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 1–2

Privacy and security

Image source: Pixabay

Classifying data as personal or public

Understanding and applying privacy and security practices is an important skill in the Australian Curriculum: Digital Technologies. In Years 1 and 2 students learn:

- to identify examples of personal data that may be stored and transmitted as they interact online for learning and communicating
- the importance of controlling their personal data
- how to protect their data and digital tools by setting passwords they can use independently.

Years 1 and 2 students could:

- list examples of different types of data that might be collected in a typical day such as name on lunch order (text), teacher taking roll (text), logging onto school computer, using bus pass (image), paying for groceries at the shop using a debit card (number). In each scenario, students identify the type of data collected; for example, name, password, travel details, bank account details.
- discuss data scenario cards (see Figure 1) and classify on a T-chart whether data is personal or public. Students should understand that personal data is something that they should keep to themselves (full name, address, school information). Personal data is connected to and can identify a specific person; for example, no-one has the same mobile phone number. Public data could include things such as favourite movie or colour or if they are left- or right-handed.
- play a game of Thumbs Up, Thumbs Down indicating if scenarios include personal or public data
- participate in a sorting relay classifying data into personal or public hula hoops

Figure 1: An example of a sorting activity for deciding whether data in each scenario is personal (owned by students) or not personal (owned by someone else or everyone)

- complete an ‘all about me’ activity, excluding names – students swap activity sheets and see if individual students could be identified just by the data on the sheet
- discuss whether an example of the same data could be classified as personal or public depending on the scenario, e.g. compare a photo of a student in their school uniform with a photo of the same student playing at a park (see Figure 2). Optional: Complete this activity digitally on an online collaboration tool such as Google Jamboard (see Figure 3)
- list data that is okay to share, could be shared with caution, and should not be shared. Students could answer questions such as:
  - What kind of things would you not tell a stranger?
  - What might we learn about a person from the personal information they share?
  - Can we guess more information from their photos?
- list data into the following categories: shared with everyone, shared with friends, shared with no-one based on shared (or provided) criteria
- role-play various scenarios demonstrating an understanding of when it is okay to share data, when permission is needed before sharing data, and what data should not be shared
- sort data images into columns (see Figure 4) deciding whether data is personal or private (owned by them), personal or private (owned by someone else) or public (owned by everyone). Optional: Complete this activity digitally on an online collaboration tool such as Google Jamboard (see Figure 3)
- play a turn up, turn down card game by reading cards and justifying if the data in a particular scenario is classified as personal or public (see Figures 5 and 6)

Figure 2: An example of a sorting activity for deciding whether an example of the same data, e.g. photos, could be classified as personal or public depending on the

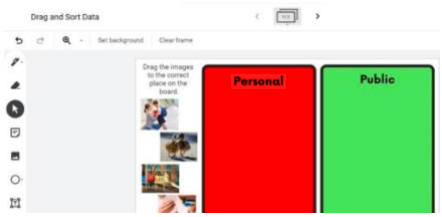

Figure 3: An example of a digital sorting drag-and-drop activity on an online collaboration tool

Figure 4: An example of sorting activity for deciding whether data is personal (owned by students), personal (owned by someone else) or public (owned by everyone)

Figures 5 and 6: An example of a turn up, turn down card game where students decide in each photo scenario if the data is personal or public

- list websites or apps that store their personal data
- rewrite and perform a common fairytale or fable including a modern data scenario; for example, the Big Bad Wolf trying to get the Three Little Pigs' addresses. Optional: Publish the completed story on a digital publishing tool such as Book Creator and illustrate using an online drawing tool such as Microsoft Paint, Paint 3D or Tayasui Sketches School. Create their scenario on a digital cartoon application such as Toontastic 3D (shopping, app signup, password)
- discuss places people use passwords, for example, phone passcode, bank PIN, online games
- discuss why it is important to keep our passwords safe
- discuss what could happen if passwords were shared with the wrong people
- identify commonly used passwords such as 'password' or '12345' (see Resources) and brainstorm other weak combinations. Students could answer questions such as:
  - What do we notice about these passwords?
  - Are some passwords better than others?
- try an online password generator (see Resources)
- discuss the importance of asking permission, before entering data online identifying who we need to ask permission from, and for what
- understand that a password is a secret string of characters (mix of letters, numbers and symbols) which allows them to access their device and data
- practise typing their password into a keyboard (see Figure 7)

Figure 7: An example of a laminated keyboard that encourages students to practise typing (and remembering) their passwords

- change their school account to use their chosen password (if permitted by school IT policy)
- discuss the difference between a username and a password
- practise accessing their own information using their username and password
- use a personal prompt card to type their login details and password into a digital device
- create a list of do's and don'ts for passwords; for example, do not use the same password for multiple sites, do create variations of the same password
- discuss if passwords need to be changed; students could decide whether people should use the same password on multiple sites.

Links to the Australian Curriculum v9.0

Table 1: Aspects of the Australian Curriculum: Digital Technologies Years 1 and 2 which may be addressed depending on the task

<table>
<tr><td>Digital Technologies Achievement standard</td><td colspan="3">By the end of Year 2 students show how simple digital solutions meet a need for known users. Students represent and process data in different ways. They follow and describe basic algorithms involving a sequence of steps and branching. With assistance, students access and use digital systems for a purpose. They use the basic features of common digital tools to create, locate and share content, and to collaborate, following agreed behaviours. Students recognise that digital tools may store their personal data online.</td></tr>
<tr><td>Strand
Sub-strand</td><td colspan="3">Knowledge and understanding
• Data representation
Processes and production skills
• Privacy and security</td></tr>
<tr><td>Content descriptions</td><td colspan="3">• represent data as pictures, symbols, numbers and words AC9TDI2K02
• use the basic features of common digital tools to create, locate and communicate content AC9TDI2P04
• access their school account with a recorded username and password AC9TDI2P06
• discuss that some websites and apps store their personal data online AC9TDI2P07</td></tr>
<tr><td rowspan="2">Technologies Core concepts</td><td rowspan="2">• Data
• Interactions and impact</td><td>Digital Technologies Core concepts</td><td>• data acquisition
• data interpretation
• privacy and security</td></tr>
<tr><td>General capabilities</td><td>• Digital Literacy
  • Practising digital safety and wellbeing
  – Manage online safety
  – Manage digital privacy and identity
  • Managing and operating
  – Protect content
• Literacy
• Critical and Creative Thinking
• Personal and Social capability
• Numeracy
• Ethical Understanding</td></tr>
<tr><td>Cross-curriculum priorities</td><td>• Sustainability</td><td>Learning area or subject connections</td><td>• English
• Mathematics
• Health and Physical Education
• The Arts</td></tr>
</table>

Learning area or subject connections

English

Learning in Technologies places a high priority on accurate and clear communication. The Australian Curriculum: Technologies is supported by and in turn reinforces the learning of literacy skills. Students need to describe objects and events; interpret descriptions; and participate in group discussions.

Mathematics

The Australian Curriculum: Technologies provides contexts within which Mathematics understanding and problem-solving skills can be applied and developed. 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*.

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 giving or denying consent as they expand their communication and collaboration experience into online and networked environments.

The Arts – Drama

The Australian Curriculum: Technologies complements The Arts curriculum, particularly in the application of the elements and principles of art/design, and aspects of aesthetics and user experiences which are incorporated into the design processes in Technologies content.

The Digital Technologies curriculum focuses on using digital systems (hardware and software) to create solutions. In each of The Arts subjects students can use digital systems to create works in traditional and emerging forms. In The Arts, students may use skills and knowledge learnt through Digital Technologies to develop their arts practice; for example, Drama may be a useful tool for students to role-play scenarios relating to privacy and security.

Resources

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

Useful links

- Wikipedia: Lists of most common passwords
  en.wikipedia.org/wiki/List_of_the_most_common_passwords
- Security.org Password Strength Checker
  www.security.org/how-secure-is-my-password/
- Codemoji Online Password Generator
  www.dinopass.com/

- eSafety education – classroom resources
  www.esafety.gov.au/educators
- eSafety kids
  www.esafety.gov.au/kids
- Google Be Internet Awesome resources
  beinternetawesome.withgoogle.com/en_us/
- Kids Helpline Online Safety Session booking
  kidshelpline.com.au/schools/sessions/online-safety
- Common Sense Password Protect Game
  www.digitalpassport.org/password-protect.html
- Playing IT Safe – Share that Photo
  games.playingitsafe.org.au/
- Australian Federal Police Think U Know (teacher/parent resources)
  www.thinkuknow.org.au/
- Life Education teacher resources (Required registration)
  www.lifeeducation.org.au/teacher-resources/bcyberwise/
- ACA cyber-sharing cards (PDF download)
  aca.edu.au/resources/cyber-sharing-cards/cyber-sharing-cards.pdf
- NetSmartzKids: Sharing is Caring activity
  www.netsmartzkids.org/activities/
- Hello Ruby: Data Selfie
  www.helloruby.com/play/27

All images in this resource are used with permission.