BLUEPRINT

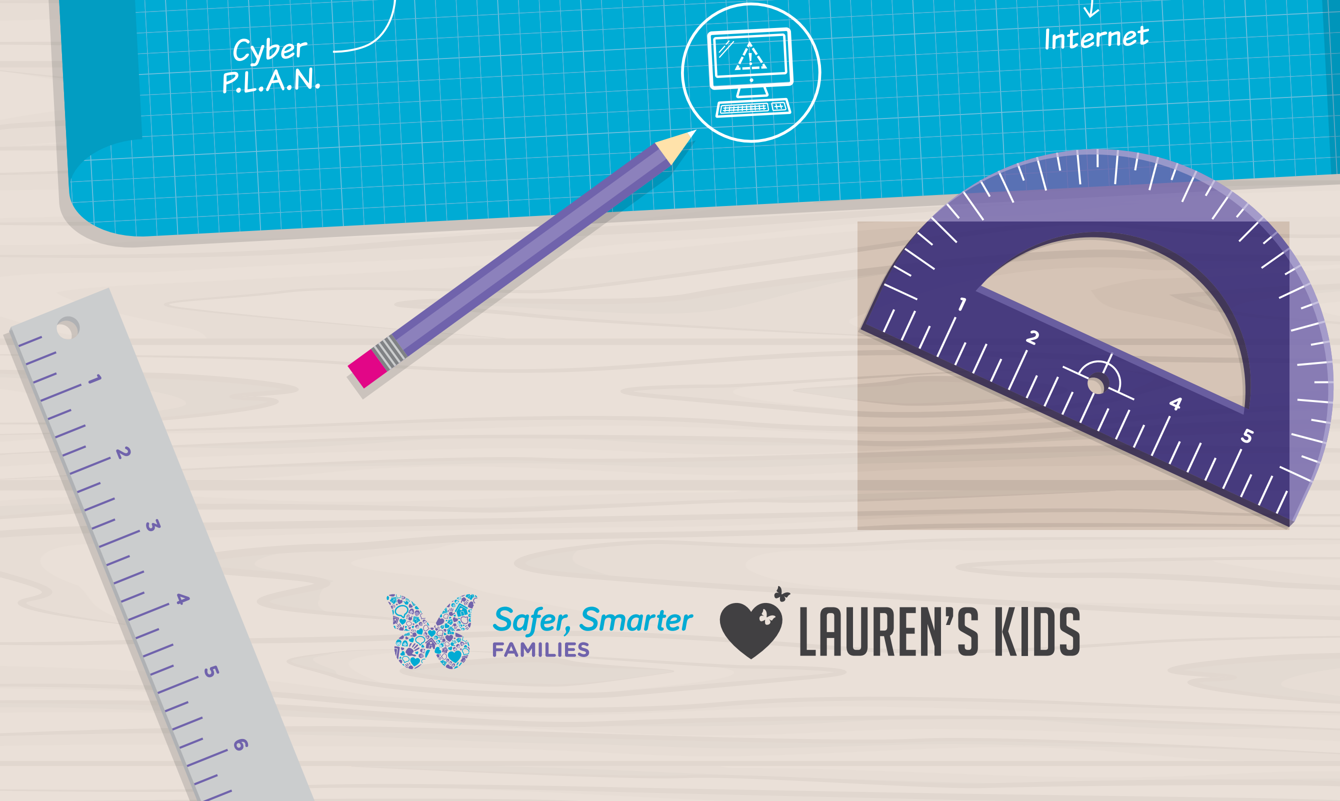
FOR BUILDING SAFER, SMARTER FAMILIES

Password

Building Safety in the Digital World

Cyber P.L.A.N.

Internet



Safer, Smarter FAMILIES

LAUREN'S KIDS

BUILDING SAFETY IN THE DIGITAL WORLD

TIPS FOR PARENTS

Brought to you by Lauren's Kids and the Broward County Sheriff's Office

DID YOU KNOW?

- 1 in 5 children are solicited sexually through the Internet before their 18th birthday.
- Access to the Internet and digital devices should first and foremost be treated as a privilege, not as a right. Allowing a child access to the Internet without very strict oversight would be like allowing that same child to travel overseas without a parent or chaperone.
- Each Internet-capable device acts as an open door for millions of people directly into your or your child's life. Multiply that by the number of devices in a normal household and the potential for harm is staggering.
- Gaming systems, deactivated cell phones, iPods, and other such digital devices can also access the internet over WiFi. Many games, even those that cater to young children, give players access to servers where they are exposed to other players who can communicate with them through gameplay and chat features.

STEPS TO DIGITAL SAFETY

Step 1: Prior to giving any Internet-capable device to a child:

- Conduct a thorough investigation into that device's capabilities.
- Ensure you are the primary user/administrator and that at no time can a password or setting be changed or an application downloaded without your approval. Do not give your child your administrative password.
- Set up the device to only allow children access to a specific set of websites or applications. These settings vary from device to device. Ask the retailer where the device is purchased for specific information about your device.

Step 2: As the device administrator, you must be present every time an application is downloaded or a game set-up is conducted. This way, you know exactly what each application is capable of doing and can choose the most appropriate settings. Changing settings at a later time is always more difficult. Research each and every application/game prior to installing it.

Remember, just because your child's friends have an application or game does not mean it is safe.

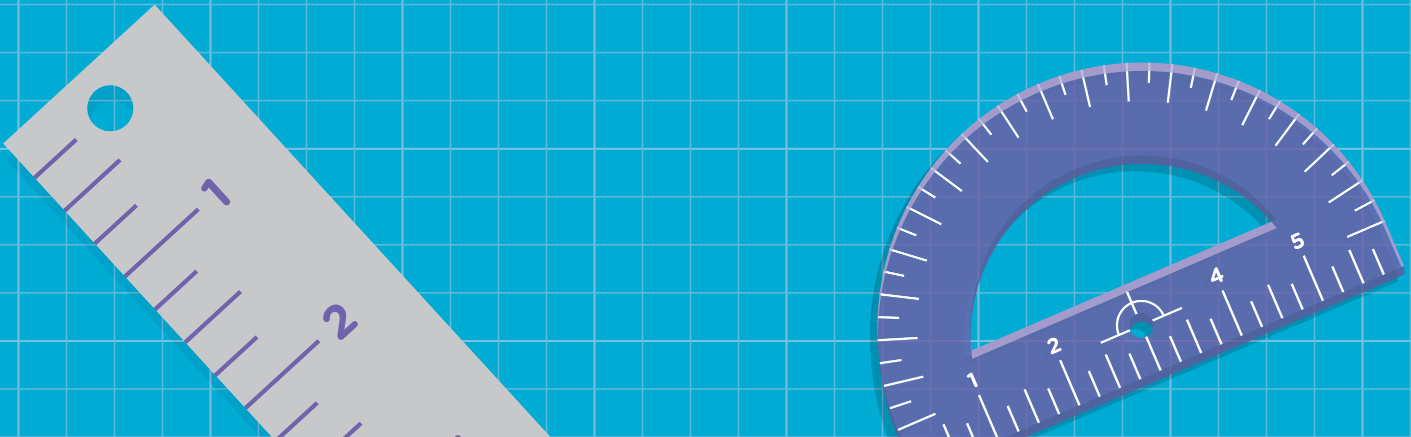
- Some applications require location settings be turned on at all times or contact lists be shared. This allows other users, many times strangers, to know the exact location of your child or who their friends and relatives are.
- Some games allow access to PvP (player vs. player) scenarios where players can communicate with each other verbally (over headsets) or by typing messages to each other.
- Some settings, in something as innocent as the camera, can allow someone to determine the exact time and location a photo was taken after it is posted on social media.

This information may seem harmless, but it is important to realize that child predators seek out victims to groom on these platforms every single day because they allow for instant access to children and provide the ability to shield one's true identity.

Step 3: The constant monitoring of children's devices is one of the most effective ways to protect them and others. Parents usually report having no idea that their child has been involved with – or even sending photographs to – strangers online. It is natural for children to want privacy and autonomy, and to attempt to shield online activity from their parents. But if parents are diligent, they will be able to spot signs of unsafe use of the Internet before problems occur. Your child may get angry or upset about your monitoring of their devices, but remember that it is your job to keep them safe.

- Monitoring devices will not only keep them safe from unsafe adults, but will also ensure your child is not engaging in any type of cyber bullying activity or being the victim of cyber bullying themselves.
- Before you grant your child access to any Internet-capable device, create a contract with your child stating that as their parent, you will protect them.
- All of their devices will be subject to monitoring by you at any time, and if the request is refused, the device will be forfeited. If this rule is established from the beginning and reinforced throughout their childhood, it will be less likely you will receive resistance from your child since device checks will be conducted regularly.
- Create a reminder on your calendar to check your child's devices and apps on a regular basis. Children are children and they will make mistakes, especially when unsupervised – so you must remain vigilant.
- Being "friends" with your children on social media should not be considered an alternate option for checking devices. Many times, children will set up multiple accounts on the same social media platform they use to communicate with other people, or they will use settings to limit your visibility into the content they post.
- Do not share any digital or Internet-capable device's password with your child. Providing the child with the password can, depending on the vigilance of the parents in monitoring devices, allow the child to change device settings and provide the ability to download applications/programs. While it is inconvenient for the parent to constantly enter passwords for their child, it is necessary to ensure their safety.
- Consider the following when providing your WiFi password to those outside your family: Your IP address can be used by others to download illegal content over your WiFi. If an investigation is conducted, your IP address will be linked to the download.
- Use a post-it note or sticker to cover the webcam that is present on most laptops and some gaming systems when the cameras are not being used to avoid the possibility of it being covertly activated.

AS CHILDREN ENTER THE DIGITAL WORLD, PARENTS AND CAREGIVERS MUST BE VIGILANT. ULTIMATELY, YOU ARE – AND NEED TO BE – THE FRONT LINE IN THEIR DIGITAL SAFETY.



The Building Blocks of Family Safety

GROUNDWORK

These activities will provide you and your elementary school child (K-5) with the background knowledge you need to understand the safety strategies at the core of the Lauren's Kids lessons. Once, completed, move forward with the additional activities in the pack.

KINDERGARTEN–5TH GRADE ELEMENTARY SCHOOL-AGED CHILDREN

DIGITAL SAFETY

The safety concepts and safety tools that you and your child are learning throughout these activities are important to keeping your child safe in the physical world. But, how do you keep your family safe in the digital world? With the daily changes that occur in technology, it is hard to keep up with all the new information, websites, apps, and terms. Keeping your knowledge of technology current, and creating procedures for use of the internet and digital devices in your home are the first steps in developing these important safety tools.

It is vital children understand safe uses for the Internet and that parents consistently monitor their children's use of the computer, tablet, phone, and all digital devices.

- What are the rules for using the Internet in your home?

- Where is your computer located in your home? Is it in a public place in your home?

- What spam filters and safety settings are enabled on your computer and other devices?

- What other digital devices does your child have access to? (Such as tablet, cell phone, iPod with internet connectivity, or gaming system with internet connectivity)

- Create a list of Internet safety rules for your household. Post them in a conspicuous place, next to a computer, tablet, or gaming or phone charging station. Review these rules with your child and allow your child to explain to you why each rule is important in helping them to make safe choices.

- Talk to your child about their use of the Internet. Help them to understand that there are some people on the Internet that are not who they say they are. We really never know who we are communicating with on the Internet, so it is always important to make safe choices.

- Do you use passwords to secure your login information on digital devices and accounts? Are your passwords private and secure? Passwords should always be used and should never be shared with your child. Access to the Internet on any device should be enabled by a parent entering the password, as should passwords to log in to digital devices themselves. While this practice may seem to be time consuming and inconvenient, it will protect your child and enable you to monitor the use of the Internet by your child.

HOW TO HELP YOUR CHILD MAKE SAFE CHOICES IN THE CYBER WORLD

Because the online community is much larger than your local community, it is important that your child understand that there are certain behaviors that are unsafe:

- Communicating with someone they don't know
- Posting personal information on the Internet
- Posting pictures online or sending a picture to someone they don't know without permission
- Entering a chat room and engaging in a conversation, even on popular gaming systems like Xbox or PlayStation
- Visiting inappropriate sites

Discuss that making safe choices on Internet devices is a condition of having access to those devices. Assure your child that they should talk to you any time they have a question about anything that they encounter on the internet that is confusing or makes them feel uncomfortable.

While it is important to respect your child's privacy, you have a responsibility as the owner and account holder of those devices to monitor their uses and activities. Your child should also understand that it is a privilege to use these devices.

Parents should monitor their child's use of the computer, tablet, phone, and all digital devices.

To Do:

○ Gather Tools

○ Prepare Soil

○ Measure

○ Wear Safety Gear

The Building Blocks of Family Safety

LAYING THE FOUNDATION

KINDERGARTEN–5TH GRADE ELEMENTARY SCHOOL-AGED CHILDREN

In Laying the Foundation, we develop key safety concepts that will continue to be built upon throughout this activity pack. These concepts have been introduced through the Groundwork activities.

Involving your child in the activities in this activity pack is very important. Reinforcing the strategies and tools your child has learned will help them make safe choices and decisions. Initiate discussions with your child and help them understand that they can develop the personal power within themselves to make choices and decisions that keep them safe. Children can use that power by recognizing warning signs that alert them to unsafe situations. Keeping the lines of communication open with your child is an important step in being one of the trusted adults to whom he or she can turn.

Parents must consider that even very young children are now more technologically savvy because they have never lived in a world without the technology that exists today. It is common to see preschool-aged children expertly navigating sites on their parents' phones or their own hand-held tablets, and technology is becoming more integrated into school classrooms. As such, it is never too early to start to discuss cyber and digital safety with your child. It is important to establish rules for your child's use of digital devices, to discuss their importance, and to monitor your child's adherence to these rules. It is always important to tie the rule itself to the "why" behind the rule. The "why" of all digital safety rules is always SAFETY. Reinforce the fact that your child must always tell you or another trusted adult about anything they encounter in the digital world that makes them feel unsafe…just like any unsafe situation encountered in the physical world.

RULES FOR THE DIGITAL WORLD

- Always ask for permission from a trusted adult. Ask for help logging in with the password before going online or using a digital device.
- Use a post-it note or sticker to cover the webcam that is present on most laptops and some gaming systems when not in use to make sure that someone doesn't remotely hack the camera on your devices. Predators can use the camera on your laptop and some gaming systems to watch you when you don't know it.
- Never send personal information or any pictures to anyone you don't know.
- Chat rooms and features are not safe. Never accept an invitation to chat with anyone online, and do not use the chat features on games or apps.
- Always tell a trusted adult if you find an unsafe website or are made to feel uncomfortable by someone's language or behavior in the digital world.

Ensuring your child's safe use of the Internet and digital devices begins with parent supervision and regular monitoring. Review the Cyber Safety Checklist for Parents below. Place a check in each box when you are sure that you have procedures in your home that address the safety of all devices and internet accessibility.

□ Computers, tablets, and phones should always be used under your supervision, with your permission, and in a public place in your home.

□ Spam settings and parental controls should be enabled on your family computer to block unsafe images and websites.

□ Make sure all accounts and digital devices are password protected. Do not allow your child access to passwords. Instead, monitor their use by logging in using your secure password each time your child wants to go online or use a device.

□ Your child should understand that anytime they are confused by something they have viewed on the Internet, or if they have an interaction online that makes them uncomfortable, you want to know and you will help them.

SHOULD I TELL A STRANGER?

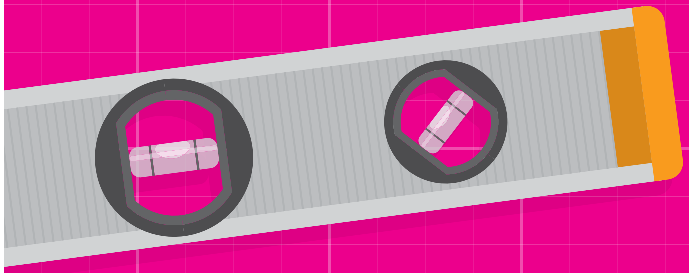
Remind your child that a stranger is just someone that they don't know or don't know well. Sometimes, a stranger may ask your child a question that is safe to answer. However, certain questions and certain kinds of information are unsafe to share with a stranger.

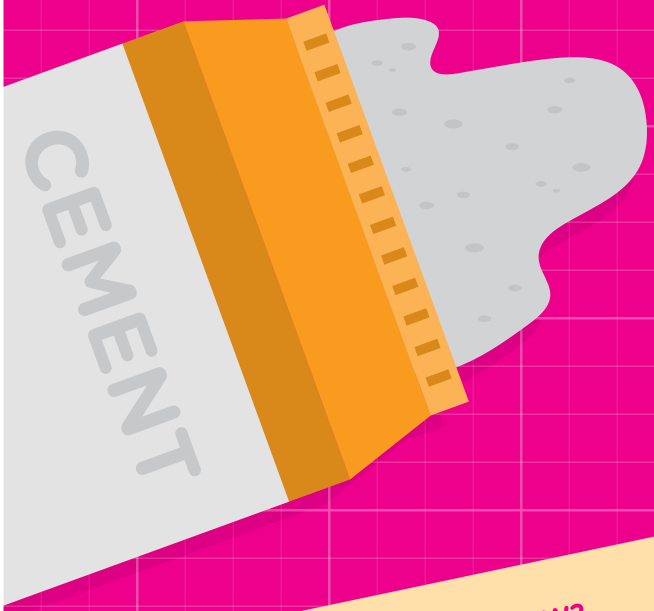
Review this concept with your child. Using the questions below, ask your child to tell you if the question is safe or unsafe? Role-play how your child could answer a safe question, and how they could decline to answer an unsafe question. Reinforce with your child they don't have to answer any question that makes them feel unsafe or confused, and that if they are unsure if it is a safe question, and they should always get help from a trusted adult.

1. How are you today? Is it safe or unsafe to answer this question? What would you say?
2. What is your address? Is it safe or unsafe to answer this question? What would you say?
3. What's your favorite color? Is it safe or unsafe to answer this question? What would you say?
4. What's your phone number? Is it safe or unsafe to answer this question? What would you say?
5. What's your favorite ice cream flavor? Is it safe or unsafe to answer this question? What would you say?
6. What's your last name? Is it safe or unsafe to answer this question? What would you say?

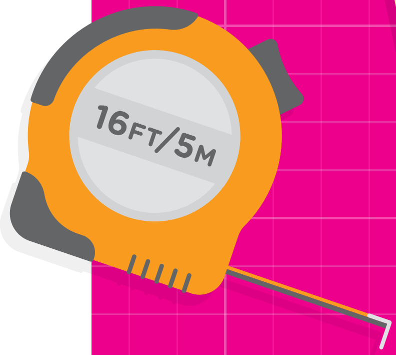
Reinforce the concept that online, everyone is a stranger because you don't know for sure who they really are. Remind your child that they should not be using chat rooms or chat features on games or apps. Children should never share information or answer any questions online – even if it seems safe to do so.

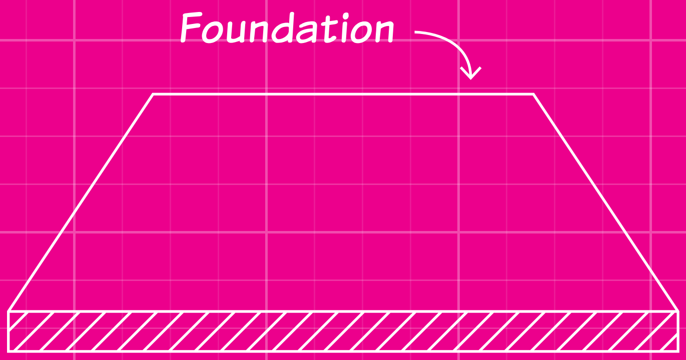
Answers: SAFE: 1, 3, 5; UNSAFE: 2, 4, 6





DID YOU KNOW?
Children who received the Safer, Smarter Kids curriculum achieved a 77% increase in knowledge of critical personal safety information.





The Building Blocks of Family Safety

POWER TOOLS

3RD–5TH GRADE ELEMENTARY SCHOOL-AGED CHILDREN

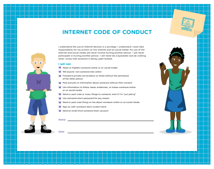
In Power Tools, you will find strategies to reinforce and apply safety lessons your 3rd–5th grade child learned through previous activities. As your child becomes more independent in school and after-school activities, they will use their Power Tools to ensure their safety. You can help your child to internalize these important safety strategies.

BUILDING POSITIVE CYBER CITIZENSHIP

Technology changes daily and new sites and apps are launched all the time, so it is vital for parents to consistently monitor their child's use of the computer, tablet, phone, gaming system, etc. While it's important to respect your child's privacy, you have a responsibility as the owner and account holder of those devices to monitor the uses and activity of them. Your child should also understand that it is a privilege to use these devices, not a right.

Your child is learning about the positive characteristics of citizenship in school, and – if they are receiving lessons from the Safer, Smarter Kids curriculum – they are also learning about the characteristics of positive Cyber Citizenship in their classroom. In Safer, Smarter Kids, expectations for appropriate behavior and responsible practices in the cyber world are stressed as part of safety education. Positive Cyber Citizenship is important in your home as well. Consider the following:

- What are the rules for the use of Internet and digital devices in your home?
- What are the safety settings on your Internet and digital devices?
- What should your child do if they find an inappropriate website or see an image or receive a message that is upsetting?
- Do you know who is photographing your child and where those photos are being posted?
- Does your child understand that once something is posted on the Internet, texted, tweeted, etc. it is permanent…even if it is deleted?
- Does your child know not to post any personal information about themselves – pictures, address, email address, phone number, etc. – online?
- Does your child understand that posting any personal information about others is inappropriate?
- Does your child understand that communicating with someone they don't know is very dangerous online because they never know with whom they are actually communicating?
- Does your child understand that chat rooms and chat features on games are dangerous?



INTERNET CODE OF CONDUCT

I understand the use of Internet devices is a privilege. I understand I must take responsibility for my actions on the Internet and on social media. My use of the Internet and social media will never involve hurting another person. I will never participate in hurting another person. I will never be a bystander and do nothing when I know that someone is being cyber-bullied.

I will not:

- Tease or frighten someone online or on social media
- Tell anyone I am someone else online
- Forward a private conversation or email without the permission of the other person
- Post pictures or information about someone without their consent
- Use information to follow, tease, embarrass, or harass someone online or on social media
- Send or post rude or scary things to someone, even if I'm "just joking"
- Use someone else's password for any reason
- Send or post rude things or lies about someone online or on social media
- Sign on with someone else's screen name
- Send an email from someone else's account

Name: ____________________

Date: ____________________

HANDS-ON ACTIVITY: INTERNET CODE OF CONDUCT

Locate the **Internet Code of Conduct** sheet in your child's Activity Book. Review the Internet Code of Conduct with your child to help in their development as a positive citizen of the cyber world and responsible user of digital devices. Your child's conduct on the Internet and with digital devices should mirror their behavior in the physical world. Appropriate behaviors and productive interactions with others is the foundation of positive citizenship.

Ask your child to sign and date the Internet Code of Conduct. Remind your child frequently that you expect them to follow the code and that their behavior online will be positive and productive.

HANDS-ON ACTIVITY: APP INVENTORY

APP INVENTORY

Directions: Together with your child, review all of the apps installed on the digital devices they have access to and list them in the table below. Fill in what type of app it is (for example - game, video player, etc.). Monitor your child's devices often to ensure that any app your child has installed is safe and has been installed with your permission and knowledge. Have your child sign the pledge at the bottom, and keep this chart in a public place in your home.

APP NAME	DEVICE	TYPE

MY APP PROMISE

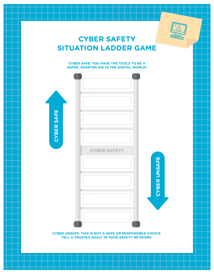
I, ________________________, promise not to install any apps without the knowledge and permission of my parents. I know that this promise keeps me safe.

________________ Child's Signature

________________ Parent's Signature

Locate the **App Inventory** sheet in your child's Activity Book. Along with your child, review all apps installed on the digital devices they use, and complete the chart for safe monitoring. Fill in what type of app it is (for example, a game, video player, etc.). Monitor your child's devices often to ensure that any app your child has installed is safe and has been installed with your permission and knowledge. Have your child sign the pledge at the bottom, and keep this chart in a public place in your home.

HANDS-ON ACTIVITY: CYBER SAFETY



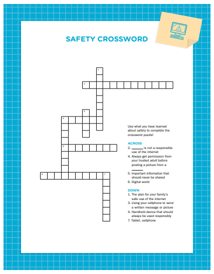
CYBER SAFETY SITUATION LADDER GAME

CYBER SAFE: YOU HAVE THE TOOLS TO BE A SAFER, SMARTER KID IN THE DIGITAL WORLD!

CYBER UNSAFE: THIS IS NOT A SAFE OR RESPONSIBLE CHOICE. TELL A TRUSTED ADULT IN YOUR SAFETY NETWORK.

Locate the **Cyber Safety Situation Ladder Game** in your child's Activity Book and help your child choose whether each situation is safe or unsafe by reading the explanations of each situation. Your child will need scissors. Answers are provided on the last page.

HANDS-ON ACTIVITY: SAFETY CROSSWORD



SAFETY CROSSWORD

Use what you have learned about safety to complete the crossword puzzle!

ACROSS

2. ______ is not a responsible use of the internet
4. Always get permission from your trusted adult before posting a picture from a ______
5. Important information that should never be shared
6. Digital world

DOWN

1. The plan for your family's safe use of the internet
3. Using your cellphone to send a written message or picture
4. Handheld device that should always be used responsibly
7. Tablet, cellphone

Provide your child with the **Safety Crossword Puzzle** activity from your child's Activity Book to help reinforce safety concepts. Answers to the crossword puzzle are provided on the last page of this booklet.

HANDS-ON ACTIVITY: WHAT THIS MEANS TO ME

WHAT THIS MEANS TO ME

Why is it important to have a Cyber P.L.A.N.? How does it keep you safe in the digital world?

____

SAFETY CHECK UP

See what you learned about building a plan for safety!

1. It is okay to text embarrassing pictures of someone if it is a joke. True or False
2. A ________________ is a safe secret and should never be shared with anyone.
3. If I find an inappropriate website by accident, I should:

____

4. I should never post pictures of others or myself on social media without the permission of trusted adults. True or False
5. What should you do if someone on a gaming site asks you for personal information?

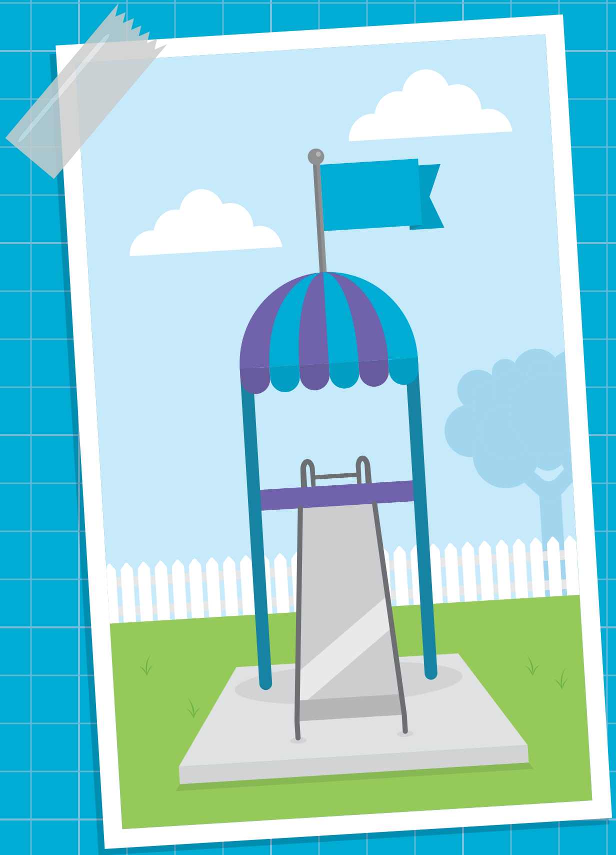
____

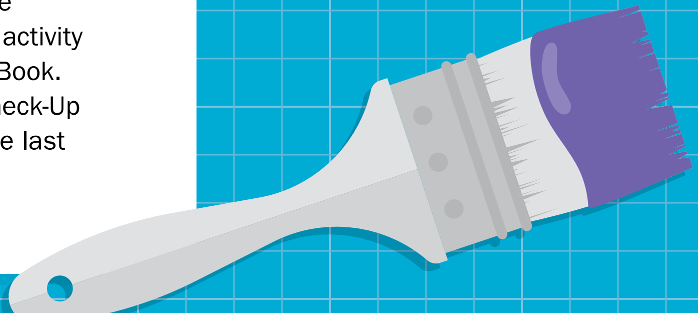
Provide your child with the **What This Means to Me** activity from your child's Activity Book. Answers to the Safety Check-Up section are located on the last page of this booklet.

DID YOU KNOW?

95% of sexual abuse is preventable with education and awareness.

Finished Playhouse!





HANDS-ON ACTIVITIES ANSWER KEY

SAFETY WORDS

S	C	M	S	C	Y	B	E	R	T	S	Q	W	U	Z
Y	E	N	C	J	O	Q	G	R	A	C	Z	W	C	V
C	L	Y	Y	R	Q	S	A	F	E	T	Y	T	A	E
A	L	K	B	H	N	K	Y	H	L	R	R	B	Z	S
M	P	V	E	N	Q	U	A	V	G	Y	Q	V	K	W
E	H	E	R	I	I	F	M	E	I	W	J	M	B	S
R	O	D	P	P	T	O	N	W	C	R	W	Z	E	V
A	N	O	L	A	D	I	N	T	E	R	N	E	T	E
T	E	J	A	S	R	Q	K	A	D	R	U	F	F	I
Y	N	S	N	S	C	B	T	W	W	U	H	E	X	Z
L	D	A	N	W	X	C	U	Z	R	A	T	O	P	K
U	M	N	G	O	U	E	G	R	V	C	E	I	O	U
L	H	W	S	R	B	P	O	F	L	I	X	F	M	A
H	D	V	F	D	C	D	U	W	X	I	T	V	S	C
D	X	K	R	O	V	Z	H	I	G	N	F	T	X	D

SAFETY CROSSWORD

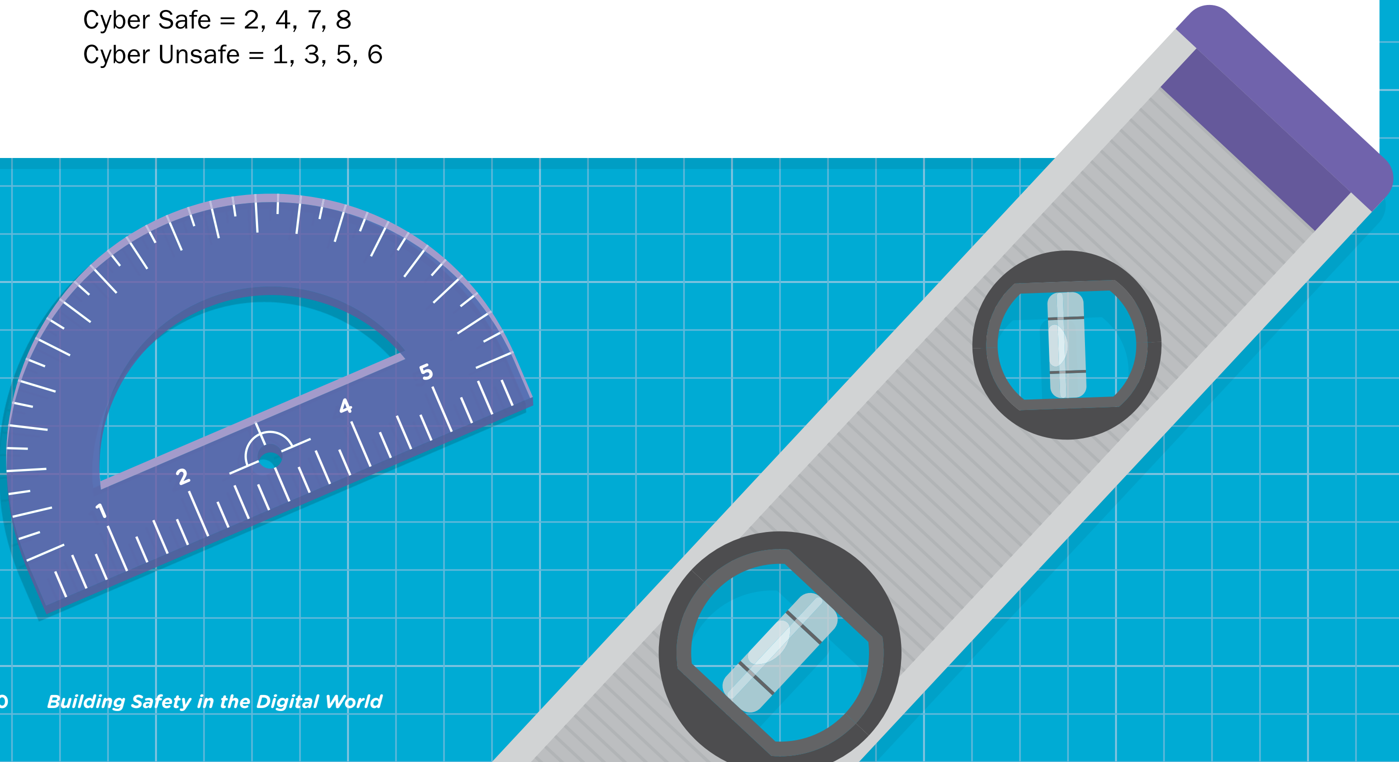
								1C										
								Y										
						2C	Y	B	E	R	B	U	L	L	Y	I	N	G
								E										
								R										
								P										
						3T		L										
			4C	A	M	E	R	A										
			E			X		N										
			L			T												
			L															
			5P	A	S	S	W	O	R	D								
			H															
			O															
			N															
6C	Y	B	E	R	W	O	R	L	7D									
									E									
									V									
									I									
									C									
									E									
									S									

WHAT THIS MEANS TO ME

1. False. Texting hurtful pictures or information is cyber bullying and is unsafe.
2. Password
3. Tell a trusted adult and block that site in our filters.
4. True
5. Never give personal information to anyone online. Block that person from being able to contact you. Tell a trusted adult in your Safety NETwork.

CYBER SAFETY SITUATION LADDER GAME

Cyber Safe = 2, 4, 7, 8
Cyber Unsafe = 1, 3, 5, 6



LAUREN'S KIDS