offers a higher level of protection. See www.csfieldguide.org.nz/en/chapters/coding-encryption/storing-passwords-securely

## Group task: Defeating biometrics

There are many ways to unlock digital devices. Students might be familiar with fingerprint and facial recognition technologies being incorporated into smartphones to unlock them. Some automated telephone systems rely on voice recognition to determine a user's identity. Personal assistants such as Alexa and Siri will only respond to voices they are familiar with. For biometrics to work, devices need to be trained and personal biometric data such as fingerprints, facial data and voice data need to be stored on the devices for comparison. Read more about biometrics in Resources.

Ask students if they have heard of deep fakes. Watch this video as a class and discuss the ramifications: www.youtube.com/watch?v=gLoI9hAX9dw (3 min). Voices can be manipulated using audio software. Read this article with students: venturebeat.com/2016/12/18/the-ethics-of-hacking-your-voice/ and discuss the ethics of voice manipulation.

Group activities:

1. Can fingerprints be manufactured to trick digital devices? Explore different materials such as putty, wax, PVA glue or synthetic materials to create fingerprints to see if they can then unlock a device utilising fingerprint recognition.
2. Can facial recognition be defeated? Test whether sunglasses, a mask or a hat affect the accuracy of facial recognition.
3. Can a personal digital assistant be tricked? Provide students with audio software to test changing their voices to determine if it affects voice recognition software such as Siri or Alexa.

*Image source: Pixabay*

## Multi-factor authentication – Student task

Purpose of task: to investigate different methods of securing passwords

Explore the different levels of security available and how you might use them yourself. Complete the following activities with a partner:

**Cyber security – Vocabulary Journal**

As you work through the tasks, add technical words as you encounter them, research their meaning, and use an example to show your understanding.

Seek help from others if needed.

| Word | Meaning | Example |
|---|---|---|
| encryption | | |
| multi factor authentication | | |
| hashing passwords | | |
| brute force attack | | |
| phishing | | |
| | | |
| | | |
| | | |
| | | |

*Figure 1: Cyber security vocabulary journal (see Appendix)*

1. Use the Cyber security vocabulary journal (Figure 1; see Appendix) to build up a dictionary of relevant terms and words that help you to explain the value of keeping your data secure and you safe online.

Here are some terms to explore. What do they mean?

a) encryption

b) hashing passwords

c) brute force attack

d) phishing attack

e) spear phishing attack

f) whaling attack.

2. List all the important details that should be considered when creating a password. Create a set of instructions for your immediate family to help them create a password that would be difficult to brea

The chapter on encryption in the CS Fieldguide is good source to help your investigation. Look at some of the terms described and determine for yourself what is the best way for you to protect your identity online with a secure and safe password. Look at how the use of multi-factor authentication further strengthens your safety online.

3. How could you create the perfect password that cannot be broken? What would such a password look like?


*Image source: Pixabay*

## Lesson 2 – Loyalty cards

Customer loyalty cards are used by businesses to encourage customers to return to their store for repeat business. When customers receive the loyalty card, each purchase is recorded on the card, which in turn encourages customers to return to the business over and over again to receive a reward.

**Can loyalty cards compromise your privacy?**

We are often asked by stores or large businesses if we wish to receive rewards for accessing their loyalty card program. Think of airlines or the supermarkets that you visit each week and whether you are asked if you are part of their loyalty program.

*Image source: Pixabay*

Ask students:

- Why do businesses offer gifts whether they be large or small for your custom?
- What do they receive in exchange from you joining their program?

There is increasing concern about the security of customer data stored on external servers. Cybercriminals are becoming increasingly active in hacking into the servers that store the individual data of customers.

There is a growing concern around identity theft and credit card fraud. It is becoming easier for criminals to connect loyalty cards with credit and debit cards. Once access has been gained, they are able to commit larger crimes.

There are many enticements offered to customers but the data that is requested when joining a loyalty program has some risks involved.

In some cases, the information customers provide can be used against them. In some court cases stores have been known to use customer data to defend themselves in case of being sued for an accident. For example, one supermarket in the USA defended itself against litigation when a customer fell and was hurt, citing the purchasing habits of the aggrieved customer, accusing him of having a drinking problem based on his purchase of alcohol from their store.

Generally, customer data is held on third-party servers. Recent news reports highlight the breaches by hackers who have accessed stored data. Loyalty cards not only have a customer's name, address and telephone number, but are often linked to partial credit and debit card information as well.

Identity thieves use this information and combine it with information from other sources. It is possible for criminals to put together separate pieces of data to build a credible file on people to access their bank account or steal their identity.

Ask students:

- How can you protect your and your family's data?

Customers should weigh up the benefits of joining a loyalty card scheme with the risk of sharing their private data for the rewards on offer. Here are some basic ground rules you could establish with students:

**Watch what you share**

- Do not put any information that might be used for identifying you online.
- Ask: do they really need my parent's driver licence details or my home address? Where possible, leave these spaces blank or consider whether it is worth joining.

**Consider a secondary email address**

- Have a second email address for receiving email from the business and also to protect you from spamming your main email account.

**Use password protection**

- Be sure to use a secure password (see the task on multi-factor authentication) and perhaps use one that is unique to your shopping cards and not your more sensitive applications used online.

**Mind the app**

- Some loyalty cards have online versions that you can download to your phone. Just be sure that the app is authentic and not a copy that is trying to capture your data.

By following a few common-sense precautions with loyalty programs, customers can reduce the risks to their privacy and get the rewards they want.

## Loyalty cards – Student task 1


*Image source: Pixabay*

Purpose of task: to design a loyalty card and data collection methods

Do you have any loyalty cards of your own?

Does your family use loyalty cards? For example, cards that are used to collect points when you are shopping at the supermarket or when your family is booking flights.

1. Create a list of each of the loyalty programs you and your family might have.
2. What personal data did each card's loyalty program seek when joining?
3. What data was required and what data was optional?
4. Do you think it was necessary to provide that much personal data?
5. What benefits did the company offer? For example, purchase 10 cups of coffee, get one free.
6. Was the joining form completed online or on paper?

**Create your own loyalty card program**

7. Design a card for your own loyalty card program. Design the card in such a way that it will bring your potential customer back to your store.
8. Create the online form for registering using Google Forms or another similar program such as Microsoft Word or Excel. Design your form and the questions you wish to ask.
   - What data are you going to request from your customer?
   - Is it necessary to have all their details or do you want the data for keeping in contact with them for other purposes?

9. How are you going to secure the data you collect so that cybercriminals cannot steal it? This is an important part of any data you collect about your customers. It will make customers feel safe – and you do want them to trust you and your business!

## Loyalty cards – Student task 2

Purpose of task: create a board game to simulate the use of loyalty cards to teach others about what data they collect

Create a board or card game with a partner that involves the collection of loyalty cards and the winning of prizes. You might like to look at some of your board games at home. For example, Monopoly might lend itself to a game that can be modified to create a loyalty card adventure.

*Image source: Pixabay*

**Create a loyalty card or board game**

- Plan how points will be collected.
- Consider when the player might have to go back a number of spaces. Did they give away some unnecessary personal data?
- Be specific with your instructions, rewards and penalties.
- Include ways that players can learn to look for security protections while using store cards.

Alternatively, create an electronic game to simulate customers using store cards. There are some cyber safety and security courses that give some ideas on building online activities:

Hour of Code: hourofcode.com/au/learn

Code Club: www.codeclubau.org/projects

## Lesson 3 – Data security

Securing data safely is extremely important for individuals and for any online service that has responsibility for a user's personal information. For example, a bank has to be constantly vigilant to an attack on their systems to protect the private data it holds.

Ask students:

- What data might a bank hold on its servers?

Discuss with students that this is not only a person's name, age and address but also other important personal data that allows access to their personal finances and other private, confidential material. The threat of identity theft is a very real concern that we all need to be aware of when sharing data online.

*Image source: Pixabay*

Ask students:

What do we mean by data?

- What is identity theft and how might it affect you, should it happen?
- What is required to recover from such a breach of security?
- How do institutions protect your data?

Data is raw information. It can be represented in a number of formats: text, numerical, a photograph or drawing or even as a digital sound wave. It is what is done with the data that creates and transforms the raw data into information.

Information is valuable. When providing data individuals should ask who the data is for and what value it has. Collected data is interpreted and patterns emerge that assist in decision-making and policy formation. For example, the 2021 Census provides vast amounts of information on the population of Australia. From this raw data, decisions on housing, schools, hospitals, transport and so on are made at government level to provide and support infrastructure into the future.

Weather bureaus and forecasters rely on the data collected from the many sensors around Australia to predict future weather events. This data is particularly important during times of high fire danger or the cyclone season in northern Australia.

In the context of privacy and security awareness, it is important for students to consider different types of data shared and viewed online.

Activity: Students think about all the different types of data they shared online this week (photos, social media posts or private messages)

Ask students:

- What types of data did you share?
- What kind of information did you reveal about yourself?
- How safe did you feel in freely passing on your personal data?
- Was the personal information you shared really necessary to provide for the websites you accessed?

## Data security – Student task 1

*Figure 1: QR code 1*

*Figure 2: QR code 2*

*Figure 3: QR code 3*

*Figure 4: QR code 4*

Purpose of task: to investigate QR codes and the data they represent

QR codes are now more and more commonly used for providing shortcuts to websites and for building security for users.

1. How do QR codes work and are they secure?

Real estate agents have been using them for many years on their 'For Sale' boards when selling houses. They eliminate the need for the user to write out a long email address.

2. How else might they be useful?

During the COVID-19 pandemic, people have been required to scan the QR code of any shop or venue before entering.

3. Why were there some concerns about privacy when there was a requirement to scan your whereabouts?
4. How might the data be stored and how might it be used?

The QR code scan has been a powerful tool for contacting people who may have been in the vicinity of a positive COVID case. It has helped in managing the pandemic and keeping us safe.

5. How else might a QR code be used for good?
6. Can you see security issues that might be a concern?
7. What are your views on the safety of QR codes and how they might be used for good and for bad?
8. Follow the QR codes on this sheet (Figures 1–4). Record where each one goes to.

There are a number of resources available to create your own QR code. Here is an example: www.the-qrcode-generator.com/

9. Create your own QR codes for websites that you have found on privacy and security.
10. Have a friend use the camera on their phone or device to test your link.

There are vulnerabilities in so many of the web tools we use every day. BE AWARE that it is possible for the free QR code generators to gather the information you are building and that the QR codes you create might also take you to a page advertising their products.

11. What else might work more securely and can you be sure your security ideas won't be hacked?

## Data security – Student task 2

Purpose of task: to create a class survey tool

1. When you are online what information do you share with others?
2. Do you upload images of yourself, your environment, your friends and family?
3. Think of all the data you give away online in your social media environments. How safe do you think you are in sharing your personal data and how confident are you in the security of the servers that hold your data?

### Create a class survey tool

*Image source: Pixabay*

In pairs, build a set of questions to survey 10 of your classmates to find out what sorts of party activities, venues, dates or events suit them.

1. What questions are really required to assist you in planning a party?
2. How safe is the data you collect? Where will it be stored?
3. Use an online survey tool, Google forms or spreadsheet to create your own survey and test it with another pair to see how they feel about sharing their personal information with you.
4. See if you can refine your questions to suit their concerns. Publish your survey and collect and organise data from 10 classmates.
5. Visualise the data so it is easier to interpret.
6. Research ways your data could be vulnerable to attacks and devise a way or ways in which to add tighter security to the valuable information in your database.
   Plan a secure means to build protection for the passwords you use to access your central database and imagine what types of biosecurity, for example retina, fingerprint might be developed in the future. Refer back to the lesson on multi-factor authentication.

## Links to the Australian Curriculum (v8.4)

Table 1: Aspects of the Australian Curriculum: Digital Technologies Year 7 and 8 (v8.4) which may be addressed depending on the task

<table>
<tr><td>Digital Technologies<br><br>Achievement standard</td><td colspan="3">By the end of Year 8, students distinguish between different types of networks and defined purposes. They explain how text, image and audio data can be represented, secured and presented in digital systems.<br>Students plan and manage digital projects to create interactive information. They define and decompose problems in terms of functional requirements and constraints. Students design user experiences and algorithms incorporating branching and iterations, and test, modify and implement digital solutions. They evaluate information systems and their solutions in terms of meeting needs, innovation and sustainability. They analyse and evaluate data from a range of sources to model and create solutions. They use appropriate protocols when communicating and collaborating online.</td></tr>
<tr><td>Strand</td><td colspan="3">Knowledge and understanding<ul><li>Digital systems</li></ul>Processes and production skills<ul><li>Collecting, managing and analysing data</li><li>Evaluating</li><li>Collaborating and managing</li></ul></td></tr>
<tr><td>Content descriptions</td><td colspan="3"><ul><li>Investigate how data is transmitted and secured in wired, wireless and mobile networks, and how the specifications affect performance (ACTDIK023)</li><li>Acquire data from a range of sources and evaluate authenticity, accuracy and timeliness (ACTDIP025)</li><li>Analyse and visualise data using a range of software to create information, and use structured data to model objects or events (ACTDIP026)</li><li>Evaluate how student solutions and existing information systems meet needs, are innovative, and take account of future risks and sustainability (ACTDIP031)</li><li>Plan and manage projects that create and communicate ideas and information collaboratively online, taking safety and social contexts into account (ACTDIP032)</li></ul></td></tr>
<tr><td rowspan="2">Key concepts</td><td rowspan="2"><ul><li>digital systems</li><li>interactions</li><li>impacts</li><li>data collection</li><li>data interpretation</li></ul></td><td>Key ideas</td><td>Thinking in Technologies<ul><li>Systems thinking</li></ul></td></tr>
<tr><td>General capabilities</td><td><ul><li>ICT capability</li><li>Literacy</li><li>Critical and Creative Thinking</li><li>Personal and Social capability</li><li>Numeracy</li><li>Ethical Understanding</li></ul></td></tr>
<tr><td>Cross-curriculum priorities</td><td><ul><li>Sustainability</li></ul></td><td>Learning area or subject connections</td><td><ul><li>Mathematics</li><li>Health and Physical Education</li></ul></td></tr>
</table>

## Learning area or subject connections

**Mathematics**
The Australian Curriculum: Technologies provides contexts within which Mathematics understanding and problem-solving skills can be applied and developed. Digital Technologies and Mathematics share a focus on computational thinking, in particular, data acquisition and interpretation, models and simulations, and generalising.

The Digital Technologies curriculum supports students to apply the knowledge and skills that underpin pattern recognition, data acquisition, and interpretation and representation, which form the basis of the Mathematics strand, *Statistics and probability.*

**Health and Physical Education**
The Australian Curriculum: Technologies takes account of what students learn in Health and Physical Education. In Digital Technologies, students have an opportunity to apply their knowledge of and skills in privacy, safety (seeking help and engaging respectfully) and applying personal protective behaviours as they expand their communication and collaboration experience into online and networked environments.

## Resources

- Australian Curriculum – Curriculum connections – online safety
  www.australiancurriculum.edu.au/resources/curriculum-connections/portfolios/online-safety

### Lesson 1 – Multi-factor authentication

- Introduction to multi-factor authentication
  www.youtube.com/watch?v=STI6vtKtHpU
- Storing passwords securely
  www.csfieldguide.org.nz/en/chapters/coding-encryption/storing-passwords-securely
- What are biometrics and are they safe?
  us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html
- Phishing – scam emails
  www.cyber.gov.au/acsc/view-all-content/threats/phishing
- Phishing, spear-phishing and whaling – same same but different. Here's how …
  computerone.com.au/phishing-spear-phishing-whaling-whats-difference
- Coding – encryption
  www.csfieldguide.org.nz/en/chapters/coding-encryption

### Lesson 2 – Loyalty cards

- How do companies use my loyalty card data?
  www.bbc.com/news/technology-43483426
- What is my data worth?
  thenextweb.com/news/loyalty-programs-cost-you-your-personal-data-are-the-rewards-worth-it
- How much data is shared about you?
  youtu.be/bqWuioPHhz0
- Canva
  www.canva.com

- Adobe Photoshop and Illustrator (for schools with education licences for student use) could be used in a design and graphics class for students to explore loyalty card design. This would complement a design and graphics course.
  www.adobe.com/au/lead/creativecloud/all-apps.html

### Lesson 3 – Data security

- QR Code Generator
  www.the-qrcode-generator.com
- Google Forms
  www.google.com.au/forms/about
- Digital Technologies Hub – Data and information
  https://www.digitaltechnologieshub.edu.au/teachers/scope-and-sequence/7-8/data-representations/data-and-information

## Useful links

- The CARS checklist
  www.nhcc.edu/student-resources/library/doinglibraryresearch/cars-checklist
- Poster explaining MFA
  searchsecurity.techtarget.com/definition/multifactor-authentication-MFA
- Data Crumbs slide deck from CSER Adelaide
  universityofadelaide.app.box.com/s/mzbf3hj6agf3m2ncedoaozwk4fccftpi
- Cyber safety and security MOOCs
  csermoocs.appspot.com/
- Cyber security and cyber safety poster from CSER Adelaide
  universityofadelaide.app.box.com/s/p261688r3h7qcvyb7tmk3zq28u1qayeh
- Multi-factor authentication explained
  searchsecurity.techtarget.com/definition/multifactor-authentication-MFA
- ACCC Scamwatch
  www.scamwatch.gov.au/types-of-scams
- eSafety education
  www.esafety.gov.au/educators
- eSafety education – Keeping your online accounts secure
  www.esafety.gov.au/young-people/keeping-your-online-accounts-secure
- eSafety education – Protecting your identity
  www.esafety.gov.au/young-people/protecting-your-identity
- eSafety education – Consent for sharing photos and videos
  www.esafety.gov.au/young-people/consent-sharing-photos-videos
- eSafety education – Your digital reputation
  www.esafety.gov.au/young-people/your-digital-reputation
- eSafety education – Be Deadly Online
  www.esafety.gov.au/educators/classroom-resources/be-deadly-online
- eSafety education – What's your brand?
  www.esafety.gov.au/educators/classroom-resources/whats-your-brand
- Digital Technologies Hub – Cyber safety
  www.digitaltechnologieshub.edu.au/families/cybersafety
- Learning for Justice – Privacy and Security Online
  www.learningforjustice.org/classroom-resources/lessons/privacy-and-security-online

*All images in this resource are used with permission*

# Appendix

# Vocabulary journal

# Cyber security – Vocabulary journal

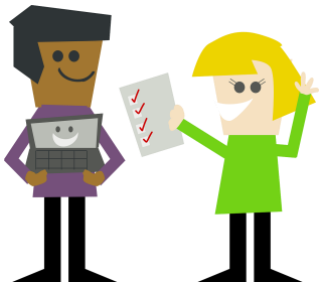

*Image source: Pixabay*

As you work through the tasks, add technical words as you encounter them, research their meaning, and use an example to show your understanding.

Seek help from others if needed.

| Word | Meaning | Example |
|---|---|---|
| brute force attack | | |
| encryption | | |
| hashing passwords | | |
| multi-factor authentication | | |
| phishing | | |
| | | |
| | | |
| | | |
| | | |

(Add rows if needed)