



# Cyber Security Resource Pack

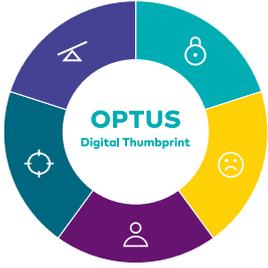
**OPTUS**

| Digital Thumbprint

October 2019

# Introduction

The **Optus Digital Thumbprint** program teaches young people to be safe, responsible and positive online through free, curriculum-aligned workshops that are fun and interactive. The Digital Thumbprint program has five key topics:



- **Cyber Security**
- **Cyberbullying and Respectful Relationships**
- **Online Digital Identity**
- **Digital Discernment**
- **Digital Balance**

Each workshop focuses on two of these topics as Core Concepts.

This document contains the teacher resources, top tips and take home sheet that support Cyber Security - what happens to your information and how to keep it secure.

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, a T-S interaction could be a teacher asking questions and a student replying. An S-S interaction could be students working in pairs. The description explains the actions and questions or concepts that are communicated throughout the lesson. Teachers can 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 Thumbprint workshop. 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. These resources can be printed and sent home with students and/or included in school newsletters.

# Cyber Security Lesson Plan 1

Section	Interaction	Description
<b>Intro</b>  Lead-in to set the context  🕒 3 min	<b>T-S</b>	<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"><li>1. What information do you need to start a Social Media account?*[Name, mobile number or email, date of birth, captcha code, password]</li><li>2. What things do you post online?*[Pictures of your yourself? Of your friends? Memes? Comments? Videos? Plans for the weekend? etc.]</li></ol> <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>

Section	Interaction	Description
<p><b>Controlled understanding activity 1</b></p> <p>To give students understanding of the consequences of their actions</p> <p>🕒 15 min</p>	S-S	<p>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."</p> <p><b>Put the students into three groups.</b></p> <p>Each group receives a profile handout about Sophia (these can be found in the handout section of this booklet). Group 1 - Profile 1, Group 2 - Profile 2.</p> <p>Students are asked to find out as much information as they can about Sophia in their groups.</p> <p>As a class, each group will discuss what they know about Sophia. After each group has discussed what they've found out, ask them if learning what the other groups know could reveal additional information to what they found, i.e. by using information about her (note that she has the same picture in each profile), anyone could find out: her name, her best friend's name, her cat's name, where she works, what job she does, her birthday, where she lives, her mobile number, where she's going to be on the weekend, which school she goes to.</p>
<p><b>Controlled understanding activity 2</b></p> <p>To give students understanding of consequences of their actions</p> <p>🕒 15 min</p>	S-T	<p>As students realise how much they now know about Sophia, discuss the implications of putting your information online. [Ensure students understand that even though Sophia has different types of information spread out over multiple social media accounts, this information can be combined to find out a lot of information about a person].</p> <p>"It turns out that Sophia is really nice, appreciates your thoughtfulness, and becomes quite popular in the class."</p> <p>"Alex has become super jealous of Sophia. What things could Alex do with the information we've learnt about Sophia? What might happen if Alex gained access to Sophia's account?"</p> <p>Lead a discussion around the consequences of making your information available online.</p>
	T-S	<p>Talk with the students about:</p> <ul style="list-style-type: none"> <li>• What might happen if someone who had a grudge against you knew where you worked and your mobile number. [They might prank call you, they might tell your manager rumours about you, etc.]</li> <li>• How they would feel if a stranger knew exactly where they would be and what they would be doing. [It would be easier for a person to rob you if they knew where you lived and when your house would be empty, people could stalk you, etc.]</li> <li>• If they would be willing to let a stranger know their school, their friends and their personal details. [They might open themselves up to having their accounts compromised and having their identity stolen]</li> </ul> <p><b>Optional:</b> Teacher can show students the Digital Thumbprint video about Sophia: <a href="https://vimeo.com/234486885">vimeo.com/234486885</a></p>

Section	Interaction	Description
<p><b>Conclusion</b></p> <p>Ensures students have understood the knowledge given and are prepared to be safe, responsible and positive online</p> <p> 5 min</p>	<p><b>T-S</b></p>	<p>Give students a quick, verbal true-false test about security and privacy.</p> <ul style="list-style-type: none"> <li>• You should have your social media privacy settings on public. [False]</li> <li>• If you use a fake name on one social media site, people won't be able to link it back to you. [False]</li> <li>• You should regularly check your privacy settings on your social media sites so you have control over what other people can see. [True]</li> <li>• Having the same password on multiple sites is okay because you can remember them easily. [False - every site should have a unique password]</li> <li>• You should review what you have on social media. [True]</li> </ul> <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>

# Cyber Security Lesson Plan 2

Section	Interaction	Description
<b>Intro</b>  Lead-in to set the context  🕒 5 min	<b>T-S</b>	<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"><li>1. "Have you ever had a bad experience online?"* or</li><li>2. "Has someone you know had a negative experience online?"* [Yes/No, what was the experience?]</li></ol> <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>
<b>Self-efficacy</b>  To allow students to identify what steps they can personally take to be safe, responsible and positive online  🕒 10 min	<b>S-S</b>	<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><b>Put the students into pairs.</b></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"><li>1. Who uses a password manager? Why might using a password manager be better than using the same password for every site?</li><li>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?</li><li>3. Has anyone been contacted by a stranger on the internet before? What did they want?</li><li>4. Which anti-virus program do you use on your computer and why?</li><li>5. Do all of your devices have a password set up on them? Is it the same password or different?</li><li>6. What services do you use that show other people your location?</li></ol>

Section	Interaction	Description
<p><b>Self-efficacy</b></p> <p>To allow students to identify what steps they can personally take to be safe, responsible and positive online</p> <p> 10 min</p>	<b>S-S</b>	<p><b>Put students into four groups.</b> Each group is allocated one of the following topics:</p> <ol style="list-style-type: none"> <li>Hacking</li> <li>Data theft</li> <li>Cyber stalking</li> <li>Identity theft</li> </ol> <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 <a href="http://cdpp.gov.au/crimes-we-prosecute/cybercrime">cdpp.gov.au/crimes-we-prosecute/cybercrime</a></p> <p>Give students guidance on where to report cyber-related incidents at: <a href="http://acorn.gov.au">acorn.gov.au</a> <a href="http://scamwatch.gov.au">scamwatch.gov.au</a></p> <p><b>Optional:</b></p> <p>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>
<p><b>Conclusion</b></p> <p>Ensures students have understood the knowledge given and are prepared to be safe, responsible and positive online</p> <p> 5 min</p>	<b>T-S</b>	<p>Give students a quick, verbal true-false test about security and privacy.</p> <ul style="list-style-type: none"> <li>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]</li> <li>You should make your details public. [False]</li> <li>You should be wary of people you don't know that try to contact you. [True]</li> <li>You should use an anti-virus program. [True]</li> <li>You should setup a separate password for your computer and phone and tablet if you have them. [True]</li> <li>You should post information that people could use to identify you or to find out your location. [False]</li> <li>You should make sure that a site's link that you click on is the correct address. [True]</li> </ul> <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.



Sophia Archer

Timeline ▾ About Friends 540 Photos Archive More ▾

Update Info 3 Activity Log 2 ...



## About

### Overview

Work and Education

Places You've Lived

Contact and Basic Info

Family and Relationships

Details About You

Life Events



Add a workplace



Studies at  
Crowds Nest High School



Lives in Sydney, Australia  
From Sydney, Australia



McLaren St, Crows Nest,  
Sydney, NSW, Australia



August 10, 2004

## Profile 2.

100% 4:15 pm Photo Sophie.A



Liked by rr\_brown, gracey18 and 22 others

**Sophie.A** Girls night in! #parentsoutoftown #slumberparty #bffs #disneynight

**Lizzie\_95kk** I'm running an hr late. Will be over around 5pm tonight. #excited!

**Sophie.A** Okay @Lizzie\_95kk we're getting pizza. Did you want pepperoni again?

**Lizzie\_95kk** Yes please! 🙏

100% 5:02 pm Photo Sophie.A



Liked by Daniel321, Emma121 and 12 others

**Sophie.A** Night training, where is everyone? @NorthSydneyOval #Finaltraining #timetosweat 🏈

**Taylor\_price** You're always early! Mum just picked me up, we'll be there in 30mins. See you soon!

**Emma121** Early again!

**Gengen88** Training doesn't start till 6pm why are you so early?

100% 10:03 am Photo Sophie.A



Liked by Taylor\_price, Gengen88 and 32 others

**Sophie.A** First ever latte art! What do you think? @CafeJK #comevisitmeatwork 🙏

**Kevin\_56** Great work Sophie!

**Emma121** Wow!

**Gengen88** Can you do it on hot chocolates?

# Digital Thumbprint

## Student Top Tips: Cyber Security

Cyber security is really important. These top tips will help you to keep your online information safe.

### 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 [howsecureismypassword.net](http://howsecureismypassword.net) can give you a rough guide as to how strong your password is.

### Use different passwords for different sites. ✓

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

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

### 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. ✓

### Respect other people's right to digital privacy. ✓

### Don't tell anyone your passwords. ✓

### Report cyberbullying at: ✓

- [esafety.gov.au/complaints-and-reporting/cyberbullying-complaints/i-want-to-report-cyberbullying](http://esafety.gov.au/complaints-and-reporting/cyberbullying-complaints/i-want-to-report-cyberbullying)

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

- See [esafety.gov.au/esafety-information/games-apps-and-social-networking](http://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. ✓

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

### 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. ✓

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

### If you need more help or information contact: ✓

#### Kids Helpline

call **1800 55 1800**  
visit [kidshelpline.com.au](http://kidshelpline.com.au)



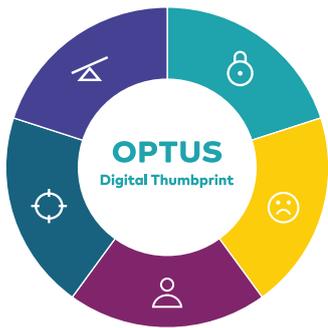
or

#### Office of the eSafety Commissioner

visit [esafety.gov.au](http://esafety.gov.au)



# Cyber Security Parent Discussion Guide



The **Optus Digital Thumbprint** program teaches young people to be safe, responsible and positive online through free, curriculum-aligned workshops that are fun and interactive. The Digital Thumbprint program has five key topics:

- **Cyber Security**
- **Cyberbullying and Respectful Relationships**
- **Online Digital Identity**
- **Digital Discernment**
- **Digital Balance**

This sheet is a resource that will help you to have a structured conversation with your children about cyber security. 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.

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

 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 [howsecureismypassword.net](http://howsecureismypassword.net)

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

 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 [esafety.gov.au/esafety-information/games-apps-and-social-networking](http://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.

 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 [youtown.com.au/apps/webcounselling/live/chat/](http://youtown.com.au/apps/webcounselling/live/chat/)

 If you or your child want to report cyberbullying, you can go to [esafety.gov.au/complaints-and-reporting/cyberbullying-complaints/i-want-to-report-cyberbullying/](http://esafety.gov.au/complaints-and-reporting/cyberbullying-complaints/i-want-to-report-cyberbullying/)

 The legal age to have an account on most social media sites (including Facebook, Twitter and Instagram) is 13. If you are unsure of the age restrictions, make sure to check the site's terms and conditions.

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

## If you need more help

# Optus Digital Thumbprint

For more free parent resources and conversation guides visit the **Optus Digital Thumbprint** website.

 [digitalthumbprint.com.au/resources](http://digitalthumbprint.com.au/resources)

**Optus  
Digital Thumbprint**



If you need more help or information contact Kids Helpline.

 1800 55 1800

 [kidshelpline.com.au](http://kidshelpline.com.au)

For more resources and information, visit the Office of the eSafety Commissioner website.

 [esafety.gov.au](http://esafety.gov.au)



Office of the  
**eSafety Commissioner**