



Virtually Safe

CLUB GUIDE

CLUB OBJECTIVES

This guide is designed for people who wish to teach online safety. The activities included in this suite are for young people who are already owners of devices and online accounts or are setting up their devices and social media accounts for the first time. Students will develop skills to help them protect their personal information online and prevent unsafe or unwanted contact when using devices, websites and apps.

By the end of the learning students will be able to:

- identify and establish personal online safety boundaries
- develop skills to question what they encounter online
- develop skills to identify problematic situations which may impact their online safety or security
- consider appropriate help-seeking and reporting strategies for dealing with unsafe situations online.

TABLE OF CONTENTS

Introduction
Club Objectives

Module 1: Introduction to Online Safety

Lesson 1: The Good Digital Citizen
Lesson 2: Digital Footprints
Lesson 3: Beware of Online Risks
Lesson 4: What is Online Safety?
Lesson 5: Refresher Lesson

Module 2: Staying Secure Online

Lesson 6: Building Great Passwords
Lesson 7: Setting up Two-factor Authentication
Lesson 8: Phishing
Lesson 9: Malware and VPNs
Lesson 10: Refresher Lesson

Module 3: Digital Literacy

Lesson 11: Verifying Online Identities
Lesson 12: Bots and AI
Lesson 13: Spotting Fake News and Disinformation
Lesson 14: Identifying Deepfakes
Lesson 15: Refresher Lesson

Module 4: Smart Creators

Lesson 16: Smart Sharing
Lesson 17: Personal Information is Private
Lesson 18: Plagiarism and Copyrights
Lesson 19: Netiquettes: Etiquettes for Online Groups
Lesson 20: Refresher Lesson

Module 5: Digital Responsibility

Lesson 21: The Social Media Influencer
Lesson 22: Online Betting
Lesson 23: Navigating inappropriate online content

Lesson 24: Digital Advocacy
Lesson 25: Refresher Lesson

Module 6: Digital Wellbeing

Lesson 26: Digital Reputation
Lesson 27: Making Good Choices
Lesson 28: Dealing with Cyberbullying
Lesson 29: Refresher
Lesson 30: Pass it on

Conclusion

Module 1

Introduction to Online Safety

Lesson 1: The Good Digital Citizen

Description

Digital citizenship has to do with the appropriate and responsible use of technology. This lesson introduces students to digital citizenship and lays the foundation for the other lessons.

Duration

40 - 50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Understand who a good digital citizen is and how to become one
- Acquire techniques for using the internet responsibly

Pre-discussion Activity

- Form a group of 5
- Take turns sharing the ways you use the internet. Do you play games, watch videos, make posts or visit websites? How many hours do you spend on the internet everyday?
- Next share 1 thing you've learnt from being online
- Finally each one should share the funniest thing they've seen online

Discussion

We use the internet for many things. Some of the information we get online helps us in making decisions such as what to eat, where to shop, the kinds of friends we want to keep and so on. These things qualify us as digital citizens. A digital citizen is someone who uses the internet effectively, regularly and responsibly.

A good digital citizen is someone who knows what is right and wrong, exhibits intelligent technology behavior, and makes good choices when using technology.

Here are some of the characteristics of a good digital citizen:

- Being confident and capable of using information communication technologies
- Using technology to relate to others in positive, meaningful ways
- Developing and using critical thinking skills in cyberspace
- Using technology to participate in educational, cultural, and economic activities
- Respecting the concepts of privacy and freedom of speech in a digital world

How can you become a good digital citizen?

The lessons in this curriculum are aimed at developing good digital citizenship in students. The focus areas are on online safety, digital wellbeing, digital literacy, and so on.

Here are some of the ways you can become a good digital citizen:

- Be civil online: Be sure to treat other people with respect. Do not bully, troll, make fun of, or say hateful things to people online.
- Do not steal: Don't lift other people's content and take ownership of it online. Plagiarism and copyright infringements are serious issues. Give credit where credit is due. The same applies to identity. Don't claim to be someone else or create a fake identity.
- Never give out your personal information, including phone numbers, addresses, etc. on social media. If you won't share this information with a stranger physically, then you shouldn't share them online.
- Keep your personal issues off social media. If you would not want your parents or relatives seeing your post, you probably shouldn't post it in the first place.
- THINK before sharing any information. Avoid spreading fake news or misinformation. Ask these questions before posting:
 - Is it True?
 - Is it Helpful?
 - Is it Inspiring?
 - Is it Necessary?
 - Is it Kind?

Wrapping Up

- Think of the ways you use the internet, are you a good digital citizen?
- What are your top takeaways from today's lesson?

Lesson 2: Digital Footprints

Description

Digital footprints are inevitable. The sites we visit, posts we make, likes, comments, shares, and other digital activities do not disappear from the internet. This lesson teaches students the importance of their actions online and how to make right choices.

Duration

40 - 50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Understand the importance of digital footprints
- Make informed choices when interacting online

Pre-discussion Activity

Draw an image of a footprint on a sheet of paper.

What websites do you visit? Do you use social media platforms? Fill them up in the footprints. Exchange your footprint with someone else to see the places they visit online.

Discussion

Digital Footprints describe the trail, traces, or "footprints" that people leave online. Your digital footprint is what represents you online. This could mean photos, audio, videos, texts, "likes," and comments you post on friends' profiles. Everything we do online creates digital footprints that migrate and persist. Something that happens on the spur of the moment - a funny picture, an angry post - can resurface years later. And if we aren't careful, our reputations can be harmed. In addition, a bad digital footprint can affect our future livelihood.

The Internet makes it easy to communicate with family, friends, and people who love the same things that you do. We send messages, share photos, and join conversations on social networks – sometimes without thinking about who else can see them too. A picture or post you think is funny and harmless today could be seen and misunderstood by people you never thought would see it – now or way off in the future. Once something's out there, it's hard to take it back.

Remember:

- Like everything else on the Internet, your digital footprint could be seen by people you've never met.

- Once something by or about you is online, it could be there forever. Think of this like you'd think about a permanent marker: The marks it makes can never be erased, even if you realize you meant to write something else.

It's also good to know when to post nothing at all – not to react to somebody's post, photo, or comment or not to share something that isn't true. In the last lesson, we mentioned "THINK before you post," and it's a good guide to contributing on the internet. The way to respect your own and other people's privacy is to think about what's okay to post, who might see your post, what effect it could have on you and others, and when not to post anything at all.

Wrapping Up

- Why do you think digital footprints are important?
- What if you delete a post you made, can it still resurface on the internet?
- What did you learn from today's lesson?

Lesson 3: Beware of Online Risks

Description

This lesson explores the risks that young people may face while on the internet.

Duration

50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Identify dangers on the internet
- Know how to avoid online risks

Pre-discussion Activity

Some things we do online are safe – but sometimes something might happen, or we might do something that is unsafe for us.

What are some examples of things that are safe on the internet, and things that are unsafe on the internet?

Discussion

Risks are possibilities of something bad occurring. The internet is an exciting place but it can sometimes be dangerous.

Cyberbullying, identity theft, hacking, sexting, are some of the dangers on the internet. These risks will be discussed in depth in the coming lessons.

Cyberbullying: Cyberbullying is when a person is threatened, harassed, humiliated, embarrassed, while using the Internet.

Examples of Cyberbullying:

- Sending someone mean or threatening emails or messages
- Tricking someone into revealing personal or embarrassing information and sending it to others
- Breaking into someone's account to send cruel or untrue messages while posing as that person
- Creating websites to make fun of another person such as a classmate or teacher
- Using websites or social media accounts to rate peers as prettiest, ugliest, etc.

Identity Theft: Identity theft is pretending to be someone else and using the person's image for fraudulent activities. Some people on social media pretend to be famous celebrities and use their images to ask people to donate money or other mischievous things.

Hacking: Hacking refers to those activities that compromise digital devices, such as computers, smartphones, tablets, and even entire networks. Hackers can sometimes create suspicious messages that deposit malware in a drive-by attack requiring no user interaction. They can also use psychology to trick the user into clicking on a malicious attachment or providing personal data. This is why you need to watch what you click or download online.

Sexting: This is engaging in a sexual conversation via chat or text. Social media "friends" sometimes request for or send nude, inappropriate and revealing pictures. This is dangerous as it has many repercussions. Remember that the internet never forgets. Once an image is shared online, it can always resurface even when deleted by the owner. Don't be pressured into engaging in sexting online.

Wrapping Up

- What other online risks can you mention?
- Have you encountered these risks or do you know anyone who has experienced them?
- What did you learn from today's lesson?

Lesson 4: What is Online Safety?

Description

The preceding lesson discussed online risks. This lesson gives students tips on how to be safe while using the internet.

Duration

40 - 50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Know how to tackle online risks
- Learn online safety tips

Discussion

Online Safety is being aware of the nature of the possible threats that you could encounter whilst engaging in activity through the Internet, protecting and managing your personal data, online reputation management, and avoiding harmful or illegal content. Simply put, it is how to stay safe while you use the internet.

Key Elements of Online Safety

Privacy, Security and Cyberbullying are key elements of Online Safety.

Privacy refers to the access that people have to your data. Most social media platforms have settings to control who sees and shares your posts.

For security, strong passwords which include combinations of letters, numbers and special characters are encouraged. Also, remember to enable 2-factor authentication and log out from devices that are not yours.

Tips to Stay Safe Online

- Never give out any personal information such as your full name, address, phone numbers or school name.
- Only use a computer when an adult is nearby.
- Never send a picture of yourself to a person that you don't know or haven't met.
- Never arrange to meet someone whom you have met through the Internet, even if you think you know them well or they seem really nice.
- Never give out your password to anyone (even your best friends) other than your parents.

- Don't fill out forms online without asking an adult first.
- Choose Strong Passwords
- Keep Your Privacy Settings On
- Make Sure Your Internet Connection is Secure. Use a Secure VPN Connection
- Use 2 factor verification for all your accounts
- Be Careful What You Post
- Be Careful What You Download

Be SMART online

SAFE: Keep your personal information safe

MEET: Friends made online are strangers; meeting them can be dangerous

ACCEPTING: Accepting files online can be dangerous, if unsure ask an adult

RELIABLE: Not everyone you meet online is reliable or trustworthy

TELL: Always tell an adult if someone online upsets or worries you

Activity

Design a creative poster telling people about online safety.

Wrapping Up

- What are your top takeaways from today's lesson?

Lesson 5: Refresher Class

Description

As the last lesson in Module 1, this lesson serves as a refresher of the previous lessons.

Duration

40 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Explain lessons 1 - 4
- Transfer the knowledge from Module 1 to other students

Activity

This Activity needs 2 judges, 1 moderator, 1 timekeeper and 3 teams.

Form 3 teams of 4 students to participate in a quiz. Each team picks a number from 1 - 12 and responds to the question. Each team can answer 4 questions. A question is 5 marks.

The Questions

1. What are digital footprints?
2. What does the acronym THINK stand for?
3. A good digital citizen is someone who _____
4. Mention four online risks
5. What are the elements of online safety?
6. What are 3 ways of becoming a digital citizen?
7. Why are digital footprints important?
8. What is online safety?
9. Mention 4 tips for online safety
10. What are examples of cyberbullying?
11. What does it mean to be smart online?
12. Why is sexting dangerous?

Activity 2

4 students should volunteer to explain a lesson they are familiar with in 5 minutes.

Wrapping Up

Did you find today's class exciting? What have you learnt?

Module 2

Staying Secure Online

Lesson 6: Building Great Passwords

Description

Passwords are an important and sensitive part of our online activities. This lesson teaches students how to build great passwords for maximum security.

Duration

40 -50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Understand the importance of passwords to security
- Learn how to create strong passwords

Activity

Get a sheet of paper. Draw two images of your favourite social media login page. In one image, write your example of a bad password. In the other image, write your example of a good password. Be sure not to use your actual social media password.

Discussion

A password is a secret combination used to access something. Passwords take different forms on different devices and accounts. For instance, to unlock your phone you may use a pattern, 4-digit number-only code, fingerprint, or face recognition. However, most online accounts will require you to type in a password.

Weak passwords make it easy for hackers and scammers to access our accounts, steal information and use it to damage our devices, relationships, and our reputations. This is why strong passwords are important.

Tips for creating strong passwords

Weak passwords commonly use personal information, are easy to crack, and can be guessed by someone who knows you (for example, "IamMaryJane" or "Ilovepringles").

Strong passwords are based on a descriptive phrase or sentence that's easy for you to remember and difficult for someone else to guess – like the first letters in words that make up a favorite title or song, the first letters of words in a sentence about something you did – and include a combination of letters, numbers, and symbols.

For example,

“I went to London for Christmas” could be used to build a password like: lw2L4Xm@s
Or Twinkle Twinkle Little Star could form a password like TwtwLi2\$taR

Password Dos and Don'ts

DOS:

- Use a different password for each of your important accounts.
- Use at least eight characters. The longer the better (as long as you can remember it).
- Use combinations of letters (uppercase and lowercase), numbers, and symbols.
- Make your passwords memorable so you don't need to write them down, which would be risky.
- Immediately change your password if you know or believe it may be known by someone other than a trusted adult.
- Always use strong screen locks on your devices. Set your devices to automatically lock in case they end up in the wrong hands.
- Consider using a password manager, such as one built into your browser, to remember your passwords. This way you can use a unique password for each of your accounts and not have to remember them all.

DONTS

- Don't use personal information (name, address, email, phone number, mother's maiden name, birth dates, etc.), or common words in your password.
- Don't use a password that's easy to guess, like your nickname, just the name of your school, favorite baseball team, a string of numbers (like 123456), etc. And definitely don't use the word “password”!
- Don't share your password with anyone other than your parents or guardian.
- Never write passwords down where someone can find them.

Wrapping Up

- Why are strong passwords important?
- What have you learnt from today's lesson?

Lesson 7: Enabling Two-factor Authentication

Description

Two factor authentication helps to keep our accounts extra secure. This lesson teaches students how to enable the feature on their account. (A projector and connected system may be needed for this session).

Duration

40 -50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Understand the need for two-factor authentication.
- Learn how to enable the feature on their accounts

Discussion

Two factor authentication (also known as 2FA, two-factor verification, and two-step authentication) is a security process where logging in to a service requires two separate steps or two “factors,” such as a **password** and a **one-time code**. For example, you may have to enter your password and then enter a code that was texted to your phone or a code from an app.

Two factor authentication is important because it gives you the control of permitting which device logs in to your account. This means that even if hackers have guessed your password, they won't have access to your account because that has to be verified with a code sent to you. The code can be sent to you via SMS or from an authenticator app.

How to enable two factor authentication

Most social media platforms have settings to allow two-factor authentication in the app or from an authenticator app.

For example, on instagram you can:

1. Go to your profile page and tap the menu icon in the top right-hand corner.
2. Select the Settings option from the list.
3. From the list that appears, select Privacy and Security.
4. Choose Two-Factor Authentication.
5. Tap on the switch icon next to Text Message.
6. If you don't have a phone number confirmed and associated with your

account, you'll be prompted to provide it.

7. After entering the number, tap the next icon to complete the setup.

These settings vary from app to app but the authenticator button is usually located in the settings.

Also, there are authenticator apps such as Google Authenticator, Microsoft authenticator, Apple Authenticator etc. which can be downloaded to your device. If you prefer to use an authentication app, you'll need to follow the steps below:

1. Go to your profile page and tap the menu icon on the top right corner.
2. Select the Settings option from the list.
3. From the list that appears, select Privacy and Security.
4. Choose Two-Factor Authentication.
5. Tap the Get Started button if you haven't previously turned on the two-step authentication feature.
6. Tap on the switch icon next to the Authentication App and follow the on-screen instructions.
7. To complete the process, enter the code you received from the authentication app.

Activity

Draw the two step authentication process using squares, arrows and labelling the steps on the squares.

Wrapping Up

- Why does 2FA make social media accounts secure?
- What have you learnt from today's lesson?

Lesson 8: Phishing

Description

Phishing is one of the many risks on the internet. This lesson explores phishing in depth and teaches students to identify phishing attempts so as to avoid being victims.

Duration

40 -50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Learn techniques people use to steal identities.
- Recognize the signs of phishing attempts.
- Be careful about how and with whom they share personal info

Discussion

Phishing is when someone tries to steal information like your login or account details by pretending to be someone you trust in an email, text, or other 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 also put viruses on your computer. Some viruses use your contacts list to target your friends and family with the same, or a more personalized, phishing attack. Other types of scams might try to trick you into downloading malware or unwanted software by telling you that there's something wrong with your device.

Some phishing attacks are obviously fake. Others can be sneaky and really convincing – like when a scammer sends you a message that includes some of your personal information. That's called *spearphishing*, and it can be very difficult to spot because using your info can make it seem like they know you.

How to identify Phishing

Before you click on a link or enter your password in a site you haven't been to before, it's a good idea to ask yourself some questions about that email or webpage. Here are some questions you could ask:

- Does it look professional like other websites you know and trust, with the product's or company's usual logo and with text that is free of spelling errors?

- Does the site's URL match the product's or company's name and information you're looking for? Are there misspellings?
- Are there any spammy pop-ups?
- Does the URL start with https://with a little green padlock to the left of it? (That means the connection is secure.)
- Is the email or site offering something that sounds too good to be true, like a chance to make a lot of money? (It's almost always too good to be true.)
- Does the message sound just a little bit weird? Like they might know you, but you're not completely sure?

Activity

Wrapping Up

- How can you help someone from falling victim to phishing?
- What did you learn from today's lesson?

Lesson 9: Malware and VPNs

Description

Online activity can be safe and secure when users are properly protected. This lesson teaches students how to avoid malware and make use of VPNs for secure connections.

Duration

40 -50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Define malware and VPNs
- Know how to prevent malware attacks

Discussion

Malware is malicious software such as computer viruses, Trojan horses and other harmful files that damage devices. Malware is usually transferred in the form of a link or file and requires the user to click on the link or open the file for the malware to work.

Malware is created by cybercriminals who want to steal information, attack systems or demand for money. Malware is spread by:

- Links and free files on social media: malware is spread by links or files shared on social media. They could be malware to get information like passwords, atm card details, etc
- Infected ads on websites: some pop-up ads contain malware that downloads to your device when you click them
- Virus on USB flash drive shared from computer to computer

How to be protected from malware

- Do not receive files or click links on social media if you can't verify what it is. Remember that not everyone is trustworthy online.
- Make downloads only from trusted sites
- Install antivirus on your device

How about VPNs?

VPN stands for Virtual Private Network. They are used for browsing securely on the internet. VPNs hide your IP address when you browse. Your IP address is your

Internet Protocol address. It is a string of numbers that is unique to your device when you browse. When you connect to a VPN, instead of your activity being associated with your IP address, now it's the VPN server's IP address that is associated with your data.

Activity

How would you explain malware and VPN to someone who has never heard about it?

Wrapping Up

Malware and VPNs can be avoided if we are cautious and take the right measures. What did you learn today?

Lesson 10: Refresher Lesson

Description

As the last lesson in Module 2, this lesson serves as a refresher of the previous lessons.

Duration

40 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Explain lessons 6 - 9
- Transfer the knowledge from Module 2 to other students

Activity 1

Impromptu Speech

This activity needs 4 speakers, 3 judges, 1 timekeeper, and 1 moderator.

The speakers are to pick a letter from W, X, Y or Z. The letters contain the title of their topics. They have 5 minutes to speak. Each person can get up to 10 marks based on how detailed their speech is and how well they use the time.

W = Phishing

X = Malware and VPNs

Y = Building Great Passwords

Z = Enabling Two factor Authentication

Activity 2

This activity needs 2 to 7 volunteers to act a drama telling people how to be secured online.

Wrapping Up

Did you gain any new knowledge from this module?

The next module is about digital literacy. What do you think that means?

Module 3

Digital Literacy

Lesson 11: Verifying Online Identities

Description

The online world gives room for false identities. Behind funny usernames and cartoon profile pictures, it's difficult to tell who's who. This lesson teaches students how to verify online identities.

Duration

40 -50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Understand that people online may not be who they say they are.
- Be sure the person is who they say they are before replying

Discussion

When we interact with people offline, we can always confirm that we know who it is we are talking to. We know them by the sound of their voice, the way they smile and other qualities. However, with online interactions it's harder to verify that we know who it is we're relating with.

The digital world enables people to mask their identity. Sometimes, people do so for fun. Other times, they impersonate people to steal personal information. When you're on the Internet, people you don't know could ask to connect with you. They may send you friend requests or message requests. When you're not sure who they are, the safest thing to do is not to respond or to tell a parent or trusted adult that you don't know the person trying to connect with you. But if you decide it's okay to respond, it's a really good idea to see what you can find out about them first.

How to Verify Online Identities

1. Check their profile: Check to see who their friends are, if you have mutual friends in common and search for other information that confirms they're who they say they are.
2. Profile photos: Profile photos make it easy to identify people. Is their profile photo blurry or hard to see? Or is there no photo at all, maybe something like a cartoon character's face? Bad photos, bitmojis, photos of pets, etc., make it easy for a person to hide their identity on social media. Also, most scammers steal photos from a real person in order to set up a fake profile and pretend to be them. You can do a search to see if you can find more photos of the person with the same name on the profile.

3. Usernames: For easy identification, most people on social media use their real name as usernames. This does not mean everybody on social media uses their real names. Some prefer usernames such as @africanbarbie or @fabulouswriter which may sound cool but make identification difficult. However, most social media sites create personalised urls for their users from the biodata used to open the account. For instance a facebook user with the name Tope Thomas, may have a personalised URL such as facebook.com/tope_thomas. If the user changes username from @tope_thomas to @funnycutetope, the URL may still contain the real name. You can also check if their URL matches a real name.
4. Profile bio: What does it say on their profile bio, status, or about me section of the page? Fake accounts might not have much information or might have a bunch of information copied or pulled together randomly to create a fake profile. Is there anything in their bio that you can confirm by searching for it?
5. How old is the account: You can check to see how long the account has been active. Does the activity you see line up with your expectations? Is the profile new or does it show a lot of activity? Does the person have mutual friends with you? You can tell if it's a fake account if there isn't much content, if pictures are often posted without captions, or if there are no signs of people posting, commenting, and socializing in them.

Verifying identities helps you avoid scammers, hackers and other issues online. Remember that on social media, you are in control of who you choose to talk to online. Make sure the people you connect with are who they say they are..

Activity

A volunteer shared with us how she received a direct message from an account on Instagram. The sender was not a friend or anyone familiar but they were requesting money to help some orphaned children in Northern Nigeria. The message was quite convincing and she was about to send some money to the account number provided when she decided to check the profile. The profile photo of the sender had the picture of a beautiful and responsible looking lady. The profile bio claimed she was the leader of a faith-based organization. However, none of the pictures on the page had captions, likes or comments. Also, the oldest post was 2 hours old. She guessed it was a fake account and did a search on the picture and name of the account, and she found the original account of the lady. She then blocked and reported the fake account that had sent her a message. That was how she avoided being scammed by a fake online account.

- What steps of verifying online identities can you find in this story?
- Why could the volunteer guess that it was a fake account?

Lesson 12: Bots and AI

Description

Students are interacting with more and more nonhuman “voices” coming out of devices, apps, and sites these days – mostly at home, but perhaps increasingly at school. Sometimes they’re called “chatbots,” sometimes “virtual assistants,” often just “bots.” This lesson helps students to get comfortable with interacting with technology voices.

Duration

40 -50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Learn about artificial intelligence
- Identify experiences with bots of various kinds.
- Analyze the impact these technologies can have on daily life.

Activity

Let’s chat about our experiences with bots by answering these questions:

- Do you know what a bot is?
- Have you talked to a bot? On what kind of device?
- What did it feel like?
- What do you think is the best use for a bot? (for example to ask for the weather report, get the news, play a game, ask for information?)

Discussion

Bots are becoming a common part of our lives due to technology. We sometimes call them “chatbots” or “virtual assistants.” One popular bot is Siri, it’s mostly on Apple devices. Another is Google’s virtual assistant.

Bots are used for many things: playing games, checking the weather, answering questions, getting directions, notifying you when time’s up, etc. They can be on mobile devices, online, in cars, or they can be special devices people keep in different rooms of their home.

Bots use what’s called AI, or artificial intelligence. Artificial intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions. In simple terms, AI learns from what you search so

it can get better at helping you. To do this, bots sometimes “remember,” or record, what you ask and say.

Scientists predict that much of future technology will involve Artificial Intelligence. It is necessary to understand how they work now, so we are not missing out on any knowledge.

The purpose for AI is to make lives easier and tasks faster. AI can help you by personalizing your learning. Since the technology works based on the patterns of what you say or search, AI can find resources similar to that.

However, artificial intelligence can be very addictive. When we rely too much on technology to find things for us, we risk the ability to learn from other sources such as learning by doing, and also making meaningful connections with other people.

It may be fun to interact with virtual assistants but be sure to put a balance to it.

Wrapping Up

- Children may sometimes get confused about chatbots and think they are relating with a real human. How would you explain artificial intelligence to a child?
- What did you learn from today's lesson?

Lesson 13: Spotting Fake News and Disinformation

Description

Students receive and share news online. This lesson teaches them how to distinguish real information from fake news.

Duration

40 -50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Understand how to verify information.
- Know the difference between fake news and disinformation
- Educate others on sharing the right information

Discussion

We receive plenty of information online but we also know that not everything online is reliable. Digital media has enabled the spread of false news that seems very convincing. They are sometimes called fake news or disinformation although both of them are different because of the intent behind it.

Fake news and Disinformation both have to do with wrong information. Fake news is sensational, emotionally charged, misleading or totally cooked-up information that copies the form of mainstream news.

Disinformation is deliberately misleading or biased information; manipulated narrative or facts; propaganda.

Fake news is information that is presented as breaking news but is not true. Disinformation is false information that is intentionally shared to make people think in a certain way about something. Fake news may be created based on wrong facts but disinformation is created on purpose.

When we don't pay attention to the kind of news we are sharing, we sometimes help the spread of fake news and disinformation. Remember the game where you are given two similar pictures and you have to identify what's the difference? Sometimes dealing with news is like that.

How to find fake news and disinformation.

If you spot these things, you are probably looking at a deceptive story.

1. **Spotting fake URLs:** A URL is the address of a webpage. It stands for Uniform Resource Locator. Most credible news sites have popular websites. Fake news sites often try to copy real sites by choosing URLs that are similar. They do this by changing letters or adding unnecessary letters to their URL. For example, an original news site is abcnews.com, someone created a fake news website abcnews.com.co to mimic the original ABC news.

Sometimes fake news and disinformation sites may not copy an existing news site in their URL. One way to verify if the site with a unique URL is a real site is to do a web search for the news organization or the URL. If the organization is real, a box will appear to the right of the search results with a description of the organization, including their website address. If the URL isn't real, you will often be able to scroll down and see headlines about the site being reported as a fake – or you'll find out the site isn't available anymore.

2. **Inspecting headlines:** Sometimes someone shares a news story without a URL. You can verify if the information is real by checking if:

- a) A story starts with a picture of something with a headline that would interest us, but when we click, the story has little or nothing to do with the picture or headline.
- b) If the headline comes in bold font or ALL CAPS, underlining, or exclamation points, the writer is trying to get you to think what you're seeing is important. Real journalists don't use those formatting tools.
- c) To get you to read a story, some people include words in the headline like "shocking" or "outrageous" or "surprising." They know words like that make us curious. But real journalists are intentional about their stories being objective. They tell the story and let us decide if it is shocking or surprising.

3. **Check for Credibility:** You can do this by trying to find out if other popular news organizations have shared the story. If they have it's probably true. If you can't find the news story on any credible site or channel, it's probably fake.

4. **Verifying sources:** You could take it a step further by doing a web search of the news source. What can you find about the organization? Do they have a website? How long have they been running? If it appears in Wikipedia or an article at a newspaper or news magazine's site, it's probably a real news organization.

Activity

Wrapping Up

Remember to use these tips before sharing information online. What was your biggest takeaway from today's lesson?

Lesson 14: Identifying Deep Fakes

Description

Deep Fakes are audio, video and image content used to spread disinformation. They can be misleading as they imitate a well known person. This lesson teaches students to identify and analyse deep fakes.

Duration

40 - 50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Understand how deep fakes are created.
- Identify and distinguish deep fakes from original videos

Discussion

Deepfakes are audio, video and image content that is created with the aid of a type of artificial intelligence in an attempt to deceive viewers or listeners into believing a false event or false message. Deepfake technology can add anyone in the world into a video or photo they never actually participated in.

If you've seen a video of the former American president, Barack Obama, calling Donald Trump (another American president) a "complete dipshit", then you've seen a deepfake. According to Merriam-Webster dictionary, "The term deepfake is typically used to refer to a video that has been edited using an algorithm to replace the person in the original video with someone else (especially a public figure) in a way that makes the video look authentic."

Technical terms to explain deepfakes

Algorithm: Algorithm is a process or set of rules to be followed when a computer is trying to solve a problem or instruction.

Neural networks: Neural networks are a series of algorithms that seek to identify similarities in a data set by a process that mimics how the human brain works.

How are deep fakes made?

Deep fakes are made from artificial intelligence. Remember in Lesson 12 we said artificial intelligence is programmed to learn from humans and create patterns based on what it has learnt. Making deep fakes involves neural networks. To make a deepfake video of someone, artificial intelligence is trained using a neural network to

study many hours of real video content so that it can pick the person's face from different angles. Then they'd combine the trained neural network with computer-graphics techniques to add a copy of the real person onto a different person.

Why are deepfakes worrisome?

Deepfakes are a cause for concern because they can spread misinformation. They can mimic important people in society who have authority in a particular area and pretend to be passing out real information from them. People need this information to make choices and they could be making choices based on fake information.

Deepfakes are also sometimes created with malicious intentions. It could be in an attempt to ruin a person's reputation or for identity theft. For instance, some videos have been released that show popular actors starring in porn videos which they never took part in.

How to spot deepfakes

People are using artificial intelligence to create technology that spot deepfakes but here are some of the ways we can identify deepfake videos

- **Bad lip syncing:** If the lips of the person in the video don't move according to the words, it could be a deep fake video. This does not mean that all videos with poor lip syncing are deepfakes. Sometimes real video gets logged by network and device speed in such a way that the audio sounds faster than the images in the video itself, this is not deepfake. If the image is moving but the lip is syncing poorly, it's most likely a deepfake.
- **Eye movement:** If the eyes in the video move weirdly or there is no blinking, it may be a deep fake.
- **Blurring or misalignment:** If some parts in the video are blurry, for instance where the head meets the neck.
- **Facial expressions:** When something doesn't look right about a face, it could mean that the face was morphed. This occurs when a simple stitch of one image has been done over another.

Activity

Take turns explaining deep fakes in 5 sentences. How dangerous are they? Can they have any positive uses?

Wrapping Up

Do some research on deepfake videos. How would you explain to someone else that they are not real.

Lesson 15: Refresher Class

Description

This module looked at digital literacy. Today's lesson includes activities to help students retain the previous lessons.

Duration

40 -50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Explain digital literacy in their own terms
- Educate others on sharing the right information

Activity

Charades

This game needs 4 volunteers, a moderator, a timekeeper, and the whole class.

The game has to do with the previous lessons in this module. The lessons are to be selected in number 1 - 4.

The volunteers will choose a number from 1 - 4, the moderator whispers the topic in their ear and the volunteer acts (no words!) in a way that would remind the class of the lesson without speaking.

If the class can remember what lesson it is, the volunteer selects someone from the class to share what they understand from the lesson.

If the class can't figure out what the volunteer is acting, the volunteer has to explain the lesson to the class.

Number 1: Deepfakes

Number 2: Verifying Online Identities

Number 3: Dealing with fake news

Number 4: Bots and AI

Activity 2

This activity is for everyone. Write a short creative poem/rap of 10 lines about digital literacy. Share it with the rest of the class if you want.

Wrapping Up

The next module will discuss Smart Creators. What do you think you'll learn?

Module 4

Smart Creators

Students are actively sharing and creating content on social

Lesson 16: Smart Sharing

Description

Sharing content online automatically makes you a media creator. This lesson looks at how to create smart, meaningful content that is safe for all digital users.

Duration

40 -50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Understand the use of content in cyberspace
- Know how to create great content

Activity

Get a sheet of paper. Write 4 reasons you think content is important.

Discussion

Content is what makes the online world thrive. People are always posting, sharing and liking information. When you first join social media, it may seem a little intimidating to begin sharing content. After a while, you may get more comfortable with sharing on your page. Having content means people connected to your profile can get information from you. How do you navigate what to share and how you should share content online?

Tips for creating great content

1. Stay true to who you are: Create content that is authentic and communicates your thoughts and opinions. Sometimes you may get inspiration from other sources but be sure that your posts reflect your true identity.
2. Map out what you want to create: Your posts and content represent you. What type of content do you want to share with others? To share any and everything may constitute junk on your profile. Decide what you want to be known for or associated with. Remember to THINK before creating content. Ask if it is true, helpful, inspiring, necessary and kind.
3. Do plenty of research: As a good digital citizen, your posts have to be well informed, even if they are just your opinion. Don't share content you haven't

verified or can't vouch for. Spreading misinformation can be dangerous. Always do your search before posting about something.

4. Do not spread disinformation: Disinformation is false information intentionally created to make people think in a certain way. People may spread wrong information out of ignorance, but disinformation is purposeful. Whatever you do, be sure not to spread disinformation on your profile.
5. Be consistent: Consistently share true and relevant information. The more you share, the more you learn better ways of creating content, and who knows you may even become a thought leader with your posts.

Wrapping Up

- What may be your barrier to creating content?
- How can you take away the barrier?
- What did you learn from today's lesson?

Lesson 17: Personal Information Stays Private

Description

Sharing on social media is fun until we begin to share too much. Where do we draw the line between openness and privacy? This lesson teaches students how to share responsibly.

Duration

40 -50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Know what information should be private
- Understand how to maintain privacy on social media.

Discussion

Privacy is something you share with people you know and trust, not random strangers. Not everyone who comes across your profile should have complete access to your life because you don't know and trust everyone you meet on the internet.

Privacy is also important because once something is out on the internet, it can't be completely withdrawn, even when deleted. Remember the lesson on digital footprints? This is why it is important to caution what type of information is posted on your profile.

You can protect your privacy by sharing only things that you're sure you want to share. There are certain personal information that you shouldn't put online. Details such as:

- Your house address
- Your date of birth
- Your password

Privacy also has to do with the content of other people you share. You need to know how to respect other people's privacy by knowing when to share or not share things that involve them. When a person is grieving or not feeling well, it may be wise to respect their privacy and keep that information offline. Also if you have embarrassing photos of someone you should respect their privacy and not post it. It adds up to their digital reputation as well.

Privacy Questions to ask before making a post

- Am I giving out too much information about myself and others close to me?
- Will I be proud to let everyone know about my post or will it be hidden from some people?
- Will my post be misunderstood?
- If it's a post of a friend or family member will they be happy that I made that post for them?
- Will I still be proud of this post later?

Remember not to make any posts in the heat of the moment. Think through your content. The purpose of keeping personal information private is not to live a filtered life but to ensure that you hold on to the things that count.

Activity

- Think of scenarios where someone may have shared too much information online.
- What kind of personal information did they share?
- What was the repercussion?

Wrapping Up

You can share great content, have fun online, and still keep your life private if you ask the right questions. Remember to ask the privacy questions before posting.

- What did you learn from today's lesson?

Lesson 18: Plagiarism and Copyrights

Description

Plagiarism is lifting somebody's work and claiming it as your own. Copyrights issues have to do with using another person's content and not giving credits to the owner. Both of these issues have to do with using content that does not belong to you. This lesson teaches students how to responsibly share content belonging to others.

Duration

40 -50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Define what plagiarism and copyrights
- Understand how to responsibly share content belonging to others

Discussion

Plagiarism is the practice of taking someone else's work and passing it off as your own. This includes quotes, images, videos that are not credited to the owner.

Copyright is a set of rights belonging to the creator or owner of a work, such as a song, literary work, movie, or photograph. These rights are backed by law and allow a copyright owner to control who, when, where, and how their work is used. Copyright infringement occurs when someone uses an author's work without permission or credit to them.

You may find an image or song that you really like and would want to share online. Before posting the content check for the owner so you can give credits.

Difference between plagiarism and copyright issues?

Plagiarism and copyright infringement both refer to the improper use of somebody else's work. They are similar but not the same. Plagiarism is using content and not saying where you got it from. Copyright infringement is using content without permission and this is against the work's copyright law.

For example, you want to run a food blog and you need some content. Plagiarism is like copying and using some of the content from a site without giving reference to the site. Copyright infringement is copying all of the content on the site and posting it in your name and this violates the ownership laws of the original owner.

Also copyrights are protected by law, so the original owner of a work can sue people for using their content without asking for permission.

How to avoid plagiarism and copyright issues?

To be a responsible digital citizen, the right thing to do is to not steal other people's work. Here are some of the ways you can avoid plagiarism and copyright issues.

- Get permission from the original owner before using their work. Leave them a message requesting to use their work. If they do not consent, do not use their work.
- Be sure to give credit to the source. You can do this by tagging the owner or leaving a link to the original site.
- If you are not sure who the original owner of a work is, state that it is not originally yours by adding something like, "source unknown" to the description of your work.
- Use free content. Some sites offer free pictures and free music that do not have copyrights. You can check sites like Pixabay and creative Commons for free pictures, videos or audio.

Activity

This activity needs 2 to 3 people for a short drama. In this drama, one person is the original creator of a content while the other person steals the content and claims it is their own. How does the owner react?

Wrapping Up

Plagiarism and Copyright infringement are serious issues. Think of how it would feel to have your work stolen. Did you learn anything from today's class?

.

Lesson 19: Netiquettes: Etiquettes for Online Groups

Description

As students interact more online, they may come across other internet users with differing views and opinions. This lesson teaches students basic etiquette for online interactions.

Duration

40 -50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Understand the need for etiquettes online
- Learn tips for appropriate online behaviour

Discussion

Etiquettes are proper conduct or code for polite behaviour that is required in any group or community. Online etiquettes are sometimes called “netiquettes”. Etiquettes describe how we should politely behave when we are among people.

Words and behaviour can be easily misunderstood online because it is difficult to pick up nonverbal communication that would have been obvious in real life interactions. Netiquettes help to ensure that with the use of words, emojis, images, audio or video, we are communicating appropriately.

Online étiquettes or netiquettes are important because they help to ensure that online communities are civil and free of discord.

How can we begin to practice better netiquette?

Simple tips for online etiquette

1. **Be respectful:** Respect other people's opinions and thoughts. Even if you don't agree with them, let them know in a respectful and clear way.
2. **Be aware of how your comments might be read:** Think through how your comments will be perceived. Are you communicating clearly what you intend to say? Strong language, capital letters, and exclamation marks can be easily misinterpreted online.

3. **Be careful with humour and sarcasm:** It may be cool to share jokes and sarcasm online but remember that you may not always be understood. Ensure that your jokes are not offensive.
4. **Remember to check friend requests and group invites before accepting them:** Always review and check out friend requests before accepting them. Check their profile for mutual connections before accepting. Remember that not everyone online is reliable. With group invites, the proper thing is to be told before being added to a group. This goes both ways; you also have to tell other people before adding them to a group.
5. **Take time to read the rules of conduct/ community standards:** Most online groups, social media sites and gaming networks have their own code of conduct or guidelines for a user's online behaviour. Read those rules so you can act accordingly. On social media, if a user goes against the stated conduct their account may be banned this is because each user has equal rights.
6. **Be forgiving:** The online world has different people with differing views, it helps to choose to forgive others ahead when they struggle with online communication. If you see something online that you don't think is appropriate, you can use reporting tools to flag it to have it taken down or not shared with you.

Activity

Your friend adds you to an online group that has some people you know and people you have never met. Describe how you would make use of netiquettes in the group.

Wrapping Up

We meet different people online, some who are like us and some who are completely different. With netiquettes you can ensure that your online interactions are gracious and stress-free.

- What did you learn from today's lesson?

Lesson 20: Refresher Lesson

Description

Students have learnt what it means to be smart creators, this lesson tests how well they can apply that knowledge.

Duration

40 -50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Explain who a smart creator is
- Share tips on creating great content online.

Activity

Get a sheet of paper. Answer these questions

- What are the tips for creating great content?
- What are netiquettes?
- Who is a smart creator?
- Why is privacy important in content sharing?
- What is the difference between plagiarism and copyright infringement?

Activity 2

This activity needs 10 people to share what has changed in their knowledge about sharing and creating content. What did they think before? What do they think now?

Wrapping Up

The next module looks at digital responsibility. How can you be digitally responsible?

Module 5

Digital Responsibility

Digital wellbeing has to do with how the internet affects your health. Technology, and how we use it, can affect how each of us feels, think and behave. It can also affect the health of our own body and mind. It is important to use digital technology in a way that makes us feel happy, safe and healthy. Digital wellbeing is about balance. Digital technology can help us to learn and grow in many ways but too much of it can harm our own well-being.

Lesson 21: The Social Media Influencer

Description

Smart consistent creators who know their content may end up as popular social media influencers. Social media users who create content may not be popular but would still wield a sphere of influence with their connections. This lesson introduces students to the world of responsible social media influence.

Duration

40 -50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Understand the job of a social media influencer
- Know how their content affects others
- Learn how to be responsible influencers

Activity

- Do you know any social media influencers?
- What would you describe their job as
- If you were to be a social media influencer, what principles will you work with?

Discussion

Influence means the ability to have an effect on the thoughts, choices, character and behaviour of someone. To have influence means that people trust what you say and the advice or recommendations that you give.

Social media influencers are people who have built trust in their field. They are like social media celebrities. Social media influencers are important to the digital world because they are opinion leaders.

Some people make money from being social media influencers. Companies pay them to market their products or services because they know people listen to them. It is critical that social media influencers are leading people right.

You may not be a popular social media celebrity but you are an influencer of your profile and all the information that can be gotten from you. Being digitally responsible means you are considerate about the type of information you share and how that information affects others.

How does your content affect other people?

Tobi likes to visit restaurants and share his experience on social media. He is a food blogger. People like Tobi's reviews so they visit the restaurants he endorses. One day, Tobi went to a restaurant but they didn't let him in because he wasn't wearing face masks. Tobi got angry and did a bad review about the restaurant. Immediately, the restaurant started to lose customers because of Tobi's post.

In this story, Tobi is an influencer. People trust his content about food and restaurants to visit. When he made a bad review, this affected their choices on whether they should visit the restaurant or not, some people decided not to and they lost customers. Tobi's content affected the people he was speaking to and the people he spoke about.

Tips for Responsible Social Media Influencing

- Understand your influence: The content you post or endorse can affect other people's thoughts and actions. Are you sharing true, accurate and inspiring information?
- Have principles: Principles are a set of rules or values that a person lives by. It is important to have principles that guide your actions. Influencers have sometimes led people to make the wrong decisions by endorsing fake products because they were paid to do so. Such influencers do not have the right principles. If someone wants you to share something against your principles, the best option is to say no.
- Be consistent with meaningful information: People can see through when you're just saying something to get their attention, or when you're genuine.

Wrapping Up

Responsible digital citizens understand how their actions affect others and are careful with their influence. What did you learn from today's class?

Lesson 22: Online Betting

Description

Online betting is common among young people and has become addictive for many. This lesson aims to educate about the dangers of online betting and its negative impact on digital wellbeing. Students will learn about the mechanics of online betting, identify the risks involved, and develop strategies for resisting peer pressure to engage in such activities

Duration

40 -50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Understand the concept of online betting.
- Identify the potential risks and consequences of online betting.
- Develop strategies to resist peer pressure related to online betting and stay responsible.

Discussion

Online betting is also known as internet gambling or online gambling. This includes activities like sports betting, casino games, poker, and bingo. It involves placing a bet on the outcome of an event, whether it's a sporting match, a card game, or a random number generator.

How Does Online Betting Work?

Online betting platforms operate by allowing users to create accounts and deposit funds. These funds are then used to place bets on various options offered by the platform. If the bet is successful, the user receives winnings, which can be withdrawn or used for further betting. The technology behind online betting involves secure payment gateways, random number generators (for casino games), and sophisticated software to manage bets and payouts.

Potential Risk Involved in Online Betting:

- Online betting can have severe financial consequences. The attraction of quick wins can lead to impulsive spending and debt accumulation. Students, with

limited financial resources, are particularly vulnerable to the idea of easy money offered by online betting platforms. This can result in financial hardship, affecting their ability to meet daily expenses or save for future goals

- Online betting can have a detrimental impact on mental health. The constant pursuit of wins can lead to addiction, characterized by obsessive thoughts about gambling, difficulty controlling impulses, and neglecting other responsibilities. This can manifest in feelings of anxiety, depression, and isolation. The fear of losing money or the shame of gambling habits can further expand these emotional challenges.
- Engaging in online betting is illegal for Underage. Underage gambling can result in legal consequences, including fines or even criminal charges. It's essential to understand that gambling platforms have age verification processes. The risks associated with underage gambling are significant, and it's crucial for young people to be aware of the legal implications.
- Online betting can be highly addictive, consuming a considerable amount of time and energy. This can divert attention from academic pursuits, leading to decreased focus, lower grades, and ultimately, a negative impact on educational goals.

Resisting Peer Pressure

1. Assertive Communication: Learning to say "no" confidently is crucial. You are encouraged to practice assertive communication techniques.
2. Building Self-Esteem: High self-esteem can help individuals resist peer pressure.
3. Seeking Support: As a student learn to talk to trusted adults, such as parents, teachers, or counselors, they can provide you with guidance and support.

Role-Play Scenarios

Scenario 1: A friend suggests placing a bet on a popular sports event, promising big winnings.

Scenario 2: A group of friends is discussing their recent gambling wins, making it seem exciting and lucrative.

Scenario 3: A friend pressures another to borrow money to place a bet, promising to share the winnings.

For each scenario, students should practice different responses, such as:

Assertive refusal: Clearly and confidently stating "no" to the suggestion.

Seeking support: Explaining their concerns and seeking advice from a trusted adult.

Activity

What strategies can you use to resist peer pressure related to online betting?

Wrapping up

How would you teach others about underage online betting?

How would you approach someone who is addicted to online betting?

Lesson 23: Navigating inappropriate online content

Description

Navigating inappropriate online content refers to the ability to identify, understand, and respond effectively to harmful or unsuitable material encountered on the internet. This includes recognizing different types of inappropriate content, such as explicit images. This lesson focuses on equipping students with the essential skills to discern and interact safely with online content.

Duration

40 -50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Differentiate between appropriate and inappropriate online content.
- Understand the potential consequences of engaging with inappropriate content.
- Develop strategies for avoiding harmful content and seeking help when needed

Discussion

The difference between Appropriate and Inappropriate Online Content:

Appropriate online content is generally safe, age-appropriate, and respectful. It is informative, educational, or entertaining without being harmful or offensive. Examples include Educational Websites, News and current events from reputable sources etc .

Inappropriate online content is harmful, offensive, or exploitative. It can have negative impacts on individuals and society. Examples include explicit sexual content that is often harmful and exploitative which is our focus.

Consequences of Engaging with Inappropriate Content:

- Emotional distress, anxiety, or depression.
- Damage to reputation or relationships.
- Exposure to harmful stereotypes and misinformation.
- Addiction or dependency on such content

Strategies for Managing Exposure to explicit sexual content:

- Critical Thinking: You need to develop critical thinking skills to evaluate the content you encounter. Ask questions like, “Is this content appropriate for my age?” or “Does this content align with my values?”
- Open Communication: Anytime you come across such content, discuss your online experiences with trusted adults, such as parents, teachers, or counselors.
- Blocking and Reporting: You can make use of your blocking and reporting buttons on social media accounts that share inappropriate content.

Activity

Student should share the value of spending time offline and engaging in other activities.

Wrapping up

When you encounter inappropriate online content, what do you do ?

Lesson 24: Digital Advocacy

Description

Digital advocacy is the strategic use of online platforms to raise awareness, build support, and drive action for a cause. It involves leveraging digital tools to engage with the public and create positive change. This lesson explores what digital advocacy is, and the tools used.

Duration

40 -50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Define what digital advocacy is
- Understand the tools and strategies .

Discussion

Digital advocacy is the strategic use of online platforms and tools to promote a cause, influence public opinion, and drive social change. It involves leveraging the power of the internet to engage with stakeholders, build relationships, and mobilize support for a particular issue.

Key Components of Digital Advocacy:

- Identifying Your Target Audience: Understanding who you are trying to reach and where they spend their time online.
- Choosing the Right Platforms: Selecting social media platforms, websites, and other digital channels that align with your target audience.
- Creating Engaging Content: Developing compelling messages, visuals, and stories that resonate with your audience.
- Building a Strong Online Presence: Establishing a credible and trustworthy online identity.
- Mobilizing Support: Encouraging others to join your cause through online actions like signing petitions, sharing content, or donating.
- Measuring Impact: Tracking the reach and effectiveness of your digital advocacy efforts.

Tools and Strategies:

- Social Media: Utilize platforms like Facebook, Twitter, Instagram, and TikTok to spread awareness and engage with your audience.

- Online Petitions: Create and share petitions to gather support for your cause.
- Email Campaigns: Build an email list and send targeted messages to supporters.
- Content Creation: Produce blogs, videos, and infographics to educate and inspire your audience.
- Online Communities: Participate in relevant online forums and groups to connect with like-minded individuals.

Lesson 25: Refresher Lesson

Description

Students have learnt various digital content and how to be responsible online.

Duration

40 -50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Define what digital responsibility is
- Understand how to build habit that promotes their digital responsibility

.

Activity

Get a sheet of paper. Answer these questions

What are good online behaviors?

What do you do when you encounter inappropriate online content?

Who is a digital advocate?

How does critical thinking foster digital responsibility?

Activity 2

This activity needs 10 people to share what has changed in their knowledge about digital responsibility. What did they think before? What do they think now?

Wrapping Up

The next module looks at digital Wellbeing. How does the internet affect your health?

Module 6

Digital Wellbeing

Digital wellbeing has to do with how the internet affects your health. Technology, and how we use it, can affect how each of us feels, think and behave. It can also affect the health of our own body and mind. It is important to use digital technology in a way that makes us feel happy, safe and healthy. Digital wellbeing is about balance. Digital technology can help us to learn and grow in many ways but too much of it can harm our own well-being.

Lesson 26: Digital Reputation

Description

Digital Reputation is an important part of our digital presence. It determines how people perceive you and the opinions they form about you. This lesson explores what digital reputation is, and how to form a good reputation.

Duration

40 -50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Define what digital reputation is
- Understand how to build and protect their digital reputation.

Discussion

A reputation is the opinion or belief that is held about someone or something. It is what people think about you. A digital reputation is how people think about you online.

Your digital reputation is defined by your behaviours in the online environment and by the content that you post about yourself and others. This includes the photos you're tagged in, blog posts you make, your comments, likes and your other interactions on social media. Your online activities shape how you are perceived by others online and offline, now and in the future.

A poor digital reputation can affect your friendships, relationships and even your job prospects – so protect your digital reputation. It is important to think about how you want to be represented online. Some people lose out on opportunities because of embarrassing content about them online. These posts may have been shared out of ignorance or just playfulness. Sometimes, the person who made the post may have had a change in their opinion or behaviour. However, It usually does not matter how long ago the post was shared, people can still hold a perception about you. It is your responsibility to ensure that people hold the right opinion about you. You can do this by building a good digital reputation.

How to build your digital reputation

1. Think before you post, send or blog: Having information to share online may be exciting but before you rush to make a post, think again. Remember to ask

if your post is true, helpful, inspiring, necessary or kind. Would you be comfortable with your parents or family members finding your post? What type of posts do you like or share? Do these posts represent you well?

2. Treat others as you would like to be treated: Be kind online. Avoid hurtful comments or interactions. Do not engage in or support cyberbullying.
3. Keep an eye on photos tagged by your friends and remove ones that are offensive.

Activity

Below are three social media profiles of Chika, Musa and Joseph. Read the profiles and say what you think their digital reputation is.

Chika is on social media as @princesschika. She posts pictures of her clothes, shoes and places she visits. She tags designers such as Nike and Adidas on her posts. She likes to get the latest outfits and blog about fashion trends.

Musa's username is @musaabdul. His posts often include motivational quotes and videos. He also shares content on literacy and how to solve mathematical equations. Musa doesn't share many photos of himself but when he does, he shares photos of him receiving an award or giving a speech.

Joseph is on social media as @cutejoeboy1. He likes to share posts that make people laugh. He posts comedy content and videos of epic fails. Joseph also shares invites to parties and links to download music on his page. He posts pictures of himself with celebrities.

Wrapping Up

People don't need to meet you to know your digital reputation. What is your current digital reputation and how can you improve it? What have you learnt from today's lesson?

Lesson 27: Making Good Choices Online

Description

We make decisions every day. When using technology, we need to think a little harder about the choices we make – because all choices have consequences. This lesson introduces students to a tool to help them make the right choice online.

Duration

40 -50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Understand how they make choices online
- Learn what tool to use when making online choices

Discussion

We live in a digital age. This is because most of our communication and interactions take place online. The internet also affects the decisions we make.

Some of the decisions we make include the type of values we choose to embrace, the way we choose to speak, the clothes and things we want and ultimately the kind of life we aspire to live. This is formed by the interactions we keep and content we consume online.

Sometimes we don't make the right decisions online because we want to be up to date, we didn't think through the consequences, or we don't want to lose friends. Examples of wrong choices include:

- Posting vulgar content because it seems cool
- Stealing or borrowing things to get more likes or impress your friends online
- Supporting hurtful comments because they were posted by your friend
- Pressuring your parents or doing wrong things to get the latest gadgets and devices even though you can't afford it yet.
- Not sharing meaningful or intelligent content because you think you would lose friends

There are other examples that help us understand wrong choices. However, remember that each of the choices we make add up to our digital footprints and create a digital reputation that may affect us negatively.

How to make good choices online

To make a good choice online, use the TEC tool:

Think, Evaluate, Choose.

1. Think of all your options. It is important to think very clearly of what you are about to do. For instance, your friend asks to reshare a content that you are not proud to be associated with. What can you do?
 - a) You can tell your friend you're not comfortable with the post and so you won't be sharing on your profile
 - b) You can share it because you don't want to offend your friend
 - c) You can either choose to ignore and not respond
2. Evaluate these options. What will happen if you choose to follow a particular option?
 - If you choose option A, your friend may be offended but they will know not to ask you to share that type of content again.
 - With option B, you may make your friend happy but you will also be misrepresenting yourself. Remember your digital footprints.
 - With option C, you didn't clearly communicate and so your friend may ask you to do the same thing again, another time.
3. Choose the best outcome for yourself and the people involved. After evaluating all your options, make the best choice based on your values and how you want to preserve your digital footprints and reputation.

Activity

Write 5 examples of good choices you can make online. Take turns sharing those choices to everyone.

Wrapping Up

What are the previous choices you've made online? Were they good choices? From today's lesson will you be doing anything differently when making choices online?

Lesson 28: Dealing With Cyberbullying

Description

Cyberbullying can be a painful experience. This lesson teaches students how to deal with cyberbullying.

Duration

40 -50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Recognize the signs of cyberbullying.
- Know how to respond when cyberbullying occurs

Discussion

Cyberbullying primarily happens online and can cause emotional and physical harm, especially if the bully is someone you interact with in daily life.

It can take place as:

- Spreading rumours online
- Posting embarrassing photos or videos
- Harassing and being mean to someone
- Sending someone mean or threatening emails or text messages
- Tricking someone into revealing personal or embarrassing information and sending it to others
- Breaking into someone's account to send cruel or untrue messages while posing as that person
- Creating websites to make fun of another person such as a classmate or teacher
- Using websites or social media accounts to rate peers as prettiest, ugliest, etc

What do you do if you or someone you know is being cyberbullied?

- Collect evidence: copy URLs or take screenshots of the material
- Report the cyberbullying material to the social media service.
- Block the person and talk to someone you trust
- Report to a trusted adult

Sometimes cyberbullying could be done by somebody you're familiar with, such as someone in your school or your neighbour. How do you manage the experience when you'll still meet the cyberbully physically?

- Collect evidence: copy URLs or take screenshots of the material
- Report the cyberbullying material to the social media service.
- Block the person and talk to someone you trust
- If it happens in school, report to your school authorities, showing them the evidence
- If it happens at home, report to your parents or guardian, showing them the evidence

Activity

Gideon has a medical condition that makes him very skinny. His classmates posted a picture of him and called him stickman. What should Gideon do?

Wrapping Up

- How would you help a friend who is being cyberbullied?
 - What did you learn from today's lesson?
- .
- .

Lesson 29: Refresher Lesson

Description

Refresher lessons help to ensure that we retain the learning in each module. This lesson has activities to check how well students are grasping the previous learnings.

Duration

40 -50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Understand how to verify information.
- Educate others on sharing the right information

Activity

Write a story on digital wellbeing.

Name your characters, their age, tell us if they are male or female. In the story, tell us what type of digital reputation they have. Did they face pressure trying to make the right choices? How did they deal with cyberbullying? Does the story end well or sadly?

Activity 2

This activity needs 10 volunteers. Each student should pick a module to explain. One module can only be picked by 2 students. This means 2 people explain Module 1, Module 2, and so on. Other students can chip in what they've left out.

Wrapping Up

This is the second to the last lesson for the club. Before the next meeting, think of ways you would like to pass your knowledge to others who are not a part of the club.

Lesson 30: What Next?

Description

This is the last lesson in the Virtually Safe club guide. Students have been fully immersed in extensive online safety lessons. In this lesson, they discuss how to extend their knowledge to other students who were not part of the club.

Duration

50 minutes session

Lesson Objectives

At the end of this lesson, students will be able to:

- Share how the club has made a difference in their digital citizenship
- Decide how to educate others on online safety

Activity

Form teams of 5 students. Each team needs a notetaker and presenter. Everyone in the team shares how they think the Virtually Safe Club has helped and what has changed in their online activities since they've been a member of the club.

The notetaker writes down their responses. The presenter of each team presents to everyone in the club.

Activity 2

Form another team of 4 with a new set of people. This team will need two notetakers and two reporters. Discuss the ways you can teach other students on online safety. Will you be coming together to set up your own club, will you share weekly content to other students online, or will you make comics to create awareness about online safety?

You can think up other creative ways but you must decide not to hold on to your knowledge. Gather the notes from your discussion and your reporters can send us your plans by email to hello@virtuallysafe.org. Be sure to include your details so we can get in touch with you and see how we can support you.

Wrapping Up

Congratulations Virtually Safe Ambassador! You made it to the very last lesson. We are confident that you are a good digital citizen with clean digital footprints and you are making the right choices online. We look forward to hearing from you. Remember to Click Smart, Click Safe.

Glossary