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.

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.

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.

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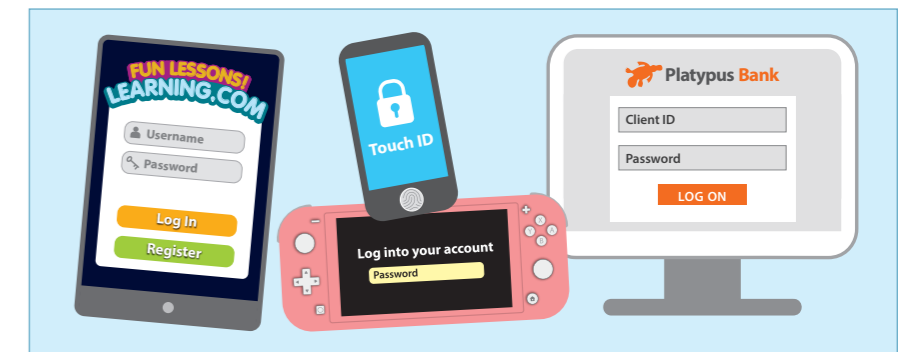
Students reflect on their online presence by drawing a footprint to represent their digital footprint. Digital footprints are formed through activities like visiting websites, clicking links, watching videos or playing games online. Websites use cookies to remember information such as usernames, game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

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