



## CLASSROOM IDEAS: Years 5–6

### Privacy and security



Image source:  
[unsplash.com/@johnschno](https://unsplash.com/@johnschno)

Students should explore the automated and non-automated processes through which data is protected, collected, generated and stored in the creation of an individual's digital footprint. As an increasingly important aspect of digital technology use in today's society, students must consider how their behaviour online can provide access to their personal data, breach social and ethical protocols, and jeopardise their safety.

As students engage in social media and online gaming, they should also develop an awareness of the impact publicly displayed data can have on their current and future lives, including social relationships and professional opportunities. By exploring this, students are practising digital safety and wellbeing as they learn to effectively manage their privacy and security in a variety of scenarios.

Key inquiry questions to initiate student discussion include:

- How can we ensure our passwords are secure?
- What are the possible repercussions of a password or security breach?
- How do we show respect for other people's data when engaging online?
- How do online applications and websites store our data?
- How can the privacy of our online behaviours impact on our future?

Years 5 and 6 students should learn how to:

- develop unique passphrases to create secure passwords
- analyse the repercussions of password sharing, breaches and compromised data
- consider their digital footprint and its longevity when contributing to an online presence
- interact ethically and respectfully when engaging with others and content online
- explain the potential consequences of their digital footprint from a young age.



Image source: Pixabay

Image source: Pixabay



Figure 1: Social media definitions.  
See Appendix 1 for details.  
Image source: Canva

## Teaching and learning activities

Years 5–6 students could participate in a social media simulation, allowing them to engage in the process of creating an online presence safely and analytically, while applying security measures to protect their privacy.

Alternatively, the same activities could be done through the analysis of an existing social media profile of interest to students; for example, a celebrity, politician, sports personality, media personality, influencer. This has the potential to integrate with learning in other learning areas such as English.

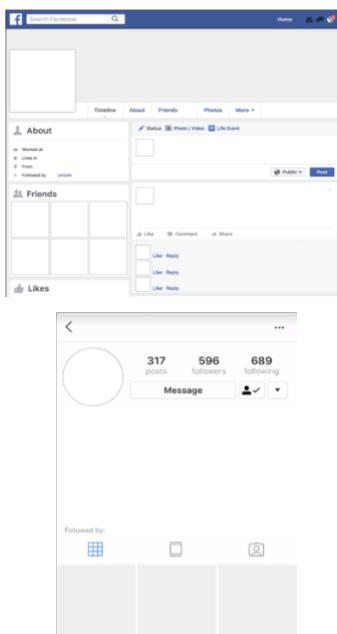
The following activities could be used in isolation (using a provided social media profile) or as a cumulative unit. While students in these years should not be using social media, it has, unfortunately, become common practice. It is important to remind students that the use of social media platforms is not recommended for students under 13 years of age and is illegal for some sites.

Note: Teachers should refer to their state or territory guidelines before undertaking the following tasks.

## Social media savvy

Students will create a mock social media profile of a character from a literary text, or a notable person being studied in another learning area.

- Use popular or known social media platforms as a template or basis (Figures 2 and 3 and Resources). Some templates are digital while others are printable to cater for a range of classroom scenarios. Alternatively, students can use Microsoft Office, Google Suite, Apple applications or web-based programs, such as Canva, to create their template by using their digital literacy skills.
- Explicitly teach the elements of a social media post (Figures 1–3 and Appendix 1 and 2) and associated jargon and how these features allow people to find online content and enhance the collection of data.



Figures 2 and 3: Social media templates that can be provided to students or displayed for digital creation by students (see Resources)



Image source: Canva

Figures 4 and 5: Social media profile identifying features posters (see Appendix 2)



*Figure 6: Sample scavenger hunt  
(see Appendix 3)*  
Image source: Canva

## Social scavenger hunt

Students will swap their mock social media profiles from the previous activity and complete a scavenger hunt (Figure 6 and Appendix 3), locating personal details provided unwittingly on the created profile.

Identify personal data of their character or notable person such as name, age, birthdate, pets, pets' names, location, postcode, street name, school, sports, friends, family and siblings (active data). This data can be tracked on a spreadsheet, word processing table, checklist or a collaborative digital whiteboard.

Tick all the categories of data you were able to identify:

First Name

Surname

Age

Pets

Location

Street Name

School

Sports

Friends

Family

Siblings

Hobbies

*Figure 7: Sample Google Form*

- Students can input the data they have uncovered in a Google or Microsoft Form (Figure 7).
- Analyse this data to initiate a discussion around the common categories of data we make public and the privacy settings available that minimise their exposure for our security.
- Discuss how tags, locations, hashtags and handles (passive data) can inadvertently provide and store personal data.

## Helpful hacker



Image source: Pixabay

Model common passwords or passphrases such as dog's name + birth date or surname + postcode.

To help students ensure their passwords for their mock accounts cannot easily be hacked, students use the personal data gathered through the scavenger hunt, to 'hack' each other's mock accounts by compiling possible password combinations from the data gathered.

Students will:

- use the data gathered to create a list of potential passwords that could be used to breach security, simply by analysing a social media page
- consider the amount of personal data that can be inadvertently publicly shared by people when posting online or playing online games, and identify which information in their mock social media profile should be private and which should be public.

Provide opportunities for students to personally, and privately, reflect on what the 'hackers' identified as potential passwords and reinforce how they should:

- identify ways privacy is exposed on these platforms (hashtags, handles, locations, tagging)
- select and moderate the personal data they personally share on websites including game sites
- create secure passwords that do not include identifying features
- secure their online accounts to ensure their data is kept private.

### Extension

To extend learning, students can employ algorithmic thinking to come up with a method to identify possible password or passphrase combinations from the data collected. Draw parallels to real-world instances where codes are run to determine passwords. The following table gives an example.

	First name	Last name	Age	Pet	Pet name
First name	johnjohn	johnsmith	john12	johncat	johndaisy
Last name	smithjohn	smithsmith	smith12	smithcat	smithdaisy
Age	12john	12smith	1212	12cat	12daisy
Pet	catjohn	catsmith	cat12	catcat	catdaisy
Pet name	daisyjohn	daisysmith	daisy12	daisycat	daisydaisy

## Seeking permission



Image source: Pixabay

Students will recognise which images included in the mock social media profile would need consent to protect the privacy of others, and how they would gain permission; for example, if a student wanted to create a blog post about their sports team which included photos from sporting matches and team events. Have students consider how they could ethically obtain these photos and gain permission for their use.

- Explore ethical behaviours (consent, age, content), including legal guidelines, around the age of use for social media and gaming platforms.
- Discuss the impact the decision of posting without someone's permission could have on that person.

## Being the boss

Analyse another student's mock social media profile from the perspective of the character running for a school leadership position or notable person applying for a future job. Students could:

- compile a list of traits the school principal or prospective employers would or would not be looking for in school leader or an employee
- compose persuasive leadership or job applications highlighting their character's or notable person's strengths
- create a pros and cons list against these criteria based on the mock social media profile
- annotate the mock social media page to highlight the data and decide if they would elect or hire this person based on their visible digital footprint (see Figure 8).



Image source: Pixabay

Messy workspace – organisation issues?

Oversharing – confidentiality concern?

Spelling mistake – poor attention to detail?

Leaves things to the last minute – poor work ethic?

grace\_2010 Nothing like leaving an assinment to the last minute ⏳ #itwillberight #deadline #lastminute

23 April

Instagram @grace\_2010 Orange, NSW

Image source: Canva

Figure 8: Annotations on mock social media profile

- explain how the character or notable person should alter data and privacy settings on the mock social media profiles to reflect a positive digital footprint
- explore data storage by websites and applications and how data can be retrieved or manipulated by other users, impacting leadership or career prospects
- discuss the longevity of what is posted online, where it is stored and how it can be retrieved. Particularly, how people screenshot content so when it is deleted by the user, it is already too late.

### **Footprint for the future**

Students will create a representation of their literal digital footprint.

Students could:

- identify what they want their online presence and data to say about them
- recognise methods they can use to display quality privacy and security practices to protect their digital footprint and people's perceptions of them.

This final, cumulative task could be completed in a number of ways:

- screen recording of a 'tour' of their now secure and private mock social media page
- digital poster annotation of privacy and security features of their replica social media page
- digital presentation of a replica social media profile
- video of a principal or an employer reviewing an applicant's social media page or a leadership or job interview situation where the principal or employer references a social media page
- Walk a Mile in My Digital Shoes presentation
- instructional video highlighting how to enhance security and privacy on a social media profile.



*Image source: Pixabay*

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

Table 1: Aspects of the Australian Curriculum: Digital Technologies – Years 5–6 (v8.4) which may be addressed depending on the task

<b>Digital Technologies Achievement standard</b>	<p>By the end of Year 6, students explain the fundamentals of digital system components (hardware, software and networks) and how digital systems are connected to form networks. They explain how digital systems use whole numbers as a basis for representing a variety of data types.</p> <p>Students define problems in terms of data and functional requirements and design solutions by developing algorithms to address the problems. They incorporate decision-making, repetition and user interface design into their designs and implement their digital solutions, including a visual program. They explain how information systems and their solutions meet needs and consider sustainability. Students manage the creation and communication of ideas and information in collaborative digital projects using validated data and agreed protocols.</p>		
<b>Strand</b>	<p><b>Knowledge and understanding</b></p> <ul style="list-style-type: none"> <li>• Digital systems</li> </ul> <p><b>Processes and production skills</b></p> <ul style="list-style-type: none"> <li>• Collecting, managing and analysing data</li> <li>• Evaluating</li> <li>• Collaborating and managing</li> </ul>		
<b>Content descriptions</b>	<ul style="list-style-type: none"> <li>• Examine the main components of common digital systems and how they may connect together to form networks to transmit data (<a href="#">ACTDIK014</a>)</li> <li>• Acquire, store and validate different types of data, and use a range of software to interpret and visualise data to create information (<a href="#">ACTDIP016</a>)</li> <li>• Explain how student solutions and existing information systems are sustainable and meet current and future local community needs (<a href="#">ACTDIP021</a>)</li> <li>• Plan, create and communicate ideas and information, including collaboratively online, applying agreed ethical, social and technical protocols (<a href="#">ACTDIP022</a>)</li> </ul>		
<b>Key concepts</b>	<ul style="list-style-type: none"> <li>• digital systems</li> <li>• data collection</li> <li>• data interpretation</li> <li>• interactions</li> <li>• impact</li> </ul>	<b>Key ideas</b>	Thinking in Technologies <ul style="list-style-type: none"> <li>• Systems thinking</li> </ul>
<b>Cross-curriculum priorities</b>	<ul style="list-style-type: none"> <li>• Sustainability</li> </ul>	<b>General capabilities</b>	<ul style="list-style-type: none"> <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>
<b>Learning area or subject connections</b>	<ul style="list-style-type: none"> <li>• English</li> <li>• Mathematics</li> <li>• Health and Physical Education</li> </ul>		

## 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.

The entire social media simulation can be undertaken by creating a social media profile for a fictional character, person of interest or personality from shared or independent texts being studied during English lessons. These mock social media profiles could form integrated *Literature* and *Literacy* tasks as students take part in *Examining literature* and examining *Texts in context* through the curation of a social media profile outlining characteristics, events and plot points, relationships and inferences.

There is also the potential to explore *Creating texts* through the construction of persuasive texts for mock job applications that address specific criteria. Students can also write extended responses where they identify evidence online, explain the impact of this and link it back to the overarching notion of privacy and security.

Throughout the unit, students will be exposed to vocabulary and examples of media that can be analysed for reliability or for features of specific text types, particularly informative (news articles, social media posts) and persuasive (fake news, phishing, advertisements, job applications) texts.

### 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 in 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.

Students can explore the notion of encryption and deciphering text through the lens of *Patterns and algebra*. Letters or words of a password can be referred to as terms of a pattern while students explore known and unknown codes to determine the rule and apply it in a way that allows them to decrypt ciphertext. Giving students the opportunity to work backwards in this way, through a logical, mathematical lens, will allow them to develop a deeper understanding of the ease with which privacy can be breached to ensure they employ rigorous security measures when protecting their data. This can also enhance their algorithmic thinking to solve these problems.

### 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 using 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/](http://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/](http://www.australiancurriculum.edu.au/resources/curriculum-connections/portfolios/respect-matters/)

### Social media savvy

- FakeBook Online Profile  
[www.classtools.net/FB/home-page](http://www.classtools.net/FB/home-page)
- Google Slides Fake Facebook Template  
[bit.ly/fakefacebooktemplate](http://bit.ly/fakefacebooktemplate)
- Fake Instagram Template  
[docs.google.com/presentation/d/17twGuRhwKTQnHxaoJirisYYes1UAB6F9wDtYeEkTPS0/template/preview](http://docs.google.com/presentation/d/17twGuRhwKTQnHxaoJirisYYes1UAB6F9wDtYeEkTPS0/template/preview)
- Google Slides Instagram Template  
[docs.google.com/presentation/d/1ogN1Pdu7HcpAm-0qFo9BNKjsaL3pd90ZppbA6-12p5U/template/preview](http://docs.google.com/presentation/d/1ogN1Pdu7HcpAm-0qFo9BNKjsaL3pd90ZppbA6-12p5U/template/preview)

### Being the boss

- The WIRED Guide to Your Personal Data  
[www.wired.com/story/wired-guide-personal-data-collection/](http://www.wired.com/story/wired-guide-personal-data-collection/)
- Innes S (2019) *The Internet is Like a Puddle* (Agócs illus) [picture book], Hardie Grant Children's Publishing.

### Footprint for the future

- Canva  
[www.canva.com/en\\_gb/](http://www.canva.com/en_gb/)
- Prezi  
[prezi.com/](http://prezi.com/)
- Biteable  
[biteable.com/](http://biteable.com/)

### Useful links

- Digital Technologies Hub – Cybersafety  
[www.digitaltechnologieshub.edu.au/families/cybersafety](http://www.digitaltechnologieshub.edu.au/families/cybersafety)
- Attacker vs Hackers – Two \*Very\* Different Animals  
[www.tripwire.com/state-of-security/vulnerability-management/hackers-vs-attackers-different-animals](http://www.tripwire.com/state-of-security/vulnerability-management/hackers-vs-attackers-different-animals)
- Be Internet Awesome – Interland  
[beinternetawesome.withgoogle.com/en\\_us/interland](http://beinternetawesome.withgoogle.com/en_us/interland)
- Learning for Justice - Privacy and Security Online  
[www.learningforjustice.org/classroom-resources/lessons/privacy-and-security-online](http://www.learningforjustice.org/classroom-resources/lessons/privacy-and-security-online)
- Common Sense Education – 23 Great Lesson Plans for Internet Safety  
[www.commonsense.org/education/articles/23-great-lesson-plans-for-internet-safety](http://www.commonsense.org/education/articles/23-great-lesson-plans-for-internet-safety)

- eSafety education  
[www.esafety.gov.au/educators](http://www.esafety.gov.au/educators)
- eSafety education – Classroom resources – Be secure  
[www.esafety.gov.au/educators/classroom-resources/be-secure](http://www.esafety.gov.au/educators/classroom-resources/be-secure)
- eSafety kids – Being safe online  
[www.esafety.gov.au/kids/be-an-esafe-kid/being-safe-online](http://www.esafety.gov.au/kids/be-an-esafe-kid/being-safe-online)
- eSafety kids – Sharing photos and my personal information online  
[www.esafety.gov.au/kids/be-an-esafe-kid/sharing-my-personal-information-online](http://www.esafety.gov.au/kids/be-an-esafe-kid/sharing-my-personal-information-online)
- eSafety kids – Security and privacy for my device  
[www.esafety.gov.au/kids/be-an-esafe-kid/security-and-privacy-for-my-device](http://www.esafety.gov.au/kids/be-an-esafe-kid/security-and-privacy-for-my-device)

*All images in this resource are used with permission.*

## **Appendix 1**

### **Social media definitions**

# SOCIAL MEDIA DEFINITIONS



Bio: Short for biography, a way to tell your followers who you are.

Handle: A username on social media, usually follows the @ symbol.

@ACARAeduau

Captions: A description that is posted with a photo/video.

Hashtag: The character # followed by letters or numbers. It is clickable and organises similar posts to be found more easily.

#

Emoji: A digital image that shows emotion or represents people, places or things.



Tag: Links someone's profile to a post which can be clicked on by followers. Also called a mention.



Location: Adding geographical data about the whereabouts of a post.



Filter: A method of editing photos and videos to enhance them or make them appear differently.

Image source: Canva

## **Appendix 2**

### **Social Media Profile Identifying Features Posters**

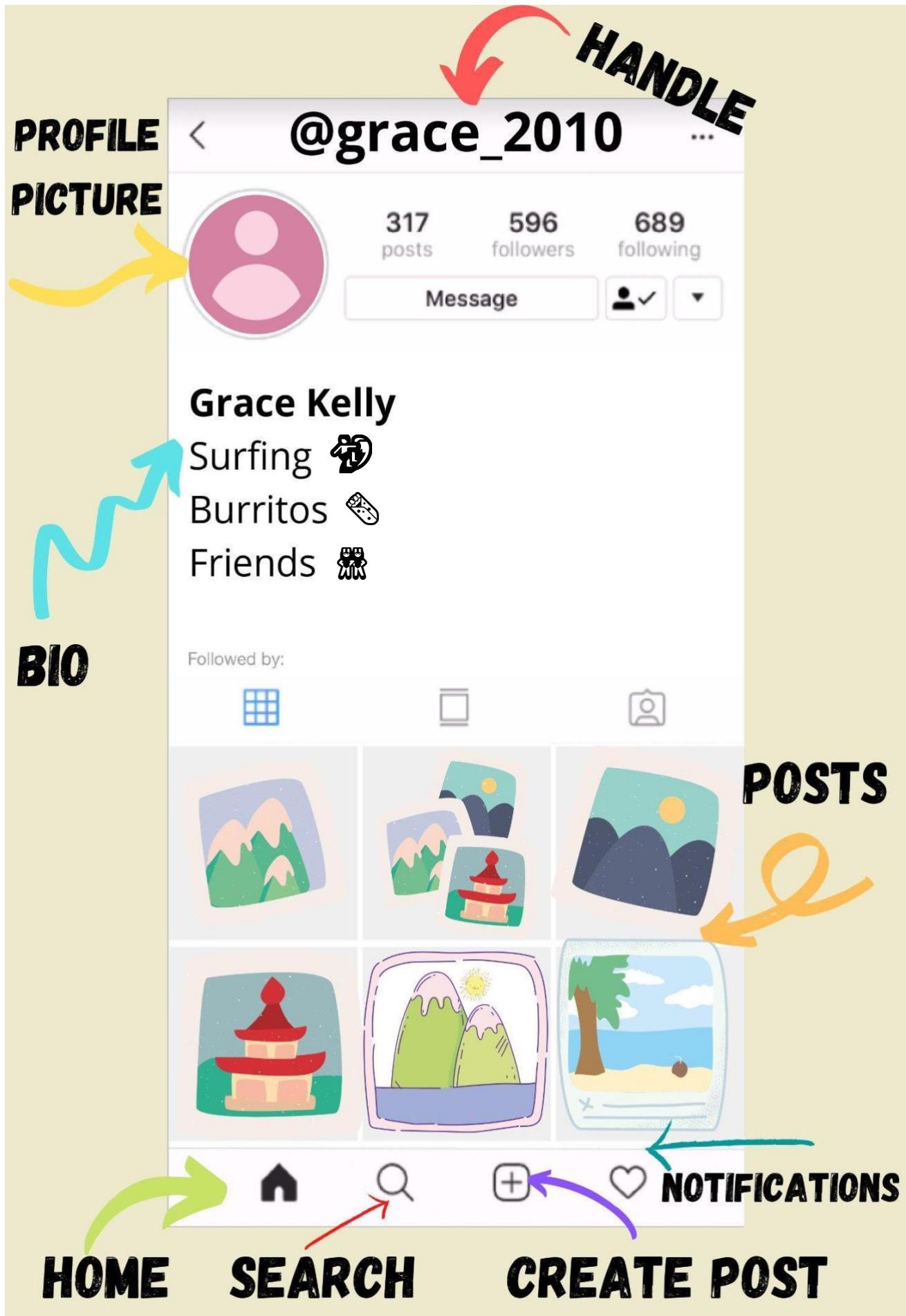


Image source: Canva



Image source: Canva

# SOCIAL SCAVENGER HUNT

name

postcode

friends

street  
name

birthdate

family

Fill the outline with  
as many personal  
details as you can  
find using someone's  
social media page.

siblings

pets

school

location

sports

age

Image source: Canva

# SOCIAL SCAVENGER HUNT

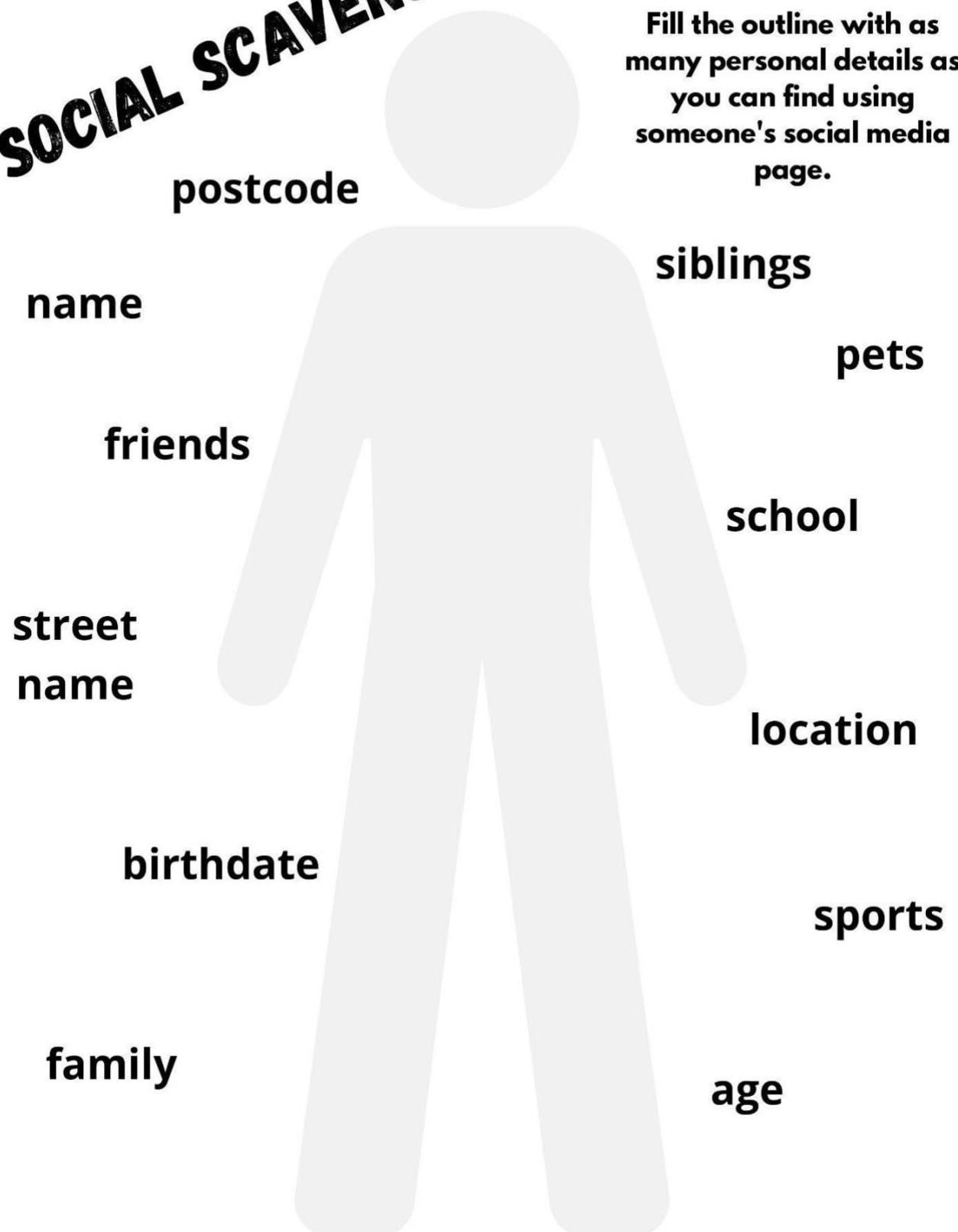


Image source: Canva