safe space
A Kid’s Guide to Data Privacy
This book belongs to:

FULL NAME

BIRTHDAY

PASSWORD
safe space
a kids guide to data privacy
START
Find the balance.
Balancing Fun and Safety

When you ride a bike, you wear a helmet to protect your head. When you swim, you wear goggles to protect your eyes. And when you use the internet, you should always protect your personal information.

This includes being careful about what and to who you share: what you like or dislike, what you buy, who your friends are, where you go to school, and lots of other things. Why shouldn’t you share these things? Because there are strangers and companies who can use them to make money, or worse, cause you and your family harm.

But sometimes you’re forced to reveal details such as your full name and birthdate online. How do you know if you’re giving away too much information? This book is about finding the balance between having fun on the internet and protecting yourself.
Color in the different ways we use the Internet.
PART OF OUR LIVES

IT FOR:

CREATION

LEISURE
Overall, the Internet is a good thing.

But, just like a kitchen knife, the Internet can be a tool for good...

...or something that can cause harm.
Encircle the GOOD items green, and the BAD items red.

GOOD OR BAD?

Letting the internet keep you from studying or spending time with family and friends

Spreading fake news

Games, movies, and online books

Catching up with family members abroad

Hackers who want to steal your private information

Buying groceries, paying bills, and getting money from the bank

Cyberbullying (making fun of or threatening others)

Online classes when you can’t go to school

Chatting with classmates and friends

Strangers inviting you for a private chat
Can you get through all the obstacles and find your way safely to the safe side of the Internet?
To play, you'll need a game piece per player and dice. If you land at bottom of a ladder, move up to the top of the ladder. If you land on the head of a snake, you must slide down to the bottom of the snake. The first player to reach square 50 wins!
What is Personal Information?

Personal information is any information which reveals your identity or describes you.

These could be things like:

- Your name
- Your birthday & your age

DID YOU KNOW

When you sign up to use social media sites like Facebook, Twitter, Instagram, and Snapchat, or games like Minecraft and Pokemon, you give them access to personal information about yourself.
You have the right to keep your personal information safe and private. This is called Data Privacy.

THIS COULD ALSO INCLUDE:
- Where you live
- Your friends
- Your friends’ phone numbers and emails
- Even your crush!
You will already be revealing things about yourself every time you’re online.

Apps or websites can find out:

- What gadget you’re using
- Photos in your phone
- What time you’re usually online
- How long you’re online
- Who you always chat with
What browser you use

What photos you “like”

How long you stay in each website

What links you click on

What and whose stories you watch

How much battery you have

What filters you use
Find the following apps and services. Color in the ones you use.

- Amazon
- Animal Crossing
- Facebook
- Fortnight
- Google
- iMessage
- Instagram
- Lazada
- Minecraft
- Pokemon Go
- Safari
- Shopee
- Snapchat
- Spotify
- Tiktok
- Twitter
- Viber
- Warcraft
- Whatsapp
- Wikipedia
- Youtube
- Zoom
Why are they getting your info?

If apps and websites know what you like, they show you more of that stuff, so you’ll keep coming back. If you often watch anime on YouTube, it will show more anime videos the next time you log on.

They use contact details like your email and phone number to get in touch with you, and store information for your security. If you forget your password, they check if it’s really you trying to sign in to your account by asking questions about yourself. But they can also use your personal information to make money – by sharing and selling it to people and businesses.
They can, for example, share with a clothing company the types of clothes you’re into based on the pictures of pants, shirts, or dresses you’ve been liking and sharing. That company can then try to sell similar clothes to you through email or ads on your favorite apps and websites.
Navigate your way through the Internet. Be careful of the traps and dead ends!
HEI!

HEY.
Your personal information is very valuable. Protect it.
It’s important to know what personal information is being collected, who’s collecting it and how it will be used.

Information about you, such as the games you like to play, what you search for online and where you shop and live, has value – just like money.

- Only use a product or service if the company is open about how it will use your personal information.
- Think twice if an app wants permission to use your personal information (like your location).
- If you’re not sure about any of these, ask your parents or other trusted adults.
Design a t-shirt about yourself using only emojis.
How can you practice data privacy?

1. Someone finds a friend’s diary. They copy an entry they like and share it online.
   Is this okay?

2. A classmate has a picture with a famous celebrity, but they only shared it with their closest friends, including you. You think it's awesome so you download the photo and post it publicly.
   Is this okay?
A classmate made a fake Facebook account impersonating another classmate, and started making embarrassing posts. What do you do?

Ask permission before posting information or photos about other people.
Post only about others as you would have them post about you.

Respect their privacy!

The GOLDEN RULE
Think before you click!
If your friends, parents or teachers see your post, will they have a good impression of you? Will someone get hurt or sad because of your post?

Be responsible. On the internet, everything can be searched, shared and found. Nothing is ever really deleted.
Where and how is all of this data stored?

Did you know that the US Library of Congress collected every single public tweet - hundreds of billions of them! - from 2006 to 2017? They may have stopped for now, but nothing prevents it, or others, from starting again.

Everything you put out there has the possibility of becoming PUBLIC and PERMANENT.

Future employers can investigate your past and decide not to hire you because of something you wrote while you were a kid.

So be careful with what you post!
If you send an email from your Yahoo account to your friend’s Gmail account, there will be a copy of that email on both Yahoo’s and Gmail’s servers.

Or your friend could have saved the pictures, files or messages you’ve sent then erased.

Even if you delete the original copy of any digital information, copies of it will continue to exist in other places.

When you delete a post from social media, it may not really be gone. It often remains in the servers (large computers) of the social media company so they can continue to use it.

This explains how they can remind you of posts you made from years back, even if you had already erased those posts!
If you post a photo, it will be stored online, letting other people use it without your permission! Try it out in this scene. Can you find all the copies of a girl’s photo?
IT'S OK TO LIMIT WHO CAN SEE YOUR INFORMATION AND WHAT YOU SHARE.

Use the privacy and security settings in your favorite online games, apps and platforms.
Assume that all your posts, texts, and messages are public.  
Anyone can copy your posts and distribute them.

Set your privacy settings.  
Study the sites and apps you use and control who sees your posts.

Remove past posts you’re not comfortable with.  
If you have pictures or posts you regret posting, go ahead and delete them.

Think about the future.  
Always ask yourself: Is there anything in this post or comment that could hurt me or others in the future?
Be careful of what you share!
The internet brings us closer.

Nowadays, you can talk to loved ones in other countries anytime! In the past, your parents had to wait for weeks, or even months, to receive a letter with photos enclosed. Now, it only takes a few seconds to post and receive pictures.

But...

You still have to be careful! There are people other than your family and friends who will see what you share. And what you share contains information about you.
A picture is worth a thousand words.

At first glance, this looks like a harmless photo. But you can still get clues about the photographed kids even if you don’t know who they are!

For starters, you now know what they look like. They’re also wearing their IDs (which you can enlarge) that state their names. Their uniforms tell you where they go to school. From there, you can find out the time they go in and out of school.
HUNT FOR CLUES

What can you find out from looking at these pictures? Then turn the book upside down to see the answers! Did you think of anything else?

Jenny Cruz
26 mins ago

3 comments • 1 share

A street sign and her house number (basically, her address) • That she has a pet • What she looks like •
Thanks to everyone who came to celebrate with me!
#happybirthdaytome
• What she and her family look like
• That they’re in Paris and therefore not at home (would bad people be able to break into their house?)

• What she and her family look like
Don’t forget!

- Do not post anything you wouldn’t want a parent, teacher, or someone you admire to see.
- Be patient. Pause and think before you post.
- Be careful about posting something you think is funny, but could end up insulting others.
1. Think of a fun phrase or sentence (at least 8 words) that you can remember.

Creating a secure password is easy and fun.

2. Choose the first letter of each word in the phrase.

CASP E A F

3. Change some of the letters into symbols or numbers.

C A $ P 1 E @ F

4. Make some letters uppercase and some lowercase.

C a $ p 1 e @ F

Now, go make your own!
Tips for securing your passwords:

Use a different password for each account.

Secure your devices.
Use strong passwords, passcodes or touch ID features to lock your device. This helps protect your information if your device is lost or stolen.

Make your passwords memorable so you don’t have to write them down.
Otherwise, someone might find or see what you wrote!

Don’t use personal information or common words.
Don’t use "password" as your password!
Use at least 8 characters, and a combination of letters (uppercase and lowercase), numbers and symbols. The longer, the better (as long as you can remember it!)

Never share your password with anyone other than your parents.

Immediately change your password if you think someone else might have gotten it.

When in doubt, throw it out.
Links in emails, tweets, posts, and online advertising is often the way bad guys access your personal information. If it looks weird, ignore or delete it.

Public wireless networks and hotspots are not secure.
Anyone can see what you are doing on your laptop or smartphone while you are connected. So be careful with the sites and apps you’re using!
Here are 2 versions of the same account. Can you find all the differences between them? Which account is safer?
Angie Dy

INTRODUCTION
My favorite things are unicorns, ice cream, and highlighters!

STUDIES AT
San Sebastian Elementary School

FRIENDS SEE ALL

LIKE COMMENT SHARE
1. Make your parents your Internet buddies.

Let them know the websites you visit or want to visit, the people who chat with you and send you e-mails, which social networking sites you’re on, and more. If you receive a suspicious message, tell them immediately.

2. Never give away personal information.

If someone or something asks you what your full name is, where you live, where you go to school, what your birthday is, or other information about the people in your life, don’t answer!
Don’t choose a username that includes personal information.

For example, if your name is Juana Rizal, you were born on April 20, 2000 and you live in Pasig City, Philippines. Don’t make JuanaRizal042000fromPH, or anything similar, your username!

You can be a champion gamer with a champion name that doesn’t reveal your identity.

Share pictures with care.

Don’t send pictures and videos of you, your family and friends, your home, and your school to strangers online.
Guard your passwords.

If someone else knows your password, they can change it and lock you out of your own account.

They can also pretend to be you and speak in a foul language, cause a dip in your player rankings (oops!), share your photos, and spread false information.

Think twice before clicking on links or downloading files.

These could be viruses in disguise or sent by someone who wants to steal your personal information.
When a stranger chats you up, tell your parents or a trusted adult. Especially when they ask you to meet up with them. If strangers talk to you online, it’s best to ignore them. You never really know who they are in real life.

Phishing is when someone tries to steal information by pretending to be someone you trust through an email, text, or other forms of online communication. Phishing emails – and the unsafe sites they try to send you to or the attachments they try to get you to open – can put viruses in your computer.

When in doubt, talk to your parents or a trusted adult. If something or someone online is bothering you, tell your parents or someone you trust about it.

A website or ad can’t tell if there’s anything wrong with your machine!
The Internet is great!

WE ARE ALL CONNECTED BY THE INTERNET

WE ARE ALL NOW DEPENDENT ON THE INTERNET

WE CAN PRACTICE ANYTHING

WE CAN NO MATTER IN THE
WE CAN FIND OUT MOST OF THE THINGS WE NEED TO KNOW

IT’S A SOURCE OF ENTERTAINMENT & ADVENTURE

TALK TO EACH OTHER WHERE WE ARE
But, be careful out there.
Be careful with what you share.

Never share your password with anyone other than your parents.

Post only about others what you would have them post about you.

Keep your wits about and the internet will be a safe and awesome place for learning, connecting, and exploring.
Let's play Bingo! Cross out all the "safe internet tips" that you already do.
There's a secret message hidden in this page!
Write the first letter of each drawing to crack the code.
The benefits of the online world far outweigh its disadvantages. Children need to know how to navigate the internet if they are to be productive and competitive in the future.

Still, children are highly impressionable and may not be ready for everything found on the internet. Their natural curiosity, combined with their lack of maturity, can make them wander off to unsafe cyber corners. Age-inappropriate content remains as the biggest risk for them.

Teaching children about online safety and privacy should begin with you, their parents and teachers. You are the adults that your children trust the most.
Be present and involved.
Be aware of when, where and how they use the internet. Show interest in the sites they visit and the games they play.

When you think your children are ready to have a social media account, set one up together. Walk them through the platform and help them understand its privacy settings. Give them tips if they receive friend requests from people outside their circle.

Set Boundaries.
Communicate and be honest with your children, but also remember you are their parent or teacher first, and their friend second.

Children must realize that they don’t get to keep their online (or other) activities 100% confidential.

Reassure your children that just because they get checked up on every now and then does not mean you don’t trust them. Rather, it is the people they’re interacting with online that you are being careful about.

Value your child’s personal information.
As a parent, it is your right to protect (and if necessary, withhold) personal details about your children. Teach them to also protect and value their personal information. Explain to them why they should first ask your permission before they provide information such as their names, ages, birthdates and addresses online.

Share with care.
We know you’re proud of your children. But remember that posting photos of your kids creates a permanent trail that follows them as they grow up.

Once you post a photo online, you lose control over it. It can easily be copied, tagged, saved and used for whatever purposes you might not have imagined.

Everything you post has information valuable to advertisers and data collectors.
**Check your privacy settings.**

Be mindful of the information you and your kids are sharing when using apps and visiting websites. Check and adjust the privacy settings of the device, browser, apps, and social networking sites you use.

If your child has a smartphone, you can make it safer by turning off location services, and preventing apps from sharing data. You have the power to decide who gets to see their posts.

**Teach the child to behave as if the Internet were a public space.**

Make sure they understand the basics of good online behavior, including thinking about the impact of posting a photo or comment. Remind them that it’s not always easy to take back something they posted online, and that texts and photos can be forwarded to anyone.

It’s good to follow the Golden Rule. Tell your kids that the things they wouldn’t do in real life shouldn’t also be done online.

Teach them how to report mean behavior or unkind content on their favorite websites.

**Stay current.**

Keep pace with new ways to stay safe online and ways to manage privacy. Share what you discover.

Finally, keep talking to your children, not just to teach them, but also to learn from them. They probably know more about what’s out there!
ANSWER KEY
ABOUT CANVAS
ABOUT CANVAS