



Digital Insight Digital Resource Pack

Introduction

This document contains the teacher resources, top tips and take home sheet that support the Digital Insight workshop, which is part of the **Optus Digital Thumbprint** program.

The two lesson plans are to be used by teachers in providing students with an interesting and engaging lesson around digital security and privacy. Each section of the lesson plan contains: the overall aim of the section, an approximate timing for the section, the interaction between teachers and students, as well as a description of the material and suggestions of how it should be delivered for maximum impact.

Lesson Plans:

These lesson plans are organised by section, interaction type, and description. The section contains important information about the purpose of each phase as well as an estimated time allocation. The interaction describes the ideal flow of information between teachers (T) and students (S). For example, interactions that flow T-S-S are about teachers giving instructions, or guidance followed by two lots of student communication with teachers. Interactions with only 'S' in them are student-led parts of the session. And the description explains the actions and questions or concepts that are communicated throughout the lesson. Teachers will use this information as a 'run sheet' for the session to ensure it runs smoothly.

Student Top Tips:

The top tips include some of the most important points students will have learnt in the Digital Insight workshop, the lessons they have had with their teachers and the topics they may have talked about with their parents. These tips will help students to ensure their information is kept safe and help them to become better digital citizens.



Parent Take Home:



The take home sheet is a resource for parents that allows them to have a structured conversation with their children about difficult topics. Parents are provided with example sentences and answers which can help them navigate a conversation about digital security and privacy with their child.

Digital Insight Lesson Plan 1

Section	Interaction	Description
Intro Lead-in to set the context 🕒 3 min	T-S-S	Start the class by asking the following two questions, trying to get as much information and interaction from the students as possible: <ol style="list-style-type: none">What information do you need to start a Facebook account?*[Name, mobile number or email, date of birth, captcha code, password]What things do you post online?*[Pictures of your yourself? Of your friends? Memes? Comments? Videos? Plans for the weekend? etc] * As these questions are for setting the context, teachers are not required to record the students' answers. They are used for leading in to the understanding activities, engaging the students and increasing lesson interactivity.
Controlled understanding activity 1 To give students understanding of the consequences of their actions 🕒 15 min	S-S	Give the following background information to the students: "Sophia is a new kid in the class. You want to make her feel welcome. To do this, you thought it would be a good idea to find out a bit about her." Put the students into three groups. Each group receives a profile handout about Sophia (these can be found in the handout section of this booklet). Group 1. Profile 1 (Facebook), Group 2. Profile 2 (Twitter), Group 3. Profile 3 (Instagram).

Digital Insight Lesson Plan 2

Section	Interaction	Description
Intro Lead-in to set the context  5 min	T-S	<p>Start the class by asking the following two questions, trying to get as much information and interaction from the students as possible:</p> <ol style="list-style-type: none"> 1. "Have you ever had a bad experience online?"* or 2. "Has someone you know had a negative experience online?"* [Yes/No, what was the experience?] <p>* As these questions are for setting the context, teachers are not required to record the students' answers. They are used for leading in to the understanding activities, engaging the students and increasing lesson interactivity</p>
Self-efficacy To allow students to identify what steps they can personally take to become a better digital citizen  10 min	S-S-T	<p>Give the students the following background information: "As you log into your social media account, you notice that there are some comments and messages that you don't remember making. You think someone might have gained access to your page".</p> <p>Put the students into pairs.</p> <p>In pairs, students discuss the kinds of personal information that someone might be able to get hold of from their social media accounts - both with and without having your password. (Their name, their best friend's name, where they work, what job they do, where they live, their email address, their date of birth, their mobile number, where they're going to be on the weekend, which school they go to etc.).</p> <p>In pairs, students discuss what personal information about you someone might be able to get hold of from their friends' social media account. (Places they go together, activities they do together, hobbies, interests, mutual friends' names, pictures etc.).</p> <p>Ask the students: "How can you keep your accounts secure?"</p> <p>Students should provide different measures of being safe online. These points can be extended by asking for personal stories that the students have about each point. The following questions can be used by teachers who are having difficulty eliciting the information from the students:</p> <ol style="list-style-type: none"> 1. Who uses a password manager? Why might using a password manager be better than using the same password for every site? 2. Has anyone changed their default settings for who can see their posts? Why did you change the settings? How did you change them? Was it easy? 3. Has anyone been contacted by a stranger on the internet before? What did they want? 4. Which anti-virus program do you use on your computer and why? 5. Do all of your devices have a password set up on them? Is it the same password or different? 6. What services do you use that show other people your location?

Section	Interaction	Description
Self-efficacy To allow students to identify what steps they can personally take to become a better digital citizen  10 min	S-S S-S	<p>Put students in to four groups. Each group is allocated one of the following topics:</p> <ol style="list-style-type: none"> Hacking Data theft Cyber stalking Identity theft <p>In their groups, students should discuss what the punishment should be for their allocated cyber-crime and say why they think it's a fair punishment. Have students list what proof would be needed to convict a person of these cyber-crimes. [Students can give punishments as fines or jail time or any other punishment they see fit. The actual answer is not as important as getting students to think about the fact that these are actually serious crimes and are punishable by law].</p> <p>In their groups, students are also asked to come up with one scenario where someone they know has committed one of these offenses. [E.g. "My friend Sandra likes Johnny and looked him up on Facebook and other forms of social media. This could be considered a form of cyber stalking". "My friend copied the class birthday list from the teacher's computer without asking, this is data theft"]. The purpose of this is to inform the students that these behaviours, although seemingly harmless, can have serious ramifications.</p> <p>If time permits:</p> <p>Highlight the relevant laws around cyber-crime at https://www.cdpp.gov.au/crimes-we-prosecute/cybercrime</p> <p>Give students guidance on where to report cyber-related incidents at: https://www.acorn.gov.au https://www.scamwatch.gov.au</p> <p>Optional: For homework, have students research the actual punishments for cyber-crimes and discuss the conviction/charges for one hacker of their choosing. Students should discuss the results of their research in the next class.</p>
Conclusion Ensures students have understood the knowledge given and are prepared to become a digital citizen.  5 min	T-S-T	<p>Give students a quick, verbal true-false test about security and privacy.</p> <ul style="list-style-type: none"> You should use a different password for each account and use 2FA or other non-password methods of security where possible (two factor authentication). [True] You should make your details public. [False] You should be wary of people you don't know that try to contact you. [True] You should use an anti-virus program. [True] You should setup a separate password for your computer and phone and tablet if you have them. [True] You should post information that people could use to identify you or to find out your location. [False] You should make sure that a site's link that you click on is the correct address. [True] <p>Ask students to declare what is the next step students will take to become safer online, so that students have a plan to change their behaviour and are committed to improving their online safety.</p>

Handouts

Profile 1. (Facebook)

facebook

Wall


Photos

Flair

Boxes

Sophia Archer

Logout



Sophia Archer is feeling exhausted!

Wall

Info

Photos

Boxes

View photos of Sophia (5)

Send Sophia a message

Poke message

Information

Networks:
Hollyhands.
Birthday:
May 16, 2000
Hometown:
Sydney, Australia

Basic Information

Sex:
Female
Birthday:
May 16, 2000
Hometown:
Sydney, Australia

Personal Information

Activities:
Basketball,
Interests:
Basketball, Summer in Denmark, coffee

Photos

2 Albums

The Family
Updated last Tuesday

Friends
Updated two months ago

Contact Information

Address:
100 Miller Road, North Sydney
Phone Number:
0419 111 222

Profile 2. (Twitter)

Home

Discover

Connect

Me

Search

Settings

Compose

Tweets

Following


Followers

Favorites

Lists

Tweet to Sophia Archer

@sparcs



Sophia Archer

@sparcs

Cats, coffee and class
Sydney, Australia


14,234 TWEETS

5,321 FOLLOWING

3,445,234 FOLLOWERS

FOLLOWING

Tweets




Sophia Archer

@sparcs

@EmilyAmazeB Emily is my BFF

View conversation

3m




Sopha Archer

@sparcs

Love my after school job! #hollyhandscape

Expand

2d




Pete Chambers

@PCman

Are you coming to #beachlife tonight for the party?

Retweeted by Sophia Archer

2d




Sophia Archer

@sparcs

Bellat #cats>dogs

View conversation

1w



Sophia Archer


@sparcs

@Shazler Love my new shoes #couchto5k

View conversation

1w

Who to follow · Refresh · View all




Queen Elizabeth I

@QueenLizOne

Followed by TheSheriff and others

Follow



James Burbage

@TheBurbs

Followed by Blackfriars and others

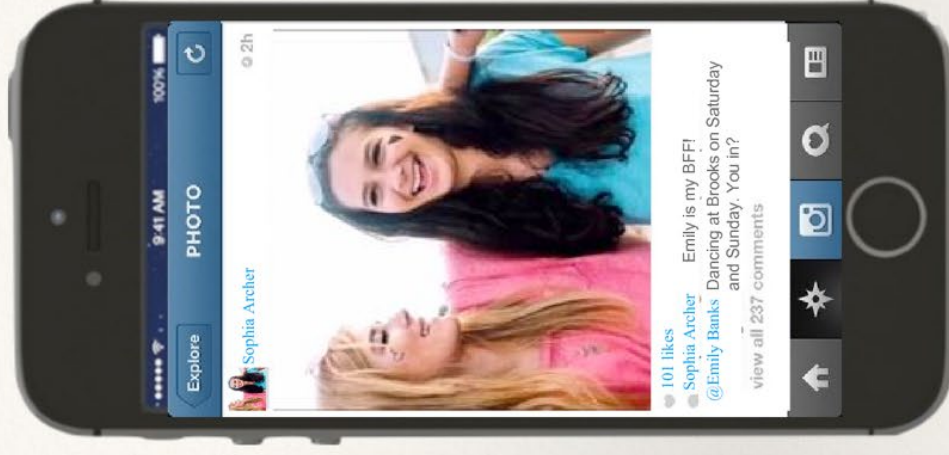
Follow

Browse categories · Find friends

Trends · Change

#theplague

Profile 3. (Instagram)



Digital Insight Student Top Tips

The following tips relate to the topic of being safe with your information online. They include some of the most important points you will have learnt in your Digital Insight workshop, the lessons you have had with your teachers and the topics you may have talked about with your parents. These top tips will help you to keep your information safe and to become a better digital citizen.

Choose strong passwords. ✓

- Use a memorable, but obscure passphrase for your password, i.e. "diversity labyrinth sighed soprano almost died."
- Remove any personal information from your password (i.e.: names, birthdays, etc.) that can be found out through social media or other means.
- Avoid popular culture phrases (i.e. music, movies, TV shows, etc.) as inspiration for your password.
- The website <https://howsecureismypassword.net> can give you a rough guide as to how strong your password is.

Make sure your account settings are set to private for information you don't want to share with others. ✓

- See <https://www.esafety.gov.au/esafety-information/games-apps-and-social-networking> for more information on how to do this for many popular sites and applications.

Make sure your phone is secure, i.e. activate PIN security, fingerprint passwords, etc. ✓

Use different passwords for different sites. ✓

- A good solution is a password manager, but they all have different benefits and risks.

Always be aware of your environment and be careful about the security of your phone and entering passwords where other people can see you. ✓

When posting, think about whether you would be comfortable if your parents or grandparents saw it. ✓

If you're uncertain about something you've received (a message, a photo, a friend request, etc.) ask a parent, teacher or friend for advice. ✓

Be careful of social media friend requests from people you don't know and always confirm it's really the person you think it is. ✓

Use 2FA (two factor authentication) wherever possible. 2FA can mean SMS messages to your phone, installing a special application or a fingerprint scan. ✓

Respect other people's right to digital privacy. ✓

If you need more help or information contact Kids Helpline on: 1800 55 1800 Or visit Kids Helpline at: <https://kidshelpline.com.au/> ✓

Don't tell anyone your passwords. ✓

Report cyberbullying at: ✓

<https://esafety.gov.au/complaints-and-reporting/cyberbullying-complaints/i-want-to-report-cyberbullying>

OPTUS PARTNERSHIPS





Digital Insight Parent Discussion Guide

This sheet is a resource that will help you to have a structured conversation with your children about difficult topics. It includes example sentences and answers which can help you navigate a conversation about digital security and privacy with your child. The following discussion points are important and often difficult topics to broach. Each discussion point below may be useful for your child and yourself in discussing cyber-security and an opportunity to do further online research together.



Write a list of the sites and apps you each use on a regular basis. If there are any sites you aren't familiar with, ask:

- "Who uses the app/site?" (E.g. Teenagers, business people, people of all different ages, etc.).
- "Why do they use the app/site?" (E.g. To connect with friends, to stay up-to-date, to plan events, etc.).
- "Where can they change the privacy settings on the app/site?" (E.g. How they can control who can see information about them on the app/site?).



Talk about what could happen if their accounts were compromised by asking the following questions:

- "What information might you lose if someone gained access to your account?" (E.g. Your photos, your messages, your videos, etc.).
- "What information on this site/app would you not want other people to know about?" (E.g. Your address, your phone number, your personal photos, etc.).
- What should you do so this doesn't happen again?



Always be aware of your environment and be careful about the security of your phone and entering passwords where other people can see you.




Be careful about posting the following on social media:


- Birth dates
- Addresses
- Information about your daily routine
- Holiday plans
- Where you go to school or work
- Photos of you or your family and friends





Discuss the importance of having a strong password:


- Use a combination of words that you can remember, but which aren't obvious. For example, the passphrase "diversity labyrinth sighed soprano almost died" is the same as a 46-character password (most websites only require 6 characters), but much easier to remember.
- Make sure your combination doesn't contain personal information (E.g. Names, birthdays, etc.) that can be found out through social media or other means.
- Avoid popular culture phrases (i.e. Music, movies, TV shows, etc.) as inspiration for your password.
- Get a rough idea of how strong your password is by visiting the website <https://howsecureismypassword.net/>


 Make sure your phone is secure (i.e. activate PIN security, fingerprint passwords, etc.).

 Discuss which sites/apps know your location and how do you make sure this information isn't shared with others.

 If your child ever sees or receives anything online that makes them uncomfortable, they should discuss it with you, friends or teachers. Alternatively, they can call the Kids Helpline at 1800 55 1800 or go to <https://www.yourtown.com.au/apps/webcounselling/live/chat/>

 If you are unsure about any of the information contained in this document or want to know more, check the resources section of the **Optus Digital Thumbprint** website: <http://www.digitalthumbprint.com.au/resources/>

 If you or your child wanted to report cyberbullying, you can go to <https://esafety.gov.au/complaints-and-reporting/cyberbullying-complaints/i-want-to-report-cyberbullying/>

 Make sure they have the strongest privacy settings on all social media sites so that only close friends can view their information, tag them in photos or share posts. The website <https://www.esafety.gov.au/esafety-information/games-apps-and-social-networking> has a guide to the security and privacy settings of many popular sites and applications.

 Be wary of giving information to people you don't know.

OPTUS PARTNERSHIPS

**Optus
Digital Thumbprint**



If you need more help or information contact Kids Helpline.

 **1800 55 1800**
 kidshelpline.com.au



Office of the
eSafety Commissioner

The Optus Digital Thumbprint program is certified by the Office of the eSafety Commissioner.

 esafety.gov.au



If you also have younger children, DQ World is designed for ages 8 - 12 and teaches 8 digital citizenship skills.

 dqworld.net