



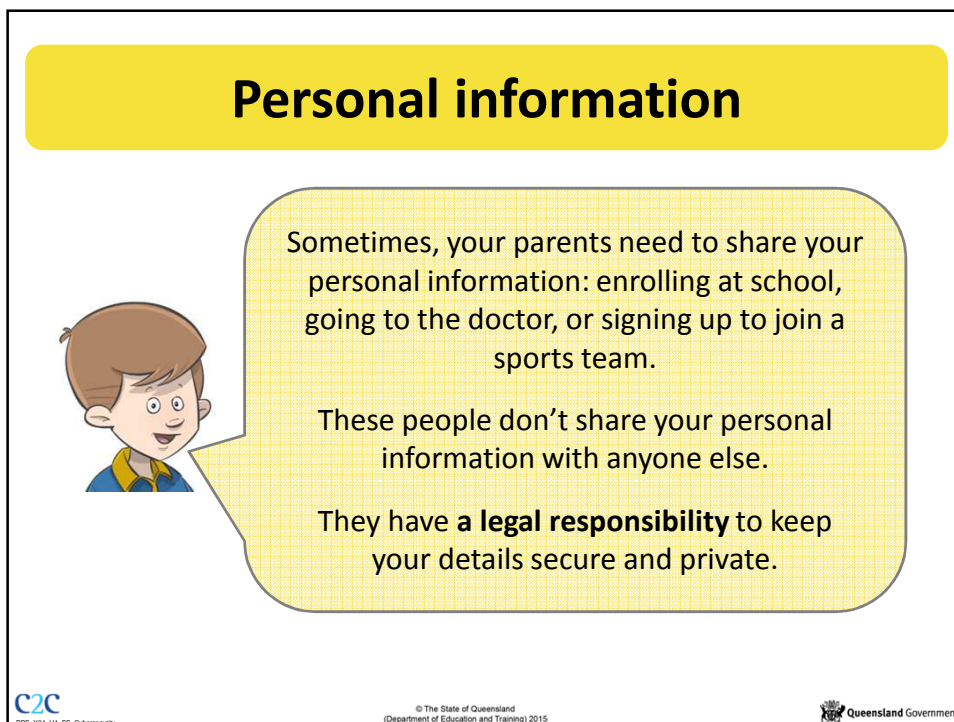
Cybersecurity

Protecting your personal information and privacy

Use this slideshow with the sheet *Cybersecurity*

C2C PPS_Y04_U4_SS_Cybersecurity © The State of Queensland (Department of Education and Training) 2015 Queensland Government

This slide features a yellow header with the title 'Cybersecurity' and the subtitle 'Protecting your personal information and privacy'. Below the header, there is a trail of black paw prints leading from the top left towards the bottom right. A line of text reads 'Use this slideshow with the sheet Cybersecurity'. The footer contains the C2C logo, copyright information for the State of Queensland, and the Queensland Government logo.



Personal information

Sometimes, your parents need to share your personal information: enrolling at school, going to the doctor, or signing up to join a sports team.

These people don't share your personal information with anyone else.

They have a **legal responsibility** to keep your details secure and private.

C2C PPS_Y04_U4_SS_Cybersecurity © The State of Queensland (Department of Education and Training) 2015 Queensland Government

This slide has a yellow header with the title 'Personal information'. On the left, there is a cartoon illustration of a young boy with brown hair, wearing a blue shirt. A speech bubble points from the boy to a text box on the right. The text box contains three paragraphs explaining that parents share personal information for specific reasons like school or sports, that they do not share it with others, and that they have a legal responsibility to keep it secure. The footer includes the C2C logo, copyright information, and the Queensland Government logo.

Personal information

Personal information is unique to each person and helps to identify them. It may include:

- full name
- school name
- date of birth
- address
- phone number
- email address.



Joining online communities

To join an online community, you may need to use your personal information to sign up and complete forms.

The people or group who run the community should keep your personal information secure, so no one else can see it or use it.

You have the responsibility of setting up a secure profile and password that does not use any of your personal information.



Online profiles



Websites and communities often ask you to set up a profile page, as a way of displaying who you are to other users. It's like your identity!

Children **should not** share pictures or information with personal details, such as their address, school, sports team, phone number or full name.

Did you know your school uniform lets people know exactly where you will be during the day?

Online settings

To keep your profile secure, you will need to set up a username and password.

These **should not** include any personal information that can easily identify you.

You should also change your settings to 'private' or 'friends only', so you only share information and images with people you know.

Otherwise, you have no control over who might see it!



Creating a secure password

Set up your password with care!

Do:

- make it at least eight (8) characters in length
- combine numbers and upper- and lowercase letters
- add special characters and symbols (! @ # \$ % * - + = . < > : ;)
- change your password regularly.

Don't:

- use nicknames, birthdates or names of family, friends or pets
- share your password with anyone – not even with friends
- give your password to anyone else to use
- store your password on your electronic device or write it down
- keep the same password for a long time and/or use it on many sites.

Why create a secure password?

- If someone guesses or finds your password, they could have access to your profile and your personal information
- A secure password stops people from taking your information, or pretending to be you
- A secure password helps protect you and other users in online communities

Protecting personal information



- **Cookies** are information files that websites collect and store on your device about you and your online activity.
- A **virus** is a program or download that does bad things to your computer or device, including stealing information.
- The **settings** on your electronic device can help you control the information you share. There is also software that can be put on your device to protect it from viruses. All devices are different, so ask an adult if you need help.
- **Scams** are tricks by people online to get important information or money from you. Scams are usually a **message** or **pop-up ad** that looks real, but is not. They may offer you free items, but there is actually a hidden cost, or you do not get what you were promised.

Cybersafety warnings

- Check sites for age limits
- Don't share passwords
- Don't trust everyone online
- Avoid 'checking in' your location
- Avoid clicking on pop-up advertisements
- Don't forward inappropriate images, videos or messages
- Don't respond to unwanted contact from people



Cybersafe practices

- Have a secure password
- Set your profile settings to 'private'
- Only visit appropriate websites
- Only communicate with people you know in real life
- Think before you post images or information
- Check your device settings
- Use a virus-protection program
- Use the **Cybersafety HELP** button



Report any problems to a responsible adult.

Class discussion



Search for the video

[Make cyberspace a better place - Katie - Cybersafety](https://www.youtube.com/watch?v=H0Qg1_-Xmr8)

https://www.youtube.com/watch?v=H0Qg1_-Xmr8

Watch the video and answer the questions:

- What did Katie do wrong?
- What did Melanie do wrong?
- What did Katie do to report the situation?
- What strategies did the girls use to deal with the situation?
- What did the girls learn from the situation?

Cybersecurity challenge

Test your knowledge and understanding of cybersecurity

- Search for the website *Budd:e*
<https://budd-e.cybersmart.gov.au/primary/main.php>
- Click on the 'New' button to create a profile with username and password
- Participate in the cybersecurity challenges



References

- ACMA (2015). #GameOn. Kids. Cybersmart website. Australian Communications and Media Authority (ACMA). Commonwealth of Australia. <http://www.cybersmart.gov.au/kids/Watch%20Videos/at-school.aspx>
- Australian Bankers Association Inc (2009). Protect your kids online. Fact Sheet. <http://www.afp.gov.au/~media/afp/pdf/p/protect-your-kids-online.ashx>
- Boystown (2014). Staying safe online. KidsHelpLine. <http://www.kidshelp.com.au/kids/information/hot-topics/staying-safe-online.php>
- Commonwealth of Australia (2015). Your Identity. StaySmartOnline website. Department of Communications. http://www.staysmartonline.gov.au/your_identity
- Childnet International (2009). What are digital footprints? Digital footprints. <http://www.kidsmart.org.uk/digitalfootprints/>
- Morris, K (2013). Teaching children about digital footprints. Primary Tech. <http://primarytech.global2.vic.edu.au/2013/02/22/teaching-children-about-digital-footprints/>
- Raising Children Network (2014). Internet safety. School age children. http://raisingchildren.net.au/articles/internet_safety.html/context/586
- State government Victoria (2013). Step by step guide: Removing inappropriate content from websites or social media sites. Education Victoria. <http://www.education.vic.gov.au/Documents/about/programs/bullystoppers/stepbystepincontent.pdf>

Attributions

- Slide 1 <http://www.clker.com/clipart-foot-prints.html>
- Slide 3 <http://www.clker.com/clipart-id-card.html>
- Slide 4 <http://www.clker.com/clipart-253829.html>
- Slide 5 <http://www.clker.com/clipart-28744.html>
- Slide 10 <http://www.clker.com/clipart-secure-monitor3.html>
- Slide 11 <http://www.clker.com/clipart-locks.html>
- Slide 12 <http://www.clker.com/clipart-question-mark-10.html>
- Slide 13 <http://www.clker.com/clipart-input-mouse.html>
- Slide 14 <http://www.clker.com/clipart-355657.html>
- Slide 15 <http://www.clker.com/clipart-programmer-2.html>

Slides 2, 5, 6 - © DETE