DIGITAL TECHNOLOGIES HUB

Australian Curriculum V9.0

Privacy and security

The protection of data when it is stored or transmitted through digital systems.

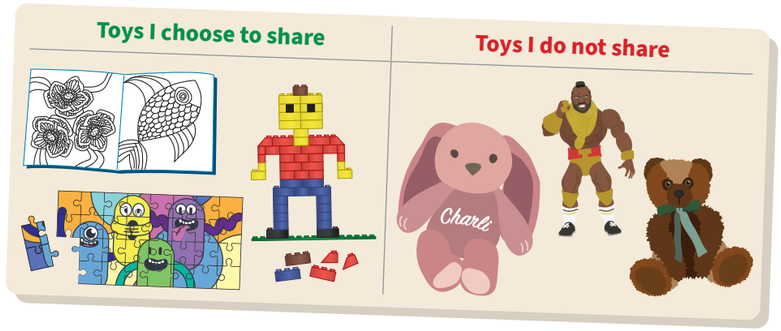
ACARA, 2022

Foundation

I can identify personal data that belongs to me.

Personal data, such as name and address, can identify someone. It is important for students to be careful online. They should ask a trusted adult before sharing any personal information to stay safe.

Use an analogy to talk about personal data, for example, your data is like your toys. What toys do you have? They belong to you and you can choose to share them or not. Talk about the way we keep data on computers safe with a password.

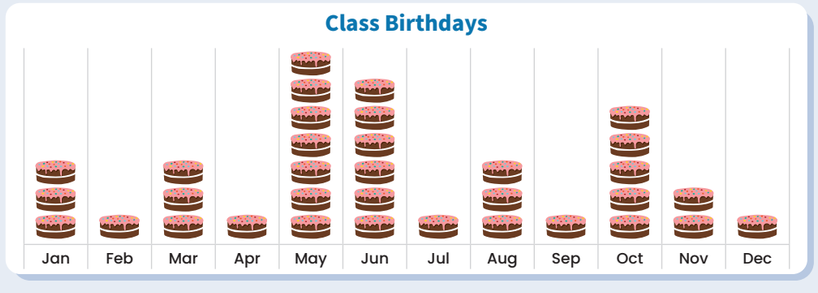


Incorporate online safety. Discuss what students should do if they see something on screen that frightens or upsets them. Create a list of actions to take in such situations.

Achievement standard	They represent data using objects, pictures and symbols and identify examples of data that is owned by them.
Content descriptions	Identify some data that is personal and owned by them | Digital Technologies AC9TDIFP01

Related content

When collecting and representing data about themselves, discuss data that we keep private and not share publically.



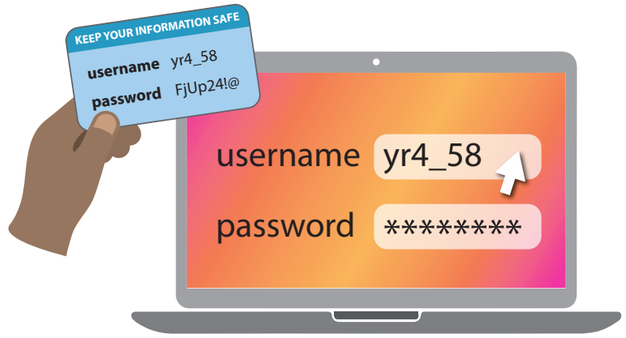
Mathematics	Collect, sort and compare data represented by objects and images in response to given investigative questions that relate to familiar situations. | Mathematics AC9MFST01

Years 1–2

I can identify some dangers of sharing data online and identify data that I must keep private.

Online situations sometimes ask for personal data, which can reveal a person's identity and location. To stay safe, students need to be aware of the dangers, avoid sharing personal data and seek a trusted adult's guidance before sharing anything online.

Use the logging in process, when students access their school account, to discuss tips on keeping their login details safe. At this stage, it is typical that the teacher provides a username and password.



Charlotte Blake

69C Springs Road
Springvale
NSW 4020

06/11/2014

charleybb@snailmail.com.au

Use video resources, such as those developed by the eSafety commission, to spark discussion and help students understand what personal data is and why it's important to protect it.

As a class, discuss scenarios where students need to decide whether to share personal information online. For example, 'You want to sign up for a new game that asks for your phone number and address. What should you do?'

Achievement standard	Students recognise that digital tools may store their personal data online.
Content descriptions	Access their school account with a recorded username and password | Digital Technologies AC9TDI2P06 Discuss that some websites and apps store their personal data online | Digital Technologies AC9TDI2P07

DIGITAL TECHNOLOGIES HUB

Australian Curriculum V9.0

Privacy and security

The protection of data when it is stored or transmitted through digital systems.

ACARA, 2022

Years 3–4

I can create and use a secure, easy-to-remember password. I can describe ways to protect my personal data and how it may be at risk, being careful about what I share online.

Creating an easy-to-remember, hard-to-guess password is important for protecting data stored online. Personal data, such as name, age and interests, forms a digital identity that can be used to personalise online experiences but also requires careful management to protect privacy and security.

Explore creating an easy-to-remember and hard-to-guess password, such as using three unrelated words combined. Discuss tips for creating strong passwords and protocols to keep them safe.

Tips for creating strong passwords

1. Use letters and numbers
2. Use a minumum of 8 characters
3. Don't include any personal information
4. Use characters such as (, &, $, *, %
5. Use a mixture of capitals and lower-case letters
6. Use something that is easy to remember
7. Change the password every 6 months
8. Use a different password for all online accounts

Use images of fictional characters with identifying visual clues. Reveal parts of the covered photograph in a 'guess who' type game to reveal more and more information about the person or persons behind the pieces covering the image.

Create an avatar for your online profile that represents you but does not reveal personal details. Describe when to use this avatar and how it may help protect your privacy and identity.

Achievement standard	Students identify their personal data stored online and recognise the risks.
Content descriptions	Access their school account using a memorised password and explain why it should be easy to remember, but hard for others to guess | Digital Technologies AC9TDI4P08 Identify what personal data is stored and shared in their online accounts and discuss any associated risks | Digital Technologies AC9TDI4P09

Years 5–6

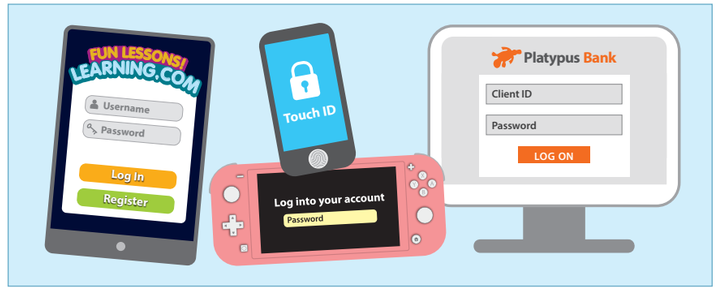
I can explain the safe use of passphrases and why using unique ones is important. I can also identify online activities that affect my digital footprint and explain how permanent information may affect my privacy.

A password is a string of characters used for authentication, while a passphrase is a longer, more secure phrase used in a similar way. Creating a secure, easy-to-remember passphrase helps us protect our online data.

passphrase: IL!keCheese!@#$]

As we use online websites and apps, we share personal data, such as our name, email and interests, and this is what shapes our digital footprint.

Create a poster showcasing how passwords are used in daily life, like smartphone biosecurity, online banking, gaming, and access to courses. Highlight the importance of strong, unique passwords for each.



Students reflect on their online presence by drawing a footprint to represent their digital footprint. Digital footprints are formed through activities like visiting websites, clicking links, watching videos or playing games online. Websites use cookies to remember information such as usernames, game progress and location to personalise experiences.

Create a video illustrating online behaviours that are safe (for example, strong passwords, cautious sharing) versus those that are unsafe (for example, public sharing, clicking on suspicious links). Highlight the permanence of online actions and their long-term impacts on personal and professional lives.

Achievement standard	Students identify their digital footprint and recognise its permanence.
Content descriptions	Access their school account with a recorded username and password | Digital Technologies AC9TDI2P06 Access multiple personal accounts using unique passphrases and explain the risks of password re-use | Digital Technologies AC9TDI6P09 Explain the creation and permanence of their digital footprint and consider privacy when collecting user data | Digital Technologies AC9TDI6P10

DIGITAL TECHNOLOGIES HUB

Australian Curriculum V9.0

Privacy and security

The protection of data when it is stored or transmitted through digital systems.

ACARA, 2022

Years 7–8

I can explain how multi-factor authentication prevents unauthorised access to online accounts. I can identify common techniques used in phishing scams to exploit susceptible users and I can also review and manage my digital footprint.

Multi-factor authentication prevents unauthorised access to online accounts by requiring additional verification steps beyond just entering a password, such as providing a one-time password or token.

Phishing scams often employ various techniques to identify and exploit susceptible users. One common tactic is the use of email addresses from unofficial domains, creating the illusion of legitimacy, such as pretending to be a well-known online retailer.

A person's online activity contributes to their digital footprint. To manage one's digital footprint, a person should always consider privacy implications and only selectively share content online, and adjust privacy settings on social media to control who sees their content.

Create a poster or infographic that explains various levels of security. Include multi-factor authentication, and describe how it works and its benefits above some other forms of authentication. Include statistics about data protection, such as frequency of password breaches and data leaks, and show the types and levels of security a person can put in place.

Research and create a presentation focusing on strategies for reviewing and managing your digital footprint across online tools. Include examples of media services that track user habits, such as music streaming platforms that curate personalised playlists based on listening habits.

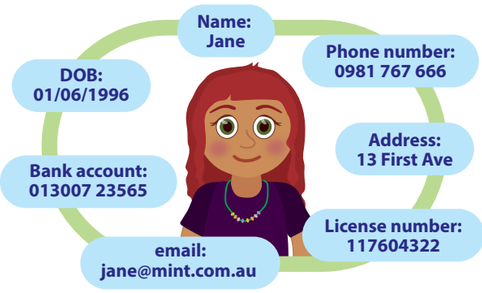
Achievement standard	Students manage their digital footprint.
Content descriptions	Explain how multi-factor authentication protects an account when the password is compromised and identify phishing and other cyber security threats | Digital Technologies AC9TDI8P13 Investigate and manage the digital footprint existing systems and student solutions collect and assess if the data is essential to their purpose | Digital Technologies AC9TDI8P14

Years 9–10

I can explain how private information moves through a system and identify when it's most vulnerable to a cyber attack. I can use the Australian Privacy Principles to evaluate how well user information is protected in online systems.

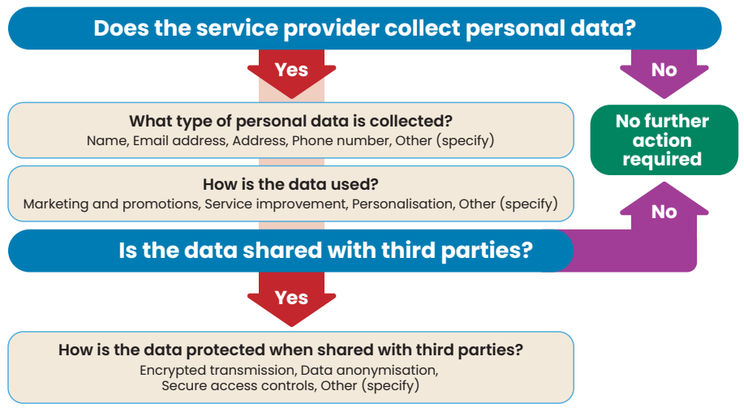
Private information is stored and transmitted in a digital system, and its vulnerabilities to cyber attacks can be identified by understanding the flow of this information.

The Australian Privacy Principles are a set of principles that regulate how Australian government agencies and some private sector organisations handle, use and manage personal data. They are designed to protect individuals' privacy rights by setting standards for the collection, use and disclosure of personal data.



Analyse scenarios to identify assets (such as personal information), threats (such as phishing) and vulnerabilities (such as weak passwords) using the cyber security threat model. Propose mitigation strategies (for example, multi-factor authentication) to protect against these threats.

Create a privacy audit toolkit for apps and websites, inspired by the Australian Privacy Principles. Design interactive elements like quizzes or decision trees to help users understand how their data is handled and suggest improvements.



Achievement standard	Students apply privacy principles to manage digital footprints.
Content descriptions	Develop cyber security threat models, and explore a software, user or software supply chain vulnerability | Digital Technologies AC9TDI6P09 Apply the Australian Privacy Principles to critique and manage the digital footprint that existing systems and student solutions collect | Digital Technologies AC9TDI6P10