The Arc of New Jersey

Home Sexuality Education Curriculum

Lesson 9
Internet Safety
(Staying safe on the computer and phone)

Contents

- Just because online sexual abuse takes place or begins on a screen doesn't mean it is any less harmful.
- People with IDD need to learn about this type of violence so they can avoid being victimized...and avoid accidentally committing their own offenses.
- Because of lack of transportation and other social barriers, the internet is a useful tool to create social connections.

Modern technology is, on the whole, pretty great (Jeff Bezos would agree!). However, it is a tool like any other that requires a little training before use.

Learning how to navigate legitimate sites, avoid dangerous ones, and identify when those with whom we interact online are not to be trusted is essential to staying safe.

This unit will explore potential exploitation via the internet, how to spot danger, and how to safely enjoy technology.

A person's cognitive age is not always the same as their chronological age. However, while everybody and each body is different, people with intellectual and developmental disabilities physically mature at the same rate as people without disabilities, and should therefore receive age-appropriate sex health information. This curriculum is intended for *all* transition students ages 14-21.

This lesson discusses predators and sexual violence. While it is important for your student to recognize danger and identify risks on the internet, you may skip portions that may not apply, such as online dating. Simply move on to the following section.

Note to caregivers/teachers:

Studies have found...

- 12% of people on the Internet have experienced some form of harassment.
- 59% of US teens have been cyberbullied or threatened online.
- One in seven children is contacted online by someone with sexual intentions.
- Children are likely to have seen pornographic content online by the age of 15.
- 40% of teens would behave differently if their parents tracked their online activity.

It is more important than ever to get involved in what our children and students are doing online.

So, be sure to go online together and practice safe navigating.
Find safe websites and talk about why they are safe.
Locate appropriate social media sites and help get them started.
Adjust settings to protect their identity and activity.

We will discuss all of these approaches - and walk you through getting them done! - in this lesson.

Let's get surfing...

The Arc of New Jersey

"Regarding sex education: no secrets!" - Albert Einstein

According to the Public Library of Science, comprehensive sex education helps students "feel more informed, make safer choices, and have healthier outcomes."
This is exactly what we want!
Our purpose is to guide you through a comprehensive and accurate home-based sex education curriculum, ensuring that you have all the information you need to teach effectively.

For Parent/Caregiver/Teacher to **read to yourself**:
You may be uncomfortable with some of this material, and that's okay. Our kit is designed so that if any of the topics is in conflict with your religious or moral beliefs, you may simply skip over those parts and pick up at a place at which you are more comfortable. You may also want to adapt or adjust certain lessons, and that's okay too.

As for the parts that are simply embarrassing, uncomfortable, or feel icky, we ask you to keep pushing through! It is important that your student/loved one gain all the knowledge they need to make safe, healthy, informed decisions as they become more independent. And that means, well, talking about stuff that we don't feel great talking about.
Just remember: The more you talk about it, the easier it gets.

For Parent/Caregiver/Teacher to **read aloud before each session**:
We are going to talk openly here, ask questions, and allow each other to express ourselves without judgement. There are no silly questions and no wrong feelings. This is a safe space. This is a learning space. If you hear something that you do not understand or that upsets you, please speak up. You can take breaks or leave the room for a while if you need to. We are going to learn together.

This unit is about INTERNET SAFETY.
Let's learn how to protect ourselves on our phone, our tablet, and on the internet!
Topics will include:
Trustworthy v. untrustworthy sites
Making friends online
Cyberbullying
Online sexual risk
If any of these topics is a trigger for anxiety or negative feelings, please speak up so we can skip those areas or talk through what bothers you.

The Arc of New Jersey

You will need:
- Pen or pencil
- Computer, laptop or smartphone
- Worksheets 28, 72, 74 - 87d

Learning objectives for this lesson:

- Distinguishing legitimate from illegitimate websites
- Understanding that the internet can be unsafe
- Protecting personal information and passwords
- Developing social "netiquette"
- Identifying and escaping cyberbullying
- Creating safe friendships in chatrooms and dating sites
- Recognizing online grooming techniques
- Understanding how to respond to online risk

You may read this lesson as it is written or use your own words.
And because everyone's abilities are different, you may choose to skip some worksheets.

NOTE TO TEACHERS

It seems almost impossible to live in this world without interacting with the internet, whether for looking for information, finding resources, or connecting with other people.

But learning how to use this technology in a safe way - keeping our information and images private and avoiding sexual violence - is so important to our health and security.

You may want to begin by *blocking pornography* on your student's phone, tablet, and computer. For those with a smartphone, simply open the camera, hold it up to the QR code (as if taking a picture), and tap the link that pops up to find out how to proceed. If the link does not pop up, try moving your camera closer or father from the QR code. For those using a computer, go to https://www.commonsensemedia.org/articles/how-to-block-pornography-on-your-childs-devices.

Section 1: Personal v. public

There is a reason that internet use has become so ingrained in our lives.
It is an amazing tool for finding out information, helping us do our work, fighting isolation, and making new friends or keeping in touch with old ones.

The Arc of New Jersey

Going online is also a great way to build independence and have meaningful experiences, even if there may wind up being negative consequences from these actions (some call it the "dignity of risk"). Chatrooms, social media, and dating sites are places where we can try new things and expand our world.
However, it is important to understand some sites and the people who visit them can be dangerous, as there is no way to tell if someone on the internet is truly who they say they are, and whether their intentions are good.
Therefore, we must learn how to be responsible and stay safe, so caregivers, teachers, and students can be confident and feel secure.

There are a few truths (to know before starting activity on the internet.
Knowing these will help us understand how to behave in a safe and responsible way.

TRUTH: THE INTERNET IS FOREVER

Have you ever said something to someone and wished you could take it back?
Has anyone ever seen you do something embarrassing and you wish they would forget it?
This is what it is like when we post something on the internet.

It is extremely difficult to take down something we have put up on the web.
Any picture you post can be sent to other people, screenshot (when someone takes a picture of the computer or phone screen), or uploaded to other sites - and you may not even know it!

Once you put something online, there is no way to tell who will see it.

So, a good rule to follow is:
IF YOU WOULDN'T WANT YOUR GRANDFATHER TO SEE IT, DON'T POST IT!
(Or your teacher, your brother, your neighbor, etc.)

Take out **WORKSHEET 74, "What Happens on the Internet, Stays on the Internet."** Hang this by your computer to always remind yourself that anything you post is probably going to stay there forever.
Then, don't post anything that should be private!

TRUTH: STRANGERS ON THE INTERNET ARE STILL STRANGERS

When we meet someone on the internet, we sometimes become very friendly.
We share stories, laugh together, talk about our dreams and our fears.
Just like friends. Like *really good* friends.

The Arc of New Jersey

But the fact is, the stranger we meet online is still a stranger, and there is no way to tell if they are who they say they are. Even if they are really, really, really convincing.
Even if they become the person you feel closest to.
Even if they send you a picture of themselves.

Take out **WORKSHEET 75, "Strangers on the Internet are Still Strangers."** Look at each picture and circle the description below it that seems true. Cross out the description that seems false. What makes you think that? Discuss why you think getting a picture of them is not good enough to prove who they are.

Sit back-to-back or go into different rooms where you cannot see each other. Take turns trying to convince each other that you are someone other than yourself.
"I'm a 56 year-old astronaut!"
"I'm a little girl who needs a ride to school."
Get really creative with how to convince each other - do you change your voice, include details that make it sound real, take a picture of someone in a magazine and text it to the other person as if it were a picture of you? Pretending to be someone else helps us understand how easy it is to trick another person - which also helps us not to believe people we talk to on the internet!

Because we cannot know that the person we are talking to is actually someone we want to know (and may be a person we definitely do not want to know!), if anyone makes you feel uncomfortable, stop talking to them! And never, ever meet someone in person who you have met on the internet (unless you go through this whole lesson first - we'll let you know how to meet someone safely!).

And like others can trick us, we should never *impersonate* someone else, either.

IMPERSONATION is pretending to be another person for the purpose of entertainment or fraud (lying to someone to get something from them).

The best advice is to be yourself, enjoy interacting with others, but do not trust anyone with anything private (again, more on this later!).

The Arc of New Jersey

TRUTH: PERSONAL INFORMATION SHOULD BE KEPT PRIVATE

We all want to make great posts - ones that get us lots of "likes."
But we should always make sure that our fabulous, interesting, most-liked posts keep us safe!

Just like private places are those where no one else can see or hear you (where you can be alone), *private information* is just for you, too!

PRIVATE, or PERSONAL INFORMATION is facts that are specifically about you.

This kind of information lets others know very important - but private - details about your life. Because we cannot really know the strangers we meet on the internet (remember, fake pictures! Fake facts!), we do not want them to know things about us that could help them find us, come meet us, or steal our money or belongings.

Private, or personal, information includes:

- Your last name
- Your home address
- Where you work
- The name of your town
- The name of your school
- The name of your school mascot (go, Tigers!)
- Your phone number
- Your bank information
- Your credit card information
- Your travel plans (which would let them know when the house will be empty)
- Your social security or government ID number
- Your passwords
- Your social media page, like Facebook, Instagram, and other platforms (they could use social media to find out information about you)
- Your email address

A great way to go about this is to use a nickname ("Hi, I'm Skippy!", “The name’s ‘Red!’”) and to say you are from a town or city near you, rather than your real information.

We can still share our hopes and dreams and thoughts and jokes!
Want to be a scientist? That's ok to tell them! But saying you are a 12th-grader at Jones School in Cityville who wants to be a scientist? That’s too much (private) information!

The Arc of New Jersey

Take out **WORKSHEET 76, "What is Personal Information?"** Use this as a reference before you post anything! If you go over the list but are still unsure of whether you can post something on the internet, check with a trusted adult first!

Take out **WORKSHEET 77, "Keeping Personal Information Private."** Look at each picture and draw a circle around anything you see that gives away personal information. How can posting that information be dangerous? Discuss!

TRUTH: PASSWORDS ARE PRIVATE!

One thing we should never tell anyone else is any of our passwords!
If someone else knows them, they can go into our account, find out information, or even impersonate us and post something we do not want posted!

Keeping passwords private are a great way to stay safe, and they should also be hard to guess!

Come up with a password that includes a mix of uppercase letters, lowercase letters, symbols, and numbers. Maybe something like "iLoveTh3ArCofNew!Jersey" or "St@ySaf3UndErThe=Arc."

Write it down and put it somewhere private and safe, like in a drawer or under your bed, so you can remind yourself if you forget it!

It is also a good idea to change these passwords every so often, to use different passwords for different sites, and to log out every time you leave your computer (especially if you use it in a public place, like school or the library).

It sounds like a lot of work, but staying safe is worth it!

Section 2: Trustworthy v. untrustworthy sites

Let's say we do everything right: we do not give out personal or private information, we do not send pictures or post anything we would not want our grandfather to see, and we keep our passwords private and hard to guess. We still need to carefully choose the websites we visit!

There are a few ways to make sure a site is *trustworthy*.

TRUSTWORTHY means being able to be relied on to be safe.

Some websites try to take or sell our information, get us to buy things we don't really want or can't afford, or give our computers viruses (which break them).

The Arc of New Jersey

Luckily, there are ways to protect ourselves.

Follow along on your computer, tablet, or smart phone throughout this lesson. It will make the information much clearer if you are looking at it!

Check for the "S."

When we look at the address bar that runs across the top of the browser on a website, we find the URL address (for instance, The Arc of NJ's URL address is "https://www.arcnj.org.")
Look to make sure that the address begins with "https," not "http."
If there is no "https" nor "http," look for a little padlock icon at the far left.
Both the "s" and the padlock icon are there to let you know that the site is secure and that no one can access your information.

Check for spelling.

A fraudulent, or fake, URL address is sometimes a misspelled version of a real URL address.
For instance, www.hellothere.com might be misspelled www.hellotheir.com or www.helothere.com.
These sites do this so that common misspellings will direct users to their site instead of the one the person is really trying to access.
Always make sure that you have properly spelled your website address before hitting "enter!"
And never go to a website that has been emailed to you if that email is poorly worded or misspelled.

Google it!

Google lists their search results in order of popularity - the ones that are used most often will appear first.
If you search a website in Google and do not see it within the first page or two, think about not visiting the site. It may not be secure.

Check for signs of realness.

Sometimes, fake websites will send emails asking us to go to their site.
But first check the website for a "contact us" or "about us" page.
Are people listed?
Is there a physical address or phone number?
Call the number from the “contact us” page of the website (not from emails from the company) and ask if they really sent an email.
If not, do not click through.

The Arc of New Jersey

Don't click hyperlinks.
If we do get an email with a hyperlink to a website (which we can just click on to be brought right to that page), do not click the link, but type the URL address directly into the address bar in a new tab. Even if it is sent by someone trustworthy, the link itself might be unsafe.

When it comes to news, consider the source.
Many sites like to publish "news" that seems unbelievable - and that's usually because it should not be believed (some news *is* fake news)! When reading up on current events or researching for school, make sure you get your information from trustworthy sources. Look for popular news sites like big city newspapers, news sources like the Associated Press and Reuters, and unbiased sources like PBS. And if it sounds ridiculous, it probably is!

Listen to your gut.
Does an offer seem too good to be true? ("A new car for $50? What a deal!")
Does the website look strange?
Are they asking for personal information?
If your intuition is telling you it's not safe, believe it! (Remember, we have a gut for a reason.)

Take out **WORKSHEET 78, "Trustworthy v. Untrustworthy Sites."** Look at each example and see if you can spot anything that might make the site untrustworthy. Discuss why or why not! If you are not sure, how would you decide whether or not to visit the site?

One great resource for figuring out if a website is trustworthy or not is the **Google Transparency Report** (https://transparencyreport.google.com/safe-browsing/search?url=https:%2F%2Fwww.smartone.com%2Ftc%2Fhome%2F). You can type in the link or scan this QR code (we are a trustworthy source!) to check it out.

Emails, texts, and messages on social media also need to be checked for trustworthiness.

- Never reply to a text from someone not in your contact list.
- Never reply when someone tries to coerce, threaten, or bribe you - for anything.
- Never reply to something sexual, like offering nude pictures or asking you for them.
- Do not reply if someone says they are a celebrity. Celebrities do not reach out to people they don't know!

The Arc of New Jersey

Section 3: Netiquette and staying safe

You might be wondering, "What is that crazy word I just read??"
Although it once was a made-up word, it is now in the dictionary.
Let's start with the root of the word:

ETIQUETTE (pronounced ET-i-ket) is polite behavior among others.

NETIQUETTE is polite behavior among others on the internet!

Although we are not interacting with others in person, talking to people online also comes with rules and responsibilities for remaining appropriate (having acceptable behavior) with others.

For instance, when posting, it is important to think first... or T.H.I.N.K. first.

Take out **WORKSHEET 79, "T.H.I.N.K. Before You Post."**
Read the actions that we should take before we post.
We must ask ourselves, "Is what I am about to post true?" "Is it helpful?" "Is it inspiring (exciting to people)?" "Is it necessary (do I have to post this)?" And "Is it kind?"
This helps us figure out if what we are posting is going to hurt anyone else or make people angry at us.
T.H.I.N.K.-ing first is a great way to ensure that we do not put something online that we will regret later (remember: the internet is forever!).
If it isn't right to say, then it isn't right to post.
Hang this near your computer to remind you to T.H.I.N.K!

Using proper netiquette is important for both behaving appropriately online and staying safe.

Remaining appropriate:

- Follow the same rules of online behavior as you do with in-person behavior. If you wouldn't say something to someone's face, do not say it online!
- Give people space. We sometimes feel eager to hear from others, but enthusiasm can turn to harassment very easily.

HARASSMENT is aggressive behavior or bullying. If we continue to bother someone to write to us or call us back, they can feel like we are harassing them.

The Arc of New Jersey

To make sure that we do not harass someone, follow the 3x3 rule: if the person has not responded after 3 attempts to contact them in one day by texting/calling/messaging, do not send another message. You may try again the following day but you may only do this for 3 days. Then you may not attempt to contact the person again.

However, if they have let us know that they don't want us to contact them at all - for whatever reason - we must respect that and stop reaching out.

Sound familiar?
It is the other person setting *boundaries* and our accepting *non-consent*! (Yes, even online!)

We must also let others know our boundaries, and give our consent or non-consent to be contacted. (Continuing to contact someone after they have asked us to stop is sometimes considered a crime! Let them know when you would like them to stop!)

This is how communication helps us - and others - stay safe on the internet. Being aware of how we and they feel helps us identify appropriate behavior.

Staying safe:

- Remember to keep passwords and personal information private.
- Black out personal information that may be in a picture or screenshot.
- Make your accounts private.

Section 4: Making friends online ★

We know that being kind, friendly, open, interested, and a good listener will help us make friends in person and online. (Basically behaving the way we would want a friend to behave with us!)

But the internet has extra challenges. How do we know where to find people we will like?
How do we know that the people we find will like us?

One good approach is to choose platforms and communities that you care about. Think about your interests, what matters to you (values), and activities you might want to learn about.
Not only will you find people and topics you know interest you, but the enthusiasm you bring will make them feel good, too!

Feel free to compliment ("I loved the ravioli recipe you posted! Is there a vegan option?") but don't compliment too much (it seems insincere), and think twice about criticizing others.

The Arc of New Jersey

And if someone does not take steps to be friendly to you, move on. There is a whole world out there!

Take out **WORKSHEET 28, "The Rejection Files,"** again. Look at the two columns on the right side of the page which explain appropriate behavior when we are rejected. All of these guidelines apply online, too!
Don't say unkind things, harass, take it personally (you are a great person!), or get discouraged. This is just one of many, many people you will meet.
Now look at the two columns on the left side of the page. Ignore these.
Why? Because you do not have to say anything - in fact, it is better if you do not. If someone expresses a desire to be left alone, if they ignore your posts or comments, or if they are nasty for some reason, *stop talking to them*.
It's just another great excuse to move forward with others!

It is just as important to recognize who *you* want to be friends with as it is to figure out how to be a friend. People who are kind, share our interests, and want to get to know us are all great qualities. But there are some people out there who take advantage of the fact that we cannot see them, and they may try to convince us that they are someone they are not... sometimes to cause harm.
So, we want to look out for signs of *cyber predators*.

CYBER PREDATORS are people who gain the trust of people online and use them for money and other gains. They often try to get their online "friends" to send them things or meet them in person.

Take out **WORKSHEET 80, "How to Spot a Cyber Predator."** Look over the clues that someone may not be who they say they are. Review these often (remember, *repetition helps us remember things!*) and hang it somewhere close to your computer!

One of the biggest "red flags" (things to watch out for) of a cyber predator is telling you to keep the friendship - and what they talk about, try to get from you, and ask you to do - a secret.

If a conversation has to be kept a secret, it means it is a bad thing (because don't we love telling everyone about good things?).
So, if someone ever asks you not to tell your caregiver about something, that is a sure sign that you should tell your caregiver immediately!

The Arc of New Jersey

We should also never (say it with me: never, ever, ever, no way, nope, NEVER) send anyone money or credit card/bank information. Even if we think they are our best online friend in the world.
Even if they tell us that they are stuck in another country and need money to fly back home.
Even if they say that they will go to prison without it!
Even if they say they love you.
If you still want to send money after all that (but NEVER credit card/bank information), you must discuss it with your caregiver or a trusted adult first.
Sometimes others can see what we cannot.
Getting another opinion may save you from losing all of your money.

Take out **WORKSHEET 81, "Making Friends Online."**
Draw a line from descriptions of what a safe person would do to the picture in the center.
Cross out those things that describe what an unsafe person would do.
Discuss why you believe you should or shouldn't trust a person with each behavior. Why do you think a person would do these things?

Let's look at some examples of what a real friend sounds like, and what a cyber predator might sound like.

Example #1 - The Flatterer

Kia was so excited to post pictures of her birthday party to her social media; she had gotten a new blue dress and put crystals on her hearing aids, and she wanted all of her online friends to see it.
Two minutes after posting, Tata commented, "You are gorgeous!" with a fire emoji 🔥 next to it.
Kia felt great and thanked Tata for his post. Tata responded, "You got it, Beautiful."

Example #1 - The Flatterer, a different way

Kia was so excited to post pictures of her birthday party to her social media; she had gotten a new blue dress and put crystals on her hearing aids, and she wanted all of her online friends to see it.
Two minutes after posting, Tata commented, "You are gorgeous!" with a fire emoji 🔥 next to it.
Kia felt great and thanked Tata for his post. Tata responded, "You got it, Beautiful. Got any pics without the dress? It's just that you are the prettiest girl I've ever seen and I want to see all of you."

In which example is Tata a cyber predator? What makes you think so?
How should Kia respond? Discuss the best ways to handle this.

The Arc of New Jersey

Example #2 - The Curious Person

Ren had met a new friend in a pickleball chatroom. Their name was Morgan, and they knew everything about the sport, so Ren asked them many questions and learned a lot. Morgan wrote that they wanted to learn more about Ren! "Where do you live?" they asked. Ren replied, "I'm right outside of Trenton." "But, like, where?" asked Morgan, "You have to live on a street. What's the name of it?" Ren wrote, "I don't really want to tell you." "Come on," wrote Morgan, "Don't be a baby. What, are you afraid? Just tell me where you live!" After two minutes of not hearing back, Morgan wrote again. "Don't ignore me, you jerk!"

Example #2 - The Curious Person, a different way

Ren had met a new friend in a pickleball chatroom. Their name was Morgan, and they knew everything about the sport, so Ren asked them many questions and learned a lot. Morgan wrote that they wanted to learn more about Ren! "Where do you live?" they asked. Ren replied, "I'm right outside of Trenton." "Cool," wrote Morgan, "I'm closer to the shore. Do you get into the city a lot?" Ren said he did. "I would love that," Morgan replied, "I'm tired of always having sand in our rugs!"

In which example is Morgan a cyber predator? What makes you think so?
How should Ren respond? Discuss the best ways to handle this.

Example #3 - The Link Sender

Jamie was playing on a gaming app with his new friend, Nita. They had spent the past three weeks gaming every day, chatting the whole time like they had known each other for years. Suddenly, Jamie's phone pinged and a message appeared from a number he had never seen before; the message was just a link. Nita said, "Hey, I just sent you a link to another gaming site. It's really cool." Jamie said, "I'm just going to type this into my laptop and see what comes up." "Totally," replied Nita, "you don't want to get a virus. Sorry I didn't just tell you about it. You did the right thing."

Example #3 - The Link Sender, a different way

Jamie was playing on a gaming app with his new friend, Nita. They had spent the past three weeks gaming every day, chatting the whole time like they had known each other for years. Suddenly, Jamie's phone pinged and a message appeared from a number he had never seen before; the message was just a link. Nita said, "Hey, I just sent you a link to another gaming site. It's really cool. Just click it and put in your credit card number. And don't go telling anyone, ok? They wouldn't understand."

The Arc of New Jersey

In which example is Nita a cyber predator? What makes you think so?
How should Jamie respond? Discuss the best ways to handle this.

Take turns pretending to be a new person in an online community; sometimes be yourself, sometimes act like a cyber predator. What is different about the way you behave as each character? How easy it is to spot when your partner is the cyber predator?

Some people we meet online will not be cyber predators - they will be good people who become our friends, and we may want to see them in person at some point.

This is great! (The only thing better than a friend is a friend-who-can-split-a-brownie-sundae with us!) But before you head out to meet them, there are some precautions you should take:

1. Check with your caregiver before agreeing to plans. It doesn't matter how good our judgment is, a second opinion is important.
2. FaceTime or Skype first. This way, you can make sure that the person is who they say they are before you meet them in person.
3. Let at least one other person know where you will be. Better yet, share your location from your phone (for iPhone users, open a message to the contact you want to share your location with; click on their picture/circle at the top of the conversation; click "Share My Location.")
4. Meet in public! Never go to their home or meet them in a private place where others cannot see or hear you until you have spent a lot of time together in person. And do not ask them to your house - we do not want people we met on the internet to know where we live! A populated park or nearby coffee shop is a good way to safely begin an in-person friendship.
5. Bring someone else along. Introduce a friend, family member, or someone you trust to this new friend, or just ask a trusted adult to sit away from you in the diner, coffee shop, park, etc. and keep an eye on you.
6. Do not accept a ride from this person - meet them there. We should never take rides from strangers, and strangers we meet on the internet are still strangers!

There are some great websites for making friends, such as:

Hello, It's Me (https://hello-itsme.com/),
specifically for people with intellectual disabilities.

The Arc of New Jersey

Section 5: Social media ★

Social networking has become one of the most popular activities in the world, and it doesn't seem to be going anywhere soon!

Sharing photos and stories of your life, getting a peek into what others have been up to, and staying in touch are great reasons to use social media.

But it comes with its own specific netiquette, and learning how to interact on these platforms will help us make friends and keep them.

1. Be careful who you "friend." Do not add strangers who request to follow you, as they may not be who they say they are. If you believe you might know the person, look at their profile before accepting their request and see how many other people are following them (and if you know any of these friends). If they have very few contacts, it may mean that they create fake profiles just to find people to take advantage of.
2. Do not follow teachers or bosses - it is definitely inappropriate! (Remember our lesson on relationships? Even if we really like them, teachers, bosses, and helpers are not our friends.)
3. Do not accept friend requests from people who say they are famous. Remember, famous people do not just reach out to people they don't know. Celebrity profiles have blue "verified" check marks ✔ next to their name; no check mark, not famous!
4. Do not criticize or say mean things about specific people, politics, or work/school (remember, the internet is forever, so once you put it out there, you can't take it back). And when it comes to the internet, you never know who will read it or how they will react!
5. Do not believe everything you read and see on social media - people tend to post only the best moments, leave out the disappointing ones, and change photos to make themselves look happy and fabulous. What we see is rarely the truth. The same goes for reading posts - just because someone posts information, doesn't mean it is true. We call this "fake news" and should ignore it!
6. Do not click on ads for items that you want to buy (and if you really want to buy it, run it by your caregiver first!). Many ads we find online are just *scams*.

SCAMS are dishonest or illegal plans or activities. They often seem too good to be true... because they are. They usually charge more money than they say they will, or won't deliver your items once you have bought them. Let someone else take a look at something you want to buy, a "giveaway" (something free), or an opportunity that interests you *before* you click the link to avoid getting scammed.

The Arc of New Jersey

7. Sometimes we will run across a fun game that pops up, like a quiz - say, "Which TV Character Are You Most Like?" or "What Color is Your Personality?" These may seem safe, but they are usually just ways of exploiting people who want to have fun. They get you to enter your name and other information, then sell that information to other companies. Keep your personal information private!
8. Remember to T.H.I.N.K. before you post! Maybe even let someone you trust look over your post before you put it on your page. They may spot something you missed.

Even if someone we meet online is not a cyber predator, they may still make us uncomfortable with what they post or how they respond to our posts.
In that case, we can always block someone we do not want to have access to our social media.
To prevent this, make all social media private (we choose exactly who gets to see it)! Here's how...

Making Facebook private:

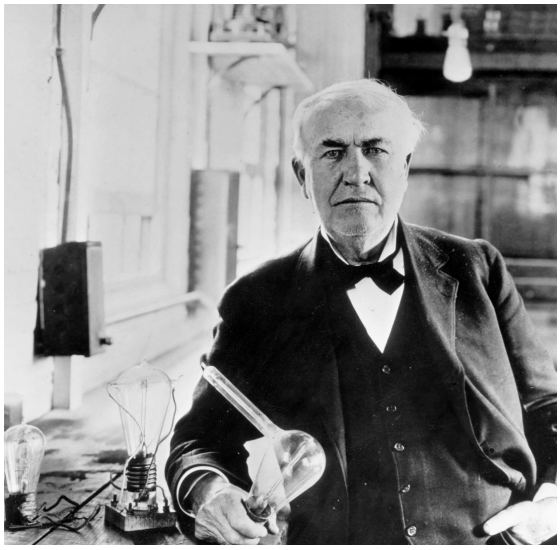
Open Facebook on your computer, laptop, tablet, or phone.
Open the Account Settings, then follow the path Settings & Privacy > Settings > Privacy.
Under Your Activity, find Who Can See Your Future Posts, and select Edit.
Set it to Friends or Only me.
Next select Profile and Tagging from the panel on the left side of your screen. Here you can control who posts messages to your timeline, and who can see what you and other users post on your timeline.
Then move on to the Blocking section from the panel on the left. Here you can completely deny access to your profile for certain users by putting them into the Block users list. Alternatively, you can put them into the Restricted list and restrict their access and allow them to only see the public posts and public information on your profile.
When you're finished tweaking your privacy settings on Facebook, go back to the Profile and Tagging section. Scroll down and select View as to see what your profile looks like to other users who aren't on your Facebook friends list.

Making Instagram private:

Open Instagram and go to your profile page.
Select the three horizontal lines in the upper-right corner of the screen to open the Menu.
Select Settings.
From the Settings menu, select Privacy.
Under Account privacy, toggle the Private account switch on.

The Arc of New Jersey

Spotlight



Mondadori Portfolio/Mondadori via Getty Images

Thomas Edison was a New Jersey inventor who brought us one of the world's greatest technological creations yet: the lightbulb! He achieved this amazing feat as a person with dyslexia and ADHD. Edison understood how **technology** brings people together, so he also invented the phonograph (record player) and motion picture camera. The next time you enjoy music or a movie, know that it is thanks to a determined person with a developmental disability!

Making Snapchat private:

Open Snapchat and navigate to your profile page.
Select the icon ⚙ in the upper-right corner of the screen to open your account settings.
Scroll down until you see the Manage Who Can section.
Select Manage Who Can Contact Me and set it to My Friends instead of Everyone.
Then go back, select Manage Who Can View My Story, and set it to Friends Only or Custom if you want to handpick who's allowed to see your Snapchat Stories.

Finally, if your social media platform ever requests to access your location, do not accept! And never "check in" to let everyone know where you are - that is personal information!

Section 6: Chatrooms and gaming sites ★

Many people use social media as a way of interacting with friends, but others prefer chatrooms, which are less about photo-, story-, and interest-sharing, and more about conversation. These rooms allow users to "talk" (text) in real time, much like instant messaging. It is a great way to interact with others without having to wait for them to check their posts.

Gaming apps are another resource for spending time with others, where multiple participants play games against each other and have texted or spoken conversations at the same time. Some consider them advanced kinds of chatroom, just with a build-in activity.

These are great tools for getting to know others without the pressure of in-person interaction. Be yourself and have fun! But as we chat with new friends and battle zombies in virtual reality, we also have to keep an eye out for safety (fun + safety = a great online experience!).

The Arc of New Jersey

- Be cautious of people who immediately want to chat privately with you as soon as you enter the room.
- Look out for people who want to talk about very personal subjects with you, like details about disabilities and medical issues, and will not get off the subject. They may well be cyber predators who are trying to find people to *exploit*.

EXPLOITATION (the act of exploiting) is using someone or something in a way that helps you; taking unfair advantage. Someone may exploit a hungry person by making them pay extra money for something to eat. Someone may exploit a person who needs a job by making them work long hours for little pay.

- Be aware of people who go out of their way to make you feel sorry for them. Do not let people exploit your sympathy.
- Do not trust people who suddenly ask you if you have a picture or webcam, or ask for your Facebook, Skype, or Yahoo messenger information. They may seem like a good friend who is interested in learning more about you, but they could well be cyber predators. To be safe, we should never send personal information to anyone we have met online. Remember: strangers on the internet are still strangers!

Take out **WORKSHEETS 82a, 82b, and 82c, "Safe or Dangerous?"** First, cut out all the green check marks and red X's, then all of the blue cards on the two pages. Lay them all out, face up.
Place a green check mark over all of the posts and messages that you believe are safe.
Why do you think this?
Place a red X over all of the posts and messages that you believe could be dangerous, or unsafe.
Why do you believe that?
Fill in your own examples on the blank cards and place either a green check mark or red X over it.
Discuss your choice!

One chatroom was created by people with disabilities, for people with disabilities. Check it out!

Disabilities-R-Us (https://www.disabilities-r-us.com/)

The Arc of New Jersey

Section 7: Dating sites ★

Dating sites and apps have been popular for the last 10 years, and singles love them for many reasons. First, you can learn a lot about a person before you even speak to them; second, you can see their picture, which lets you know even more about them (look, they have a pet snake! They are climbing a mountain in their wheelchair!); finally, you can meet and interact with someone from the comfort of home.

Some sites/apps are designed for people looking for true love, while others are good for meeting lots of people whom you may or may not want to date. Either way, dating apps are here to stay.

There are certain things to look for when choosing a dating site or app:

1. Is it safe? A dating site/app should have features that allow you to report inappropriate or dangerous behavior, as well as ways to block people we do not want contacting us. You may want to report or block a user if they:
   a. Request financial assistance
   b. Request photographs
   c. Are a minor
   d. Send harassing or offensive messages
   e. Attempt to threaten or intimidate you in any way
   f. Seem to have created a fake profile
   g. Try to sell you products or services
2. Do many people use it? If a dating site/app is popular, it means something is working! Plus, the more popular it is, the more people available to meet!
3. Do you want a site/app specifically for people with disabilities or for every kind of person? It all depends on your comfort level and what you are looking for. We want to find people who have something in common with us, but that does not have to mean a disability - it can mean a love of cooking or an allergy to pollen! The choice is yours.
4. Do you want a site/app that is free to use or one that costs money? Some people prefer ones that require payment, because that means those who use it are serious about finding love! Either way, let a trusted adult help you figure out if a paid site is worth the money or if it's a scam!
5. Most sites/apps work for people of any sexual orientation - LGBTQ+ or heterosexual. Make sure there is a large enough community for what you want!
6. You may want to become a member on a couple of sites, not just one. This will allow you to view and be viewed by even more people. But don't join too many - it will get hard to remember from where and how you know somebody and, if they are paid sites, it can get expensive.

The Arc of New Jersey

Before you venture online, it is a good idea to know what you are looking for. What kind of person do you want to meet? How will you know if you should write to them?

A good way to figure this out is to think about your relationship values.
Remember values? They are the things we care about that guide our attitudes and actions; the reasons we choose to do the things we do.

Relationship values are the things we care about that we look for in a partner.
It is like a checklist of the things we want and need in another person.

Take out **WORKSHEET 83, "Relationship Values."** Look over the list of qualities, or things you value in a person you would want to date. Circle the things that matter to you. Then ask yourself, "Why do I care about these things? Which would I be willing to give up, and which do I require?" Then look at the list on the right - check out the different ways you can find out if a person you are talking to has the qualities you want and need!

Once we have figured out what we are looking for (or at least have a better idea of what we want), we can then choose our dating apps and create a *profile*!

A PROFILE is a written introduction to who you are. It helps others understand our likes and dislikes, how we choose to live, and what we want from life.

When writing a dating profile, show your personality!
Write about your passions, your hobbies, and your idea of a perfect date.
Include goals you are working toward, like learning how to paint or planning a trip to Italy.
Concentrate on your good traits and what excites you - being negative might make people not want to interact with you.
Most important, be honest - about what interests you, what you are looking for, and a mention of your disability. Show them who you really are! There is a lot there to love about you!

Most dating sites also ask you to post a picture or two, so people can see who you are.
A good idea is to post one picture that really shows off your face, and one a little farther away.
Maybe include things that are meaningful to you, like a photo of you with your dog or icing a cake you just baked! Although you want to show your best self (choose a picture you are proud of), there is no need to look glamorous; just choose one that shows beautiful YOU.

The Arc of New Jersey

Take out **WORKSHEET 84, "My Dating Profile."** Look at the pictures on the "computer screen" and circle the ones that would be good to use on a dating site. Why did you choose the ones you did? Look on the left side of the page and circle the phrases you think would be good to include in your profile. Why do you think those are better than the others? Finally, look on the right side of the page and circle the comments you think would be good to write on someone else's profile. Why are these better than the others?

Once you have completed your profile, you may begin hearing from people who want to get to know you. Enjoy meeting new people safely and in a way that honors your values.

1. Some people might not be what you expected. Or the kind of person you want to know. That's ok - ignore them and keep moving forward. You should not respond to people who are unkind or make you feel uncomfortable - delete them and keep going!
2. Be careful of people who come on "too strong" - these are people who give too many compliments, say you are what they have been looking for, and tell you that they love you way too soon. Cyber predators like to make people feel good before they exploit them (take advantage of others for their own gain). Many people will say nice things to you (I mean, those pictures you chose were perfect!), but if it sounds right out of a fairy tale, it is probably not real.
3. You may reach out to someone who does not want to get to know you. Or you will begin to get to know a person and they will suddenly stop responding to you, or tell you that they are no longer interested. Again, that's ok! We are all there to learn about each other, and no one person is perfect for everyone. So take out your Rejection Files (Worksheet 27) and read it over and over! This is how you want to behave when rejecting people and being rejected by others. It is not personal - we just all have our own relationship values.

You can either both get on computers, tablets, or your phones, or else sit back-to-back. Take turns rejecting each other via text, chat, or verbally (follow the Rejection Files guidelines!) and accepting rejection. The more you do it, the easier it gets (remember: *repetition helps us remember things!*)

4. At some point, one of you may decide that you want to meet someone in person. If the other person wants to meet but you are not ready, then do not do it! You have your boundaries and if you do not want to go, then you should not consent. It's ok. Anyone who is worth meeting will wait until you are ready.

The Arc of New Jersey

If you do decide you want to meet, make sure to follow the guidelines for visiting with people you have met on the internet (p.14). That includes getting your own transportation (never get in their car, don't let them know where you live!), meeting someplace public, maybe bringing along a friend or family member to sit in the room, and letting others know where you will be. You may be developing a relationship with each other, but until you really know each other, strangers on the internet are still strangers!

5. Don't forget to take care of YOU. It is so much fun meeting people and seeing if you are romantically interested, but don't ignore the other things you love. Take time for yourself, your family, and your friends. Get your work and chores done. And enjoy your time away from the dating site. It is only one part of your life, and it should not take away from the other parts.
6. FINALLY: REMAIN AWARE OF SEXUAL RISK.
   Remember when we talked about recognizing sexual risk? Here is a reminder:

   1. They don't stop when you give your assertive non-consent. (If you communicate "no," they should stop!)
   2. They tell you to keep your relationship a secret. (When someone tells you not to tell your caregiver or a trusted adult, that means they are doing something wrong and you should tell your caregiver or trusted adult.)
   3. You find yourself doing something sexual that you don't want to do. (That means you have not given your consent - and not giving consent is the same as giving non-consent.)
   4. What you are doing feels wrong.

The best way to protect ourselves, however, is to trust our gut!

Take out **WORKSHEET 72, "Trusting Our Gut,"** again. Review what it means to trust your gut - how it feels in your body, the emotions you experience, and what your intuition is telling you. We know when something feels wrong - trust that!

There are several good dating sites to try - some for people with disabilities, some inclusive of everybody. We make no promises that they will all work for you, but they all have safety features, are popular, and look exciting! Use your good judgment and be cautious while exploring. If interested, scan the QR codes below to visit some sites, or type in the URL address yourself.

The Arc of New Jersey

Dating4Disabled (https://www.dating4disabled.com/)

Special Bridge (https://www.specialbridge.com/)

Hiki (https://www.hikiapp.com/)

Section 8: Cyberbullying ★

Because we don't know who people really are when they post on the internet, sometimes they will exploit that fact and *cyberbully* others.

CYBERBULLYING is posting or sharing harmful or mean content about someone else on the internet, social media, apps, texts, video games, or digital devices.

This includes mean comments, profanity, threats to one's safety, sharing nude or inappropriate photos, threatening to share nude or inappropriate photos, spreading rumors, impersonating someone else, and engaging in cruel or hurtful behavior in groups online.

Just like in person, cyberbullying hurts. And in New Jersey, it is a crime.

How do we know if something we see is cyberbullying? It has to do with *intent*.

The Arc of New Jersey

INTENT is something that is planned or done for a purpose, such as to harm or threaten them.

So, sending a friend a funny picture of another friend is not cyberbullying, but posting on social media to embarrass them is cyberbullying.

Take out **WORKSHEET 85, "Is it Cyberbullying?"** Draw a line from each behavior to either "cyberbullying" or "not cyberbullying." Discuss your answers!

How do we handle what we think might be cyberbullying?

- If someone has posted something of us that we do not want online, ask them to take it down. If they did not have bad intent, they will apologize and remove the post immediately.
- If they do not take it down, make sure to take screenshots! Sometimes, people will suddenly remove what they have done if they realize they will get in trouble (and then say they never posted anything bad in the first place). Photos and keeping a list of when and what they have done can be used as proof.
- Always tell a trusted adult when we think we are being cyberbullied. They are there to help protect you!
- If someone posts something mean, embarrassing, or threatening about us, we should block them right away.
- Report any cyberbullying to the site or platform.
- In the case of threats to our health or safety, we should report it to the police. New Jersey has laws against cyberbullying!
- There are also laws against "harassment, intimidation, or bullying that is reasonably perceived as being motivated either by any actual or perceived characteristic," such as a disability. If the mean or embarrassing posts are about our disability, race, or sexual orientation, we should report them to our school district (if we are a student) or to the U.S. Department of Justice Civil Rights Division (https://civilrights.justice.gov/#three).
- To avoid accidentally cyberbullying someone else, always get their permission before posting a photo or writing about them. If they say they do not want you to post, you shouldn't post. (Remember: consent is important, even online!)

Being cyberbullied can feel very upsetting; it is important to talk to caregivers or trusted adults so they know what is going on.
Caregivers and trusted adults should also check in often on how their student is doing. Being aware of their online activity and following them on social media will help you navigate the World Wide Web safely, together!

The Arc of New Jersey

Section 9: Online sexual risk ★

We know about sexual risk when we are in person with someone, but that does not mean that the internet is safe. There are just as many risks for sexual violence online as there are out in the world - and maybe more! That's because people on social media or in chatrooms can pretend to be someone completely different from who they really are.
And other on these sites often open up to others more honestly, because they feel more secure when no one can see them. This may result in giving away personal information.
These factors create a perfect setting for sexual violence in the form of *grooming*.

GROOMING is when someone builds a relationship, trust, and emotional connection with someone else so they can manipulate or abuse them.

Grooming is all about building trust - getting us to talk about our wants, needs, fears, and frustrations, so they can exploit them (take advantage of them for their own gain).

It also involves finding out important details about us to use against us.

The people who do this are usually very good at it - they pretend to be a good friend and sometimes we cannot tell the difference! Anyone can fall prey to a groomer.
(Remember: IT IS NEVER THE VICTIM'S FAULT. EVER.)

Here are examples of what BOTH a friend and a groomer might do:

- Listen to our problems
- Share their problems with us
- Cheer us up when we are down
- Give us compliments
- Ask about our life
- Offer advice
- Reach out often

These behaviors are wonderful when they come from a friend.
And grooming does, at first, seem like real friendship. But that is what makes is so sneaky. Because if we are not on the lookout for grooming techniques, we may not recognize when it is not actually friendship.

When meeting new people online, we want to look out for “red flags,” also known as “warning signs.” These are little clues that let us know that something is not right, and that the person we are speaking to is not to be trusted.

The Arc of New Jersey

Take out **WORKSHEET 86, "Grooming Red Flags."** Look at the list of behaviors and see which ones are warning signs of grooming. Hang this near your internet device to make it easier to remember what to look out for!

Online predators/groomers often look for people who are open-hearted, young, or looking for a connection with someone else. They then take advantage of this trust by isolating the person (distancing them from others), becoming an important person in their life, and making sure that the relationship remains a secret.

- Groomers may compliment you in ways that are extreme - usually about your appearance.
- Groomers may try to have sexual conversations or share sexual messages with you.
- They might send or ask for sexual pictures or videos.
- They might ask you to take part in live streams or video chats that become sexual.
- They can try to pressure or threaten you into selling drugs, hurting other people, or doing something illegal.
- They may try to blackmail you (threaten to tell your secrets or share photos or personal information about you) so you will give them money.
- They may ask you to meet in person or go somewhere with them.
- They will almost always tell you to keep your conversations and the relationship a secret. But, as we know, if someone tells us to keep a secret, that is a clue that we should tell a trusted adult immediately! (Nothing good or safe ever has to be kept secret, right?) They may also advise you not to tell anyone because it would get you into trouble or that no one would believe you. Again, this is not true! It is why we have trusted adults. And if one trusted adult does not happen to believe you, tell another. And another. And another. Keep telling until you get the response you need!
- Groomers will probably try to find out a lot about you: "Tell me about your disability;" "Have you ever had sex?;" "What's your biggest secret?;" "Tell me secrets about your family and friends;" "What is your address?" Do not tell them any of this! It is personal and private.
- They may also tell you a secret to keep between the two of you - this is to make you feel like they trust you. The truth is, the secret might not even be real!
- Some groomers send gifts. It is a way to make you believe they really care about you. But these gifts are not true friendship, they are a way to get you even closer to them.
- If someone you have met online wants to meet you in person - and alone - say no. Wanting to be alone and away from other people is a red flag when it comes to online predators. If the person is really your friend, they will accept your non-consent and not ask you again.

The Arc of New Jersey

Take out **WORKSHEETS 87a, 87b, 87c, and 87d, "From a Groomer or a Friend?"** Read over the message exchanges and figure out if you (in the green talking bubbles) are hearing from a friend or a groomer (in the gray boxes). What makes you think that? If you are not sure if someone is a friend and you sense a red flag, what should you do? Discuss!

If someone we meet or have been getting to know online turns out to have red flags (warning signs), you should STOP TALKING TO THEM RIGHT AWAY.
There is no need for an explanation, no need for a goodbye.
This is because we trust our gut, and when our guts tells us that someone might be dangerous or at least not who they say they are, we need to get away from them.

Then tell a trusted adult, and decide together if you should report the predator/groomer to the platform/app.

And remember to track what has happened - that includes taking screenshots or photos of your interaction online, and taking notes with dates and times.

You may also want to talk about your feelings with your trusted adult, a member of the clergy, a teacher, a doctor, or a therapist. It can feel very bad and a little scary to meet someone online who turns out not to be the friend they say they are. Don't be afraid to be honest about your feelings.

Here are some more helpful tools for internet safety.

Be Internet Awesome
https://beinternetawesome.withgoogle.com/en_us/

Stomp Out Bullying
https://www.stompoutbullying.org/dugital-u

Common Sense Media
https://www.commonsense.org/education

END OF LESSON 4

Be sure to check in with your student about how they feel. Hard topics can bring up emotions like sadness or fear - make sure your student is ok, and talk it through if they are not. Then you can see if they have any questions! Great job!

The Arc of New Jersey

Glossary

CYBER PREDATORS are people who gain the trust of people online and use them for money and other gains.

CYBERBULLYING is posting or sharing harmful or mean content about someone else on the internet, social media, apps, texts, video games, or digital devices.

ETIQUETTE (pronounced ET-i-ket) is polite behavior among others.

EXPLOITATION (the act of exploiting) is using someone or something in a way that helps you; taking unfair advantage.

GROOMING is when someone builds a relationship, trust, and emotional connection with someone else so they can manipulate or abuse them.

HARASSMENT is aggressive behavior or bullying.

IMPERSONATION is pretending to be another person for the purpose of entertainment or fraud (lying to someone to get something from them).

INTENT is something that is planned or done for a purpose, such as to harm or threaten them.

NETIQUETTE is polite behavior among others on the internet!

PRIVATE, or PERSONAL INFORMATION is facts that are specifically about you.

PROFILE is a written introduction to who you are. It helps others understand our likes and dislikes, how we choose to live, and what we want from life.

SCAMS are dishonest or illegal plans or activities.

TRUSTWORTHY means being able to be relied on to be safe.