unicef
for every child

DIGICHAMPS:
A Module Set on Instilling Digital Responsibility to Children

DIGICHAMPS:

A Module Set on Instilling Digital Responsibility to Children

Table of contents

Lets get started on your digital champion journey

Module 1: Navigating the Digital World 17

Pre-activity 1 Digipedia: What we know about the digital world 20
Activity 1:1. Its a Match 21
Activity 1.2. Let's Connect: Exploring the Digital Landscape 26
Activity 1.3. Social Media Carousel Pros and Cons of the Digital World 27
Activity 1.4. Digital Scavenger Hunt: Fact and Figures of Children in the Digital World 30

Module 2: Practicing Digital Rights and Responsibilities 33

Pre-Activity 2. Sorting Challenge: Right vs Responsibility 36
Activity 2.1. My Right, My Responsibility! 38
Activity 2.2. Red Flag or Green Flag: Where's the Netiquette? 44
Activity 2.3. I Spy: Looking at My Own Social Media 47

Module 3. Ensuring Digital Safety and Security 49

Pre-Activity 3. Cybersecured! 52
Activity 3.1. STOP or GO: Digital Safety Simulation 55
Activity 3.2. Fraud Alert! 60
Activity 3.3. Fact or Fiction? 65
Activity 3.4. My Online Trail 72
Activity 3.5. Docufilm Analysis: The Power of Privacy 74

Module 4: Understanding Cybercrime, Cyberbullying, and OSAEC 75

Pre-Activity 4. Cybercrime Pre-Test 79
Activity 4.1. Red Flag or Green Flag? Recognizing Cybercrime Risks 82

Activity 4.2. Video Analysis: 'George' 87
Activity 4.3. No to Bullies, Yes to Allies! A 'Campaign Against Cyberbullying' Activity 90
Activity 4.4. Docufilm Analysis 93
Activity 4.5. Policy Drafting Workshop 96
Activity 4.6. Guardians of the Digital Galaxy: Poster against OSAEC 99

Module 5. Fostering Digital Well-being **101**

Pre-Activity 5. Digital Well-being Self-Assessment 104
Activity 5.1. A Day in a Life of a Digital Citizen 106
Activity 5.2. Digital Balance Check-In 109
Activity 5.3. A Better Day in the Life of a Digital Citizen 113
Activity 5.4. (Take Home Activity)Family Digital Well-being Action Plan 114

Module 6. Exploring Artificial Intelligence **115**

Pre-Activity 6. AI or Not? 118
Activity 6.1. My Day, My AI: A Personal Inventory 119
Activity 6.2. Where's the AI? 123
Activity 6.3. Ethics Challenge: Roleplaying for Responsible Use 126

Module 7: Advocating Digital Responsibility **130**

Pre-Activity 7. Am I A Champion? 133
Activity 7.1. DigiChamp Persona Activity: Design Your Digital Hero! 135
Activity 7.2. Digital Responsibility Action Plan 138
Activity 7.3. Digital Responsibility Awareness Campaign 140

Welcome to DigiChamps: A Module Set on Instilling Digital Responsibility in Children. DigiChamps is a comprehensive module set designed to empower children with the skills and knowledge needed to navigate the digital world responsibly. In today's technology-driven era, equipping our students with the tools to become responsible digital citizens is essential. This module set aims to instill a sense of awareness, critical thinking, and ethical behavior when engaging with online and social media platforms. Recognizing that children can and must be involved in decisions concerning themselves and their future, this module is derived from a series of co-creation and consultative workshops with children and teachers as well to concretize how a digital responsibility module should look like in today's age.

At the end of this module set, the learners will be able to:

1. Equip learners with a comprehensive understanding of the digital landscape and its impact on children.
2. Empower learners to recognize, enumerate, and practice their digital rights and responsibilities and exhibit responsible online behavior.
3. Enable learners to identify potential digital dangers, mitigate risks, evaluate online content for legitimacy, recognize fraudulent activities, and establish methods for maintaining a secure and positive digital presence.
4. Describe the legal framework concerning cybercrime including cyberbullying and Online Sexual Abuse or Exploitation of Children (OSAEC).
5. Educate learners about the concept of digital well-being strategies for promoting a healthy digital lifestyle.
6. Familiarize learners with artificial intelligence, its applications, opportunities, and challenges.
7. Advocate for digital responsibility and create effective awareness-raising activities.

Module Title	Module Objectives	Estimated Duration
Module 1: Navigating the Digital World	1. Describe the pillars of the digital world and the components of the digital landscape. 2. Identify the opportunities and challenges presented by digital technology. 3. Explain how children are engaged and exposed to the digital world.	4 hours
Module 2: Practicing Digital Rights and Responsibilities	1. Enumerate one's digital rights and responsibilities. 2. Display responsible online behavior and proper netiquette when interacting with social media and other digital platforms. 3. Demonstrate responsible and ethical behavior in digital environments.	4 hours and 30 minutes
Module 3: Ensuring Digital Safety and Security	1. Identify the potential dangers of the digital world and the ways to mitigate/ prevent them from happening. 2. Evaluate online content and interactions to identify scams, identity theft, and other fraudulent activities. 3. Differentiate legitimate online content and fake news. 4. Create a plan for a positive digital footprint and account security.	6 hours
Module 4: Understanding Cybercrime, Cyberbullying, and OSAEC	1. Describe the legal framework surrounding cybercrime, including relevant legislation such as the Cybercrime Prevention Act of 2012 (Republic Act No. 10175). 2. Identify cyberbullying and develop strategies for addressing it. 3. Explain Online Sexual Abuse or Exploitation of Children (OSAEC).	5 hours

Module Title	Module Objectives	Estimated Duration
Module 5: Fostering Digital Well-being	1. Evaluate the concept of digital well-being and understand its critical role in balancing digital and offline life. 2. Analyze the mental health impacts associated with digital overload, including stress, anxiety, and physical symptoms. 3. Identify warning signs and consequences of excessive digital use, with a focus on internet and mobile gaming addiction, and propose preventive measures. 4. Develop and implement practical strategies and action plans, including family-based initiatives, to promote digital well-being.	3 hours
Module 6: Exploring Artificial Intelligence	1. Define artificial intelligence, identify its various applications, and the opportunities and challenges it presents. 2. Explain the responsible use of AI, including behavioral, ethical, and legal considerations. 3. Evaluate the potential contributions of AI applications in education.	4 hours and 30 minutes
Module 7: Advocating Digital Responsibility	1. Analyze the importance of digital responsibility and its impact on peers. 2. Apply strategies for promoting digital responsibility and becoming digital heroes. 3. Create effective promotional materials to raise awareness of digital responsibility.	4 hours
	TOTAL ESTIMATED DURATION	31 HOURS

DigiChamps is designed as a dynamic and adaptable framework, allowing educators or trainers to tailor the module set to the specific needs of their training sessions or classroom environments. The curriculum can be delivered as a complete course or broken into shorter, more focused segments, ensuring that each session aligns with the unique pace and engagement levels of the participants.

While the provided time estimates offer a useful guideline, they are flexible and can be adjusted based on factors such as class size, interaction, and the depth of discussion required. Instructors are encouraged to carefully select and adapt activities from the modules to best suit the interests and skill levels of their learners, ensuring the content remains both relevant and impactful.

This module set empowers educators to create a responsive learning experience that not only addresses the fundamental aspects of digital responsibility but also evolves to meet the ever-changing challenges of today's digital landscape.

Lets get started on your digital champion journey

Think back to your first encounter with technology. What was it like? Did it spark curiosity, or maybe a little confusion? This module will equip you with the skills to confidently navigate the digital world. In this module, we'll be exploring various digital tools. Do you have a smartphone, laptop, tablet, or smart TV (or any combination of these)? How comfortable are you navigating websites and online applications (scale of 1-5)?

Before we start with the different modules, let us look at your current knowledge level through a pre-test.

INSTRUCTIONS:

Choose the BEST answer for each question.

1. **Which of the following is NOT a part of the digital world?**
   - ☐ Social media platforms
   - ☐ Board games
   - ☐ Smartphones
   - ☐ Online games

2. **What is one way the digital world has impacted how we communicate?**
   - ☐ We can only talk to people who live near us.
   - ☐ We can easily video chat with friends and family who live far away.
   - ☐ We have to write letters to communicate with each other.
   - ☐ Communication is much slower than it used to be.

3. **What is the term used to describe the gap between those who have access to technology and those who don't?**
   - ☐ Digital divide
   - ☐ Global gap
   - ☐ Information gap
   - ☐ Connection difference

4. **What is something you can do to stay safe online?**
   - ☐ Share your password with everyone you know.
   - ☐ Only visit websites that your parents approve of.

☐ Click on every link you see in an email.
☐ Never talk to anyone online you don't know in person.

5. **Digital citizenship is about:**
   ☐ Using a computer for browsing the internet.
   ☐ Being a responsible and informed user of technology.
   ☐ Only playing online games.
   ☐ Communicating with friends through social media.

6. **Which of the following is NOT a positive aspect of the digital world?**
   ☐ Risk of cyberbullying and online scams
   ☐ Access to information and communication tools
   ☐ Ability to connect with people from all over the world
   ☐ Encouragement of creativity and innovation

7. **When using the internet for a school project, it's MOST important to:**
   ☐ Find the most entertaining websites on the topic.
   ☐ Copy and paste information from the first website you find.
   ☐ Critically evaluate the information you find and choose credible sources.
   ☐ Only use information from printed books and encyclopedias.

8. **The digital divide refers to the gap between:**
   ☐ Different age groups using technology
   ☐ People with and without access to technology
   ☐ Those who prefer social media and those who don't
   ☐ Rich and poor countries' online infrastructure

9. **What is digital security, and why is it important in today's digital age?**
   ☐ Digital security involves protecting online identity, data, and assets from malicious activities.
   ☐ Digital security refers to protecting physical assets from theft.
   ☐ Digital security focuses on securing social media accounts.
   ☐ Digital security is not essential in today's digital landscape.

10. **Which of the following is NOT a type of malware?**
    ☐ Phishing
    ☐ Trojan Virus

☐ Ransomware
☐ Spyware

11. What is social engineering, and how does it contribute to digital threats?

☐ Social engineering involves securing online accounts through advanced encryption techniques.
☐ Social engineering is a legitimate method for resolving conflicts on social media.
☐ Social engineering exploits human psychology to manipulate individuals into revealing sensitive information or performing actions.
☐ Social engineering has no relation to digital security.

12. What is the difference between fake news, disinformation, and misinformation?

☐ They are all interchangeable terms with the same meaning.
☐ Fake news is fabricated stories presented as factual news, disinformation involves spreading false information with malicious intent, and misinformation refersto the unintentional sharing of false information.
☐ Fake news refers to exaggerated headlines, disinformation involves propaganda, and misinformation is accidental sharing of false information.
☐ Disinformation and misinformation are the same, while fake news is any news that is unpopular.

13. What constitutes a digital footprint, and why is it significant?

☐ A digital footprint consists of physical marks left on digital devices.
☐ A digital footprint encompasses all online activities and interactions, and it's significant because it can affect privacy, security, and reputation.
☐ A digital footprint refers to printed documents related to online activities.
☐ A digital footprint is not important in today's digital age.

14. What is the main purpose of Republic Act No. 10175, also known as the Cybercrime Prevention Act of 2012 (Republic Act No. 10175, signed into law on September 12, 2012, and upheld by the Supreme Court in 2014)?

☐ To regulate the use of computers and the internet.
☐ To prevent individuals from accessing the internet.
☐ To provide legal protection for cybercriminals.
☐ To protect data privacy and integrity.

15. **Who are the primary law enforcement agencies tasked with handling cases involving violations of the Cybercrime Prevention Act of 2012 (Republic Act No. 10175, signed into law on September 12, 2012, and upheld by the Supreme Court in 2014) in the Philippines?**

    ☐ Department of Justice (DOJ) and Philippine National Police (PNP)
    ☐ National Bureau of Investigation (NBI) and Philippine National Police (PNP)
    ☐ Department of Justice (DOJ) and National Bureau of Investigation (NBI)
    ☐ Cybercrime Prevention Division (CPD) and Philippine National Police (PNP)

16. **What are some reasons why the Philippines has become a hotspot for online child sexual exploitation according to the provided text?**
    ☐ Lack of internet access among Filipino adults.
    ☐ High level of education and awareness among Filipino families.
    ☐ Endemic poverty facilitates a surge in abuse, with parents and relatives often facilitating the exploitation.
    ☐ Strict enforcement of cybercrime laws by law enforcement agencies.

17. **What is the primary purpose of the Anti-OSAEC and Anti-CSAEM Law (Republic Act No. 11930, lapsed into law on July 30, 2022 and took effect on August 14, 2022) (RA No. 11861)?**
    ☐ To regulate internet access for minors in the Philippines
    ☐ To protect children from online sexual abuse and exploitation and child sexual abuse or exploitation material
    ☐ To monitor social media platforms for offensive language
    ☐ To provide financial aid to victims of cyberbullying

18. **What is the main purpose of practicing digital well-being?**
    ☐ To completely eliminate the use of digital devices
    ☐ To prioritize self-control and use technology intentionally
    ☐ To stay connected with friends and family online at all times
    ☐ To use digital devices for entertainment purposes only

19. **What should you do if you suspect a friend is engaging in cyberbullying behavior?**
    ☐ Ignore the situation and hope it resolves on its own
    ☐ Confront your friend publicly to shame them

☐ Have a private conversation expressing your concerns
☐ Join in on the cyberbullying to avoid conflict with your friend

20. If you are concerned that a friend may be struggling with gaming addiction, what is the BEST course of action?

☐ Avoid talking to them about it altogether.
☐ Confiscate their gaming devices and limit their internet access.
☐ Have a calm and open conversation about your concerns.
☐ Threaten to tell their parents if they don't cut back on gaming.

21. What is artificial intelligence (AI)?

☐ Computer systems that can perform complex tasks previously only possible for humans
☐ Computer systems that can perform only simple tasks
☐ Computer systems that are incapable of learning from data
☐ Computer systems that can only perform tasks with human intervention

22. What is the primary goal of the UNESCO Recommendation on the Ethics of Artificial Intelligence?

☐ Promotion of technological advancement without restrictions
☐ Protection of human rights and dignity in AI development and deployment
☐ Facilitation of unrestricted AI use in legal systems
☐ Advancement of AI technologies at the expense of environmental concerns

23. What does the bystander effect refer to in the context of online behavior?

☐ The tendency of individuals to intervene in online conflicts
☐ The hesitancy of individuals to intervene or speak up against online threats
☐ The immediate response of individuals to report online harassment
☐ The proactive involvement of individuals in online discussions

24. How can digital responsibility champions empower others to be responsible digital citizens?

☐ By telling them what to do
☐ By punishing them for bad online behavior
☐ By controlling their online activity
☐ By sharing resources and tips

25. Which of the following is an example of setting a good example of digital responsibility?

- ☐ Sharing personal information about someone else online without their permission
- ☐ Participating in cyberbullying or online harassment
- ☐ Spending all your free time playing online games
- ☐ Critically evaluating the source of information before sharing it online

Answer key		
1. B	11. C	21. A
2. B	12. B	22. B
3. A	13. B	23. B
4. B	14. D	24. D
5. B	15. B	25. D
6. A	16. C	
7. C	17. B	
8. B	18. B	
9. A	19. C	
10. A	20. C	

➤ MODULE 1
Navigating the Digital World

MODULE OVERVIEW:

This module provides an introductory exploration of the digital world and the principles of digital citizenship. Learners will delve into the impact of the digital landscape, understand the concept of digital citizenship, and develop skills for responsible online engagement. In this module, we will learn about the basics of the digital world.

MODULE OBJECTIVES:

In this module, we will be able to:

- Describe the pillars of the digital world and the components of the digital landscape.
- Identify the opportunities and challenges presented by digital technology.
- Explain how children are engaged and exposed to the digital world.

SUB-TOPICS:

- Overview of the Digital World and Landscape
- Benefits and Challenges of the Digital World
- Children in the Digital World

Materials Needed: sticky notes, markers, masking tapes, paper, markers, projector and screen, handouts, internet-enabled devices.

Topic	Activity	Description	Duration
Pre-Activity	Introduction to the Module	Overview of the module, setting expectations, and engaging participants in a discussion about their experiences with the digital world.	10 mins
	Pre-Activity 1: DigiPedia	A brainstorming activity where participants list and categorize digital concepts to establish a shared understanding of the digital world.	20 mins
Overview of the Digital World	**Activity 1.1:** It's a Match!	An interactive matching game where participants pair digital terms with their correct definitions to build foundational knowledge.	20 mins
	Discussion	A guided discussion on how digital technology influences communication, work, and everyday interactions.	20 mins
	Activity 1.2: Let's Connect	Participants visually map out different digital platforms, tools, and technologies, identifying how they interact and impact each other.	30 mins

Topic	Activity	Description	Duration
Benefits and Challenges of the Digital World	**Activity 1.3:** Social Media Carousel	A creative group activity where participants design mini-posters to highlight both the benefits and challenges of digital technology.	50 mins
	Discussion	An exploration of digital accessibility, security, misinformation, and the evolving digital landscape.	20 mins
Children in the Digital World	**Activity 1.4:** Digital Scavenger Hunt	A research-based activity where participants gather facts and figures about children's experiences in the digital world, analyzing both opportunities and risks.	50 mins
	Discussion	A reflective discussion on how digital platforms shape children's learning, socialization, and well-being, with a focus on protection and empowerment.	20 mins
		ESTIMATED TOTAL HOURS	4 hours

➤ Pre-Activity 1. DigiPedia: What we know about the Digital World

Before logging into the concepts of the digital world and digital citizenship, let's take a moment to reflect on our current understanding of the topic. This activity will allow us to share our knowledge and insights about the digital landscape and citizenship.

INSTRUCTIONS:

1. Reflect on your current understanding of the digital world. Consider what you already know, your experiences with technology and social media, and any ideas or thoughts about the topic.
2. Using the provided sticky notes and markers, write down key concepts and terms related to the digital world. What are some of the key words or phrases that come to mind when you think of the "digital world"? There are no right or wrong answers your notes, take a moment to read what others have shared and consider any similarities or differences in your responses.
3. With your learning facilitator, your notes will be explored and discussed, citing any similarities and differences. Some of you may be asked to explain or provide context for your notes briefly.
4. After reviewing the DigiPedia board, what are the most frequently mentioned words or phrases? Why do you think these concepts are so prominent in our understanding of the digital world? Conversely, are there any words or ideas that appear less often, but you believe they are important to consider in the bigger picture? Why?

OVERVIEW OF THE DIGITAL WORLD

Digital technology has become integral to our daily lives in our modern, interconnected society. Whether scrolling through social media feeds, communicating via online platforms, or even texting, our interactions with the digital world are constant and extensive. It has reshaped the world around us profoundly, influencing everything from how we work and communicate to how we perceive reality.

TERMS IN THE DIGITAL WORLD

➤ Activity 1.1 It's a Match

For this activity, we will explore key terms and concepts that shape our online experiences. From cyberbullying to digital citizenship, each term plays a vital role in understanding the digital world we navigate daily. By matching these terms with their corresponding definitions or descriptions, you'll test your knowledge and better understand how digital technologies impact our lives.

INSTRUCTIONS:

1. Each of you will receive a card with a digital term or description.
2. Your task is to match the digital term with its correct definition or description.
3. Take your time to review the terms and definitions before making your matches.
4. We'll review the correct answers together once everyone has made their matches.

cyberbullying	cybersecurity	data privacy	digital citizenship
digital divide	digital footprint	digital literacy	digital rights
digital world	internet	internet of things (IoT)	online etiquet
online identity	online safety	social media	

TERMS	DESCRIPTIONS
	A. The responsible and ethical use of digital technologies, encompassing behaviors, rights, and responsibilities in the digital environment.
	B. Measures and precautions taken to protect oneself from online threats, including cyberbullying, identity theft, and online scams.
	C. Protecting personal and sensitive information collected, stored, or transmitted online, ensuring compliance with privacy laws and regulations.
	D. The gap between individuals or communities with access to digital technologies and those without.
	E. The digital representation of an individual's persona or presence on the internet, including usernames, profiles, and online personas.
	F. Refers to a vast network of interconnected devices and objects that communicate with each other over the internet, often embedded with sensors and actuators that can collect and exchange data without human intervention.
	G. Guidelines and norms governing polite and respectful behavior in digital communications and interactions, also known as netiquette.
	H. Online platforms and websites that allow users to create, share, and interact with content for social connections and engagement.
	I. Refers to the network of digital technologies, including the internet, computers, smartphones, and other electronic and digital devices that facilitate communication, information processing, and sharing.

TERMS	*DESCRIPTIONS*
	J. The ability to effectively access, evaluate, and utilize digital information and technologies, including internet navigation, information retrieval, and digital communication skills.
	K. The use of digital technologies, such as social media, email, or text messages, to harass, intimidate, or bully others online.
	L. Practices aimed at safeguarding digital systems, networks, and data from cyber threats like hacking and malware.
	M. The rights and freedoms of individuals in the digital realm, including freedom of speech, privacy rights, and access to information.
	N. The trail of digital data left behind by an individual's online activities, including social media posts, search history, and online purchases.
	O. A global network of interconnected computers and servers that enables data transmission and exchange.

ANSWER KEY:		
A. Digital Citizenship	*F. Internet of Things (Iot)*	*K. Cyberbullying*
B. Online Safety	*G. Online etiquette*	*L. Cybersecurity*
C. Data Privacy	*H. Social Media*	*M. Digital Rights*
D. Digital Divide	*I. Digital World*	*N. Digital Footprint*
E. Online Identity	*J. Digital Literacy*	*O. Internet*

The digital world encompasses a vast ecosystem of interconnected technologies, platforms, and data. With its diverse range of technologies and innovations, the digital world has significantly altered how we communicate, work, learn, interact, and live.

THE PILLARS OF THE DIGITAL WORLD

These pillars represent the foundational elements underpinning the digital world's functioning and development. Connectivity, data, and devices are the fundamental pillars of the digital world, driving innovation, connectivity, and transformation across various sectors and industries.

- **Connectivity:** The internet and high-speed networks revolutionize information sharing and collaboration. Connectivity revolutionizes how individuals, organizations, and systems interact, allowing for real-time exchange of data and seamless integration of digital technologies into various aspects of our lives. The internet fuels learning with online resources, fosters social connections with friends and family, and provides endless entertainment.

- **Data: Data** is the lifeblood of the digital world, encompassing all the information generated, collected, and processed by digital systems and devices. Data fuels advancements in various fields, including healthcare, finance, marketing, and entertainment, driving innovation and improving decision-making processes. Innovations in data analytics, machine learning, and artificial intelligence (AI) technologies leverage large volumes of data to uncover patterns, make predictions, and derive actionable insights.

- **Devices:** Smart devices, such as smartphones, tablets, wearables, and IoT (Internet of Things), interface between users and the digital world. These devices enable individuals to access online services, applications, and content, transforming how we communicate, work, and interact with our environment. They empower users with instant access to information, communication tools, entertainment options, and productivity-enhancing features, shaping how we live and interact with technology. From educational apps to video calls with loved ones, devices offer learning opportunities and creative outlets.

➤ Checkpoint Question 1.1: How does the digital world impact your daily life, and why is it important to you?

The digital world, with its endless possibilities, has become an integral part of a child's life. Let's explore how the three key pillars - connectivity, data, and devices - shape a child's daily experiences:

1. CONNECTIVITY

1. With connectivity, you can access a vast library of online resources, from educational websites to interactive games.
2. Connectivity allows you to stay in touch through video calls and messages, fostering bonds despite the distance.
3. Rain or shine, there's always something fun to do online. You can enjoy playing educational games with friends, or watch age-appropriate shows on streaming services. (Remember, parental guidance is important!)

2. DATA

1. Data plays a role in your learning apps. These apps can adapt to your learning pace, focusing on areas needing improvement.
2. Parental control apps leverage data to filter out inappropriate websites, keeping you safe from harmful content.
3. You might see ads for the games you like based on your online activity.

3. DEVICES

1. You can use tablets to access educational apps and ebooks, turning any waiting room into a learning space.
2. To talk to your loved ones, you can use your phone coupled with headsets to update each other of important life events.
3. You can use a drawing pad to create colorful sketches.

These are just a few examples. The digital world offers a vast playground for children to learn, connect, and create. For parents and caregivers, it's important to be aware of both the benefits and challenges, ensuring a safe and positive online experience for the children.

The digital landscape is the term used to describe the spaces and networks created by technological developments and digital infrastructure, as well as the role of stakeholders in these areas. It refers to the interconnected ecosystem of digital platforms, tools, and technologies that shape our modern society's online experiences. This includes websites, email systems, social networks, mobile applications, video-sharing platforms, and other digital mediums facilitating communication, information exchange, and collaboration.

➤ Activity 1.2. Let's Connect: Exploring the Digital Landscape

The digital landscape is vast and interconnected, with various components shaping our online experiences. In this activity, you'll visualize the multiple components of the digital landscape and explore how they interact.

INSTRUCTIONS:

- Grab a piece of paper and a marker. Write down one component of the digital landscape in your paper. For example, you could write websites, social networks, mobile devices, etc.
- One learner will come to the front of the room and stand with their paper visible to the group.
- Connect with the learner by standing beside or around him at the front if you believe your component interacts with the one written on their paper.
- Selected learners will explain how their component interacts with the one written on the front learner's paper.

BENEFITS AND CHALLENGES OF THE DIGITAL WORLD

➤ Activity 1.3 . Social Media Carousel: Pros and Cons of the Digital World

Let us think about how the digital world has affected our lives. In how things work, there are always at least two sides, whether creating opportunities or posing challenges – the pros and the cons. In this activity, think about these pros and cons and show them creatively.

INSTRUCTIONS:

1. Form groups of 4-6 people. Each group will create a carousel of posters highlighting the digital world's pros and cons. You may opt to create a paper poster or digital poster depending on available resources and your preference.
2. For 10 minutes, brainstorm the key points you want to convey on each mini poster. What are the most essential pros and cons of the digital world that you want to highlight?
3. Design four mini-posters, focusing on a different aspect of the digital world. Use markers, pens, and other supplies to make your posters visually appealing.
4. Each group will have three minutes to present their carousel, explaining the pros and cons highlighted in each mini poster.

EXPLORING THE BENEFITS OF THE DIGITAL WORLD

The digital world offers many benefits that shape how we live, work, and interact. It is vast and dynamic, constantly evolving to provide new opportunities and possibilities. This section will highlight some key benefits, including global connectivity, enhanced communication, access to information and education, efficiency and automation, and job opportunities. However, it's essential to remember that other benefits of the digital world may not be listed here.

1. **Global Connectivity:** Facilitates connections and cultural exchange on a global scale, fostering international collaboration and trade.

2. **Enhanced Communication:** The digital world has transformed communication through apps, social media, and video calls. It enables the rapid spread of new ideas.

3. **Access to Information and Education:** The digital era provides easy access to all information due to centralized and accessible data. It democratizes access to knowledge and learning resources, empowering individuals to acquire new skills and education regardless of geographical barriers.
4. **Efficiency and Automation:** Streamlines processes across industries, enhancing productivity and enabling humans to focus on tasks that require creativity and critical thinking.
5. **Job Opportunities:** Remote working facilitated by the internet has created new job roles, such as internet technology specialists. Individuals can also start their online businesses.

ADDRESSING CHALLENGES AND CONSIDERATIONS

As our society continues to grow with the complexities of our increasingly digital society, it's essential to recognize and tackle the various issues that arise. Let us explore some key challenges and potential solutions, focusing on the digital divide, cybersecurity, social impact, and more. It's important to note that while the list we'll discuss is comprehensive, it is not exhaustive. Many other challenges and solutions when we speak of the digital world are present, but our goal is to spark conversation and inspire action in addressing these critical issues.

Challenges and Considerations	Potential Action Areas for Young People
Digital Divide - recognizes the gap between those with access to digital technologies and those without.	Advocate for programs and initiatives that provide free or affordable internet access and devices to underserved communities. Volunteer with organizations that offer digital literacy training and support to marginalized groups, helping bridge the technological access gap.
Digital Crime - hackers and cyber threats exploit vulnerabilities, leading to financial losses or breaches.	Educate peers and community members about online safety practices, such as using strong passwords, enabling two-factor authentication, and avoiding phishing scams.

Challenges and Considerations	Potential Action Areas for Young People
Social Impact - easy communication can weaken real-life social skills and community bonds.	Organize offline events and activities that promote face-to-face interactions and strengthen community ties, such as group outings, volunteer projects, or hobby clubs. Lead by example by practicing mindful technology use, setting boundaries for screen time, and prioritizing in-person connections with friends and family.
Information Misuse - easy access to information increases the chance of misuse, such as spreading false information.	Participate in media literacy workshops and initiatives to develop critical thinking skills and discern credible sources of information. Create and share content that promotes fact-checking, critical analysis, and responsible information sharing on social media platforms and online communities.
Cybersecurity and Privacy - protecting personal data and preventing unauthorized access to sensitive information.	Stay informed about cybersecurity best practices and privacy settings on social media platforms and encourage peers to do the same. Advocate for stronger data protection laws and regulations by engaging with policymakers, signing petitions, and participating in advocacy campaigns focused on digital rights and privacy.

➤ Checkpoint Question 1.2. As digital technologies advance, what dilemmas and questions might young people encounter in their digital interactions and decision-making processes?

CHILDREN IN THE DIGITAL WORLD

Every day, children interact with the digital world. There might be circumstances in which access to digital technology is limited. Still, we cannot deny that the digital landscape has become a fundamental environment for children as they learn and develop. It offers benefits to children, opening ways for communication, creativity, and learning. With these benefits, it also presents serious risks, including cyberbullying, extortion, and risks to privacy. It is, therefore, more important than ever to establish the necessary conditions for a safer digital environment and provide children with the right digital skills to address the exacerbated risks it poses.

➤ Activity 1.4 Digital Scavenger Hunt: Fact and Figures of Children in the Digital World

In this activity, you will look up various facts and figures concerning children's experiences in the digital world. Through this scavenger hunt, you can conduct research, verify information, and deepen your understanding of key issues related to children's digital experiences.

INSTRUCTIONS:

1. Gather into teams of 3-5 members. Each team will work together to complete the scavenger hunt. Within each team, assign roles such as researcher, fact-checker, recorder, etc. You can strategize how to divide tasks.
2. Use your digital devices to search online for facts and figures on children in the digital world. Navigate various websites, digital resources, and online databases to find accurate information. Select at least 3 facts and figures.
3. As you find relevant facts and figures, record your findings and cite the sources you used to verify the information. Take notes and screenshots as needed to document your research.
4. Share this with the group during the open discussion.

With children's exposure to the digital world, they have also become vulnerable to the harms it may bring. The internet lets predators reach them anywhere, making harmful content easier to create and share. Also, massive data processing can threaten their privacy without them knowing. Online risks affect every child, making it simple for bullies, predators, and others to target them. Since 2012, about 100 million children worldwide, the majority from Africa and Southeast Asia, have connected to the internet for the first time (UNICEF, 2017). Lacking adequate protection, the world's most vulnerable children will be at even higher risk when navigating the digital world.

The Philippines has a high mobile and internet penetration rate. Philippine Statistics Authority (PSA) reported in 2020 that more than half of the total households had internet access. According to a 2019 study by TotallyAwesome, 84% of Filipino kids choose the internet over television. This high level of connectivity increases exposure to both the benefits and risks of the digital world.

The United Nations International Children's Emergency Fund (UNICEF) published The State of the World's Children – Children in a Digital World in 2017. In the report, some opportunities for children are presented:

1. Digital technology has vast potential to enhance education, but addressing educational challenges requires more than technology.
2. Connected children and youth express their voices through various digital mediums like blogs, videos, social media, and podcasts.
3. The digital economy creates new markets and job opportunities, benefiting youth lacking specialized skills.
4. Digital technologies are crucial in assisting vulnerable groups, such as children, in humanitarian crises.

With the promise of connectivity that the digital world presents to the youth, there are also missed opportunities. In the same UNICEF report mentioned above, some digital divides affect children:

1. Basic internet connectivity remains challenging for children in the poorest countries and rural areas.
2. Various factors, including education, user skills, device type, and access to local language content, influence how children utilize the internet, shaping their online activities and opportunities.
3. Unconnected children miss educational resources, global information, and opportunities to develop digital skills, friendships, and self-expression online.
4. Connectivity in the digital age is becoming increasingly vital for children transitioning into adulthood and the workforce.

Children's presence in the digital world has expanded significantly, with technology becoming integral to their daily lives. As children navigate the digital landscape, it's crucial to understand its impact on their development, behavior, and well-being.

➤ CHECKPOINT QUESTION 1.3. How can we ensure that all children can safely and effectively navigate the digital landscape while maximizing its benefits for their development and well-being?

The Organization for Economic Cooperation and Development (OECD) has recommended principles for ensuring a safe and beneficial digital environment for children. The principles are directed towards various actors involved in children's participation in the digital world, emphasizing the importance of upholding children's best interests and protecting their rights. These principles are:

1. **Fundamental Values** – actors should prioritize children's best interests and protect their rights in the digital world.
2. **Empowerment and Resilience** – steps should be taken to help children and caregivers understand their rights, manage risks, and access support services. Children should feel empowered to express themselves and participate in digital issues.
3. **Proportionality and Respect for Human Rights** – protective measures should be balanced, based on evidence, and effective while respecting children's freedom of expression and other rights.
4. **Appropriateness and Inclusion** – actors should consider children's diverse needs and ensure no child is left more vulnerable due to factors like lack of digital access or inadequate digital literacy.
5. **Shared Responsibility, Cooperation, and Positive Engagement** – stakeholders should collaborate, engage in dialogue, and cooperate to create a safe digital environment. Parents, guardians, caregivers, and educators should guide children to be responsible digital users.

The digital world has become an integral part of our daily lives, shaping how we communicate, work, learn, and interact with the world around us. Digital technologies offer connectivity, collaboration, and innovation opportunities, from social media platforms to online learning resources. However, with these opportunities come challenges and responsibilities. It's essential for individuals, especially young people, to develop an understanding of the digital world, including its benefits and risks.

➤ MODULE 2
Practicing Digital Rights and Responsibilities

MODULE OVERVIEW:

As digital citizens, it's crucial to understand our rights and responsibilities in the online world, ensuring that we contribute positively to digital communities. Through interactive discussions and practical exercises, we will explore various topics related to digital citizenship, netiquette, and responsible online behavior to help us navigate digital environments confidently and responsibly.

MODULE OBJECTIVES:

At the end of this module, the learners can:

- Enumerate one's digital rights and responsibilities.
- Display responsible online behavior and proper netiquette when interacting with social media and other digital platforms.
- Demonstrate responsible and ethical behavior in digital environments.

SUB-TOPICS:

1. Becoming a Digital Citizen
2. Digital Rights and Digital Responsibilities
3. Common 'Netiquettes' and Responsible Use of Social Media

Materials Needed: sticky notes, markers, masking tape, paper, printed scenario cards, discussion prompts, whiteboard markers, projector and screen, internet-enabled devices

Topic	Activity	Description	Duration
Pre-Activity	Introduction to the Module	Overview of the module, setting expectations, and engaging participants in a discussion about their experiences with the digital world.	10 mins
	Pre-Activity 2: Sorting Challenge	A hands-on activity where participants sort statement cards into "Right" or "Responsibility" categories to distinguish digital entitlements from obligations.	20 mins
Becoming a Digital Citizen	Discussion	A guided discussion exploring the nine elements of digital citizenship (access, commerce, communication, literacy, etiquette, law, rights/ responsibilities, well-being, security) as detailed in the document.	20 mins
Digital Rights and Responsibilities	Activity 2.1: My Right, My Responsibility	An interactive role-play where groups analyze real-life digital dilemmas and deliberate on ethical choices, demonstrating how to balance digital rights with corresponding responsibilities.	60 mins
	Discussion	A comprehensive discussion reviewing the core digital rights (e.g., access, privacy, expression) and responsibilities (e.g., respectful communication, data protection), along with an exploration of how the Ten Rights of a Child translate to digital contexts.	30 mins

Topic	Activity	Description	Duration
Common Netiquettes and Responsible Use of Social Media	Discussion	A focused discussion on the ten netiquette guidelines that underscore best practices for respectful and effective online communication.	20 mins
	Activity 2.2 Red Flag or Green Flag	An evaluative activity where participants review online behavior scenarios and classify them as "Red Flag" (violating netiquette), or "Green Flag" (appropriate) reinforcing standards for digital conduct.	30 mins
	Discussion	A discussion that examines the role and impact of social media in daily life by reviewing usage statistics and exploring how digital platforms influence youth and society, emphasizing mindful and responsible engagement.	30 mins
	Activity 2.3: I Spy	A self-reflection activity where participants analyze their own social media feeds to identify recurring behavioral patterns and pinpoint areas for improvement in their online interactions.	30 mins
	Discussion	A discussion that reviews key principles for responsible digital and social media use focusing on verification, respect for privacy, digital literacy, and ethical engagement to reinforce a safe and inclusive online environment.	20 mins
		ESTIMATED TOTAL HOURS	**4 hours and 30 mins**

➤ Pre-Activity 2. Sorting Challenge: Right vs Responsibility

In this activity, you will be presented with a list of statements related to rights and responsibilities. Your task is determining whether each statement describes a right or a responsibility. This activity will help you understand the distinction between these two concepts before exploring their application in the digital world. Here are some questions to help you decide:

1. Does the statement describe something you are entitled to have or do?
2. Does the statement describe an action you should take?
3. Does the statement contribute to the well-being of yourself or others?

STATEMENTS:

1. Honoring contractual agreements. (Responsibility)
2. Freedom of speech. (Right)
3. Access to information. (Right)
4. Respecting authority figures. (Responsibility)
5. Following laws and regulations. (Responsibility)
6. Equal treatment under the law. (Right)
7. Respecting others. (Responsibility)
8. Ownership of property. (Right)
9. Practicing one's religion. (Right)
10. A fair trial. (Right)
11. Privacy. (Right)
12. Protecting the environment. (Responsibility)

BECOMING A DIGITAL CITIZEN

Since we live in the digital world, we have become digital citizens. But what is digital citizenship? Digital citizenship is the ability to access digital technologies and stay safe (Halfpenny). A digital citizen is an individual who cultivates the necessary skills and knowledge to navigate the vast landscape of the internet and digital technologies. Being a responsible digital citizen has become increasingly important in today's digital age. As technology evolves, so do the skills and knowledge required to navigate the digital landscape effectively.

NINE ELEMENTS OF DIGITAL CITIZENSHIP

1. **Digital Access** – means having the tools and internet connection needed to use technology. For young people, this ensures they can access educational resources, stay connected with friends and family, and explore opportunities for personal growth online.
2. **Digital Commerce** – involves the online buying and selling of goods and services. Learning about e-commerce helps young people make informed decisions about spending and saving money, preparing them for financial independence in the future.
3. **Digital Communication** – covers how we interact with others online. Teaching young people about digital communication helps them build relationships, express themselves, and collaborate effectively in virtual spaces.
4. **Digital Literacy** – is about effectively understanding and using digital information. For youth, this means learning to evaluate online sources, identify misinformation, and conduct research online.
5. **Digital Etiquette** – is about using technology respectfully and responsibly. Teaching youth about digital etiquette helps them navigate online interactions with kindness and respect, preventing cyberbullying and maintaining positive online reputations.
6. **Digital Law** – involves understanding the rules and regulations governing technology use. For young people, this includes knowing their rights online and how to protect their privacy and security.
7. **Digital Rights and Responsibilities:** Digital rights are the privileges of being online, like freedom of expression, while responsibilities are the duties that come with it, such as respecting others' rights and practicing online safety.
8. **Digital Well-being** – focuses on maintaining well-being in the digital age. Educating young people about digital health helps them develop healthy habits and manage digital stress.
9. **Digital Security** – protects personal information and devices from online threats. Teaching youth about digital security empowers them to stay safe online and protect themselves from cyberattacks.

Effectively, anyone who uses digital technology can be considered a digital citizen, regardless of age, background, or level of expertise. However, being a good digital citizen entails more than mere technological proficiency. It involves being well-informed about the potential risks and challenges associated with digital technologies and actively engaging in efforts to mitigate these issues.

➤ Checkpoint Question 2.1: What actions do you plan to take to demonstrate responsible and ethical behavior in digital environments?

DIGITAL RIGHTS AND RESPONSIBILITIES

In the digital world, people have rights and responsibilities online, much like in real life. Rights are things you are entitled to as a person. They are freedoms and protections that ensure your well-being and allow you to live your life according to your values. Responsibilities are the duties and obligations you have towards yourself, others, and your environment. They are the actions you take to contribute to a functioning society. Digital rights are about the freedoms and entitlements people have online, like privacy and expression. On the other hand, digital responsibilities involve behaving ethically and respectfully online to create a safe and positive online environment. Understanding these concepts helps us navigate the digital world more responsibly and effectively.

➤ Activity 2.1. My Right, My Responsibility!

This activity aims to discuss and analyze real-life scenarios related to digital rights and responsibilities. You will explore various situations and reflect on ethical decision-making and responsible behavior in digital environments.

INSTRUCTIONS:

1. Form five (5) groups. Each group will be presented with a scenario involving digital rights and responsibilities. These scenarios will cover a range of situations, such as privacy concerns, online communication, intellectual property, and cybersecurity.

Scenario 1: Sarah found a USB drive containing personal documents and photos. She wants to access the files to see if she can identify the owner and return it. What are the digital rights and responsibilities involved? How should Sarah proceed?

Scenario 2: John received a forwarded message on social media claiming to offer free gift cards in exchange for personal information. He is tempted to participate but is unsure about the offer's legitimacy. What should John consider before taking any action?

Scenario 3: Alex accidentally shared a private email with sensitive information to a large group of recipients, including people who were not intended to see the content. What steps should Alex take to rectify the situation and uphold digital responsibilities?

Scenario 4: Emily witnessed her friend being cyberbullied in an online gaming community. She wants to intervene but is unsure about the best approach. What are Emily's digital rights and responsibilities in this situation? How can she support her friend while promoting a positive online environment?

Scenario 5: David created a digital artwork and posted it online. Shortly after, he discovered that someone else had copied his artwork without permission and claimed it as theirs. How can David protect his intellectual property rights and address the issue responsibly?

2. Within your group, discuss your scenario thoroughly. Consider the rights and responsibilities, ethical considerations, and potential consequences of different actions. After discussing your scenario, collaboratively decide on the most ethical and responsible course of action.

3. Each group will role-play their chosen course of action for the given scenario using the provided questions.

YOUR RIGHTS AND RESPONSIBILITIES

Becoming a digital citizen is knowing and exercising your rights and ensuring that your digital responsibilities are also fulfilled. As a digital citizen, you have the right to:

1. access and use computers and electronic devices,
2. access and use digital content,
3. create, share, and express ideas and opinions freely in digital communities,
4. privacy, data protection, and anonymity online,
5. report inappropriate content or behavior,
6. access the digital world and its resources securely, and
7. control personal data, including informed consent and the right to be forgotten.

As a digital citizen, you have the responsibility to:

1. communicate respectfully and use appropriate language and behavior when interacting online,
2. respect intellectual property laws and others' rights to their work,
3. follow rules and codes of conduct on digital platforms,
4. report cyberbullying, threats, and misuse of digital resources,
5. decline to share false information,
6. protect personal and private information, including logins and passwords, and
7. safeguard digital systems and networks against unauthorized access or misuse.

While the above list outlines common digital rights and responsibilities, there is no fixed or exhaustive list. As technology evolves and digital environments continue to change, new rights and responsibilities may emerge. Even with the current digital environment, there may be other rights and responsibilities listed in other references. As digital citizens, it's crucial to constantly reflect on our actions and decisions in the online world. We must consider the ethical implications of our behaviors and strive to uphold principles of respect, integrity, and accountability. By staying informed, engaging critically, and fostering a culture of empathy and responsibility, we can navigate the complexities of the digital landscape while contributing positively to online communities and promoting a safe and inclusive digital environment for all.

➤ Checkpoint Question 2.2 When it comes to what's right and wrong online, who should be responsible for setting the rules and making sure people follow them? Should it be the online platforms, or should it be up to each individual user?

Ten Rights of a Child viewed through the Digital World

Children have certain rights that are inherent and must be respected by everyone. As children are the future, their well-being should be of utmost importance. These rights include basic necessities for survival and development, as well as the ability to express themselves and live in a safe and peaceful environment. The following ten rights are the fundamental needs and freedoms that every child deserves in order to reach their full potential:

1. To be born, to have a name and a nationality.
2. To be free, to have a family who will take care of them.
3. To have a good education.

4. To develop their potential.
5. To have enough food, shelter, and a healthy and active body.
6. To be given the opportunity for play and leisure.
7. To be given protection against child abuse, danger and violence brought by war and conflict.
8. To live in a peaceful community.
9. To be defended and assisted by the government.
10. To be able to express their own views.

Looking at these rights, they should also be observed and respected in the digital world, since children themselves are also digital citizens. Here's how the 10 rights of a child translate to the digital world:

Rights of a Child	Application in the Digital World
To be born, to have a name and a nationality	This translates to having a safe online identity. This may not involve a legal name, but it means having control over the information they share online and being protected from exploitation.
To be free, to have a family who will take care of them	This translates to freedom from online dangers and harassment. It involves promoting a supportive family environment that educates children about safe internet usage and monitors their online interactions.
To have a good education	This includes access to quality educational resources online and the ability to critically evaluate online information. Ensuring children have access to educational platforms, digital libraries, and online learning tools is crucial for their development.
To develop their potentials	The digital world offers many tools and platforms for children to develop potential. This right involves fostering a supportive online environment that encourages creativity, innovation, and personal growth.
To enough food, shelter, and a healthy and active body	This can connect to awareness campaigns about online dangers like cyberbullying or addiction to online games that can affect a child's well-being. It can also encompass access to reliable internet connectivity, devices, and digital literacy resources. It ensures children have the

Rights of a Child	Application in the Digital World
To be given opportunity for play and leisure	This right extends to digital play and entertainment. It involves providing children with access to age-appropriate online games, social platforms, and creative outlets that promote healthy digital leisure activities.
To be given protection against child abuse, danger and violence brought by war and conflict	This is a crucial right in the digital world. It includes protection from online predators, cyberbullying, and exposure to violent or inappropriate content.
To live in a peaceful community	This translates to promoting online civility and respect for others in online interactions and social media use. It also involves creating safe online spaces where children can interact without fear of discrimination or violence.
To be defended and assisted by the government.	Governments have a role to play in regulating online content, protecting children from online dangers, and promoting digital literacy. This includes legislation on data privacy, online safety, and child protection, as well as providing support services for victims of online abuse or exploitation.
To be able to express their own views.	This translates to the right to participate in online discussions in a safe and respectful environment, while also being aware of responsible online behavior.

➤ **Checkpoint Question 2.3. How do you think the rights of a child should be respected and protected in the digital world? Can you give examples of how some of these rights apply to your online experiences?**

COMMON 'NETIQUETTES' AND RESPONSIBLE USE OF SOCIAL MEDIA

As digital citizens, we have spent so much time online that it is important to consider how we behave. Netiquette (a combination of "net" and "etiquette"), or Internet Etiquette, refers to the proper way of conducting oneself while communicating online. As our digital world expands, it's crucial to understand how to interact respectfully in various online spaces. Practicing netiquette ensures positive online interactions and fosters a welcoming online community.

10 Netiquettes to Observe

1. **Remember there is a human on the other side:** Treat online interactions with the same respect and courtesy you would in face-to-face communication. Remember that behind every screen is a person with feelings and emotions.
2. **Apply your normal standards of behavior online:** Maintain the same standards of behavior and conduct in digital communication as you would in real-life interactions.
3. **Be aware of context and tailor your communication accordingly:** Understand the community standards and guidelines of the platform you're using and adapt your communication style accordingly.
4. **Respect others' time and bandwidth:** Avoid posting irrelevant or spammy content that may clutter others' feeds or waste their time. Avoid forwarding chain emails or sharing irrelevant content excessively.
5. **Avoid posting embarrassing or offensive content:** Be mindful of the content you share online and avoid posting anything that could be perceived as inappropriate, offensive, or unlawful.
6. **Share content from reliable sources and verify information:** Prioritize sharing information from credible and authoritative sources, and always verify the accuracy of information before sharing it to prevent the spread of misinformation and fake news.
7. **Respect human privacy:** Avoid invading others' privacy or sharing personal information without their consent. Respect the confidentiality of private conversations and messages.
8. **Represent yourself well:** Be mindful of the content you post online as it shapes others' perceptions of you. Avoid inflammatory or controversial content and maintain a positive online presence.
9. **Engage respectfully and constructively:** Steer clear of excessive trolling and flaming, which can escalate into heated and unproductive arguments.
10. **Cultivate empathy and forgiveness:** Recognize that people make mistakes and offer grace and forgiveness when misunderstandings or conflicts arise.

➤ Activity 2.2. Red Flag or Green Flag: Where's the Netiquette?

In this activity, we'll explore various scenarios you may encounter in your online interactions and evaluate them based on netiquette principles. As technology evolves and more people engage in digital communication, it's crucial to understand and follow netiquette guidelines to maintain positive and respectful interactions in virtual spaces. Through this activity, you'll have the opportunity to assess different situations critically and determine whether they adhere to netiquette standards.

Instructions: (Note that this can be converted into a online gamified version (like the use of Kahoot!, Slido, Mentimeter, Quizizz, or other tools)

1. Read each scenario provided carefully and consider the actions described in the context of netiquette principles.
2. Determine whether each scenario represents a "Red Flag" (violates netiquette principles) or a "Green Flag" (aligns with netiquette principles). If in doubt or you feel that it may not be Red or Green, you may use the "secret" flag which is the Yellow Flag to signify that you feel neutral, or the answer cannot be ascertained.

SCENARIOS

1. A student sends an email to a professor with a clear subject line, a courteous greeting (e.g., "Dear Professor Smith"), and a well-formulated question about an assignment. The email concludes with a thank-you and the student's signature.
2. On a public social media platform, a user responds to another person's opinion using insults, derogatory language, and personal attacks. The comment immediately escalates into a heated argument.
3. During an online group project, a team member posts a comprehensive update on a shared platform. The update summarizes recent progress, outlines next steps, thanks teammates for their contributions, and invites further feedback.
4. On an online forum, a user replies to a discussion thread by first acknowledging the original poster's viewpoint, then providing additional, verified information with links to credible sources.
5. A social media user comes across a sensational article with a provocative headline. Without reading the full content or verifying the source, they immediately share the article with their followers.

6. In a collaborative project, one team member logs into a shared document and makes significant content revisions. They delete several colleagues' comments and modify key sections without informing the rest of the group.
7. During a weekly video team meeting for an important business agenda, a participant spends several minutes sharing a personal story about their weekend challenges and personal struggles.

Answer Key:

1. Green Flag. The email treats the professor respectfully and mirrors face-to-face courtesy. The clear, professional communication represents the student well.
2. Red Flag. Using insults and personal attacks disregards the human element and fails to promote constructive dialogue. This behavior negatively impacts the user's online reputation.
3. Green Flag. The update is context-aware and keeps everyone informed while respecting colleagues' contributions.
4. Green Flag. The user supports their perspective with credible sources and encourages constructive discussion.
5. Red Flag. Failing to verify the source risks spreading misinformation.
6. Red Flag. Making unilateral changes and deleting colleagues' comments shows a lack of respect for collaborative input.
7. Red Flag. Spending excessive time on personal disclosure during a work meeting disrespects others' time and detracts from the meeting's purpose. The behavior fails to maintain the professional standards expected in a formal setting.

➤ Checkpoint Question 2.3 What other netiquette guidelines do you think are essential for maintaining positive online interactions and fostering a respectful digital community?

RESPONSIBLE USE OF SOCIAL MEDIA

Everywhere you go and everywhere you look, people from different walks of life stare down at a screen. More likely than not, these individuals are engrossed in scrolling through a social networking site or social media pages. The Oxford Reference defines social media as "websites and applications that enable users to create and share content or to participate in social networking." With a wide variety of options available for online social networking, ranging from Instagram and YouTube to TikTok and Facebook, it's evident that social media plays a significant role in our daily lives.

In the Philippines, social media has become integral to daily life, particularly among youth. Statistics reveal a significant presence of Filipinos on various social media platforms. With millions of users actively engaging online, platforms like Facebook continue to dominate the digital landscape.

1. SOCIAL MEDIA USAGE

- 82.4% of all Filipinos are active on social media platforms, with a significant concentration among the 20 million youth aged 15-24 years old. (Kyoto Review, 2022)
- 94% of Filipino youth use the internet or own a smartphone, highlighting their strong digital presence. (Kyoto Review, 2022)

2. AGE DISTRIBUTION ON SOCIAL MEDIA

- The largest proportion of social media users falls within the 18-24 age group, constituting 52.7% of the total user base. (Talkwalker, 2019)
- Runners-up include 25-34 year-olds (31%), followed by 13-17 year-olds (13.8%) and 35-44 year-olds (2.2%). (Talkwalker, 2019)

3. FACEBOOK DOMINANCE

- Facebook remains a dominant force in the Philippines. The number of Facebook users in the country is substantial, with millions actively engaging on the platform. (Statista, 2023)
- Among the youth, Facebook continues to be a popular choice for social interaction and content sharing. (Statista, 2023)

4. WEEKLY SOCIAL MEDIA USAGE BY CHILDREN

- Among children who utilize social media weekly, 97% fall within the 16-17 years age group. (Statista 2021)

- These young users primarily access social media from the comfort of their homes. (Statista 2021)

➤ Activity 2.3 I Spy: Looking at My Own Social Media

The objective of this activity is to conduct a review of your own social media content to observe and identify patterns of behavior. Analyze your social media activity and produce insights into the types of content you engage with.

INSTRUCTIONS:

1. Open your social media accounts and take a close look at the content that you share and engage with on social media. As you scroll through your feed, pay attention to the topics, language, and tone of the posts.
2. With the guide questions below, take notes and reflect on your observations as you scroll through your social media feed.

GUIDE QUESTIONS

1. Are there any specific recurring topics or themes in your posts and interactions?
2. What words and language do you typically use in your posts and comments? Are they positive, neutral, or negative in tone?
3. Do you come across any content that you would consider rude, shaming, flaming, or inappropriate? Why do you believe this content falls into that category?
4. How do you typically engage with content on social media? Are you active in promoting positive interactions and meaningful discussions?
5. Have you ever reacted impulsively or engaged in negative behavior online? What triggers these reactions?
6. Outline your key findings and observations with your social media feed. Are there areas where you can improve your online behavior and communication habits?
7. Based on your reflections, identify specific actions or strategies you can implement to promote positive engagement and responsible use of social media. Write one statement for your commitment, and everyone will be asked to say it out loud.

GENERAL GUIDE TO RESPONSIBILITY USE DIGITAL AND SOCIAL MEDIA PLATFORMS

As we immerse ourselves in social media platforms, it's essential to recognize the responsibility that comes with this digital interaction. Social media offers big potential for connecting with others, sharing experiences, and accessing valuable information. However, its misuse can lead to negative consequences, including cyberbullying, misinformation, and addiction. Therefore, it is crucial to navigate social media with mindfulness and responsibility to foster positive relationships and maximize its benefits. In using social media, we can keep in mind several principles to ensure responsible usage. These guidelines help individuals navigate the digital landscape responsibly.

1. **Verify and share thoughtfully** – before sharing any content, verify its accuracy and credibility. Be mindful of the potential impact of your posts on others and the broader community. Only share information that you have confirmed to be accurate and from reliable sources.
2. **Respect privacy and foster inclusivity** – respect the privacy of yourself and others by carefully managing your online presence and sharing only what you're comfortable with. Create an inclusive online environment by promoting respectful interactions, avoiding cyberbullying and harassment, and embracing diversity of opinions.
3. **Prioritize well-being and mindfulness** – take proactive steps to protect your mental health and well-being while using social media. Set boundaries for your usage, take breaks when needed, and curate your online experience to focus on content that uplifts and inspires you.
4. **Cultivate digital literacy** – develop digital literacy skills to critically evaluate information and navigate the online world effectively. Challenge biases, seek out diverse perspectives, and fact-check content before sharing it.
5. **Uphold integrity and responsibility** - act with integrity and responsibility in all your online interactions. Be accountable for your words and actions, understand the potential consequences of your online presence, and strive to contribute positively to the digital community.

➤ Checkpoint Question 2.4 What strategies do you believe are most effective in promoting responsible social media use among children and youth?

➤ MODULE 3
Ensuring Digital Safety and Security

MODULE OVERVIEW:

The digital world offers many opportunities for learning, communication, and entertainment, but it also comes with some risks and challenges. This module will explore how to ensure digital safety and security for us and others. We will learn about the common threats and dangers that we may encounter online and how to evaluate online content and interactions to spot fake news and disinformation. We will explore how to create a plan for a positive digital footprint and account security to protect our personal information and reputation online.

MODULE OBJECTIVES:

At the end of this module, the learners can:

- Identify the potential dangers of the digital world and the ways to mitigate/prevent them from happening.
- Evaluate online content and interactions to identify scams, identity theft, and other fraudulent activities.
- Differentiate legitimate online content and fake news.
- Create a plan for a positive digital footprint and account security.

SUB-TOPICS:

- Cybersecurity Threats
- Online Fraud: Digital Scams and Identity Theft
- False Information
- Digital Footprint

MATERIALS NEEDED:

swriting instruments, large paper or poster boards, colored pencils, crayons, markers, sticky notes, projector, screen, whiteboard/flipchart, timer/clock

Topic	Activity	Description	Duration
Pre-Activity	Introduction to the Module	Overview of the module, setting expectations, and introducing the importance of digital safety and security in today's online world.	10 mins
	Pre-Activity 3: Cybersecured!	A self-assessment activity where participants evaluate their cybersecurity practices using a checklist to identify strengths and vulnerabilities in their online behavior.	15 mins
Digital Threats and Safety	Discussion	A guided discussion exploring various digital threats such as malware, phishing, and social engineering, and outlining strategies to protect personal and sensitive information online.	20 mins
	Activity 3.1: Stop or Go	An interactive exercise where participants review online scenarios and decide whether each situation warrants a "STOP" (risky behavior) or a "GO" (safe practice) response, reinforcing key cybersecurity principles.	20 mins
	Discussion	A follow-up discussion that clarifies safe practices, reinforces key concepts from the simulation, and addresses any misconceptions regarding digital safety measures.	20 mins
Online Fraudulent Activities	Activity 3.2: Fraud Alert!	A creative group activity in which participants design a comic strip depicting scenarios of online scams and identity theft.	60 mins

Topic	Activity	Description	Duration
	Discussion	A comprehensive discussion that examines various online scams, methods of identity theft, and practical measures to prevent fraud, drawing on real-world examples to emphasize vigilance and proactive security.	30 mins
False Information	Discussion	An introductory discussion on the concepts of fake news, disinformation, and misinformation, exploring their origins, impacts, and how to critically assess online content.	15 mins
	Activity 3.3: Fact or Fiction	An evaluative group activity where participants analyze online articles and social media posts to determine which pieces of information are factual and which are misleading.	30 mins
	Discussion	A focused discussion on the various forms of false information (e.g., clickbait, propaganda, manipulated content) and practical tips for identifying and verifying the authenticity of online content.	20 mins
Digital Footprint	Discussion	An exploration of digital footprints, differentiating between active (intentional sharing) and passive (unintentional data collection) footprints, and discussing their impact on privacy and reputation.	10 mins

Topic	Activity	Description	Duration
	Activity 3.4: My Online Trail	An interactive group activity where participants map out a fictional digital footprint using sticky notes, identifying key online activities and brainstorming strategies to secure and manage their digital presence.	30 mins
	Discussion	A practical discussion on how to monitor, manage, and secure one's digital footprint, supported by real-life examples, to safeguard personal information and enhance online reputation.	20 mins
	Activity 3.5: Docufilm Analysis	An analytical activity where participants watch the documentary "The Power of Privacy," which explores the challenges and opportunities of digital privacy in the 21st century.	60 mins
		ESTIMATED TOTAL HOURS	**6 hours**

➤ Pre-Activity 3. Cybersecured!

To ensure you are following the best practices for cybersecurity, you will complete a self-assessment checklist in this activity. The checklist will help you identify any areas where you need to improve your security measures. You will mark each item on the checklist as done or not done. This checklist is based on the California State University San Bernardino cybersecurity checklist.

Security Measure	Am I doing this?	If not, how can i observe this as a cybersecurity behavior
I use multifactor or two-factor authentication whenever possible for accounts with sensitive data.		
I use anti-virus & anti-malware software.		
I choose strong passwords.		
I use a password-protected screen saver in my devices.		
I update all software and operating systems on my computers and mobile devices.		
I never provide passwords or other sensitive information in response to an email or enter them on an untrusted site.		
I never respond with personal information nor open attachments from unexpected emails or unsolicited phone calls.		
I follow appropriate procedures and/or seek independent counsel when unexpected or unusual requests come through.		
I clear my private data from Web browsers.		
Never save passwords in a Web browser.		
I only download software from reputable sources.		
My firewall is turned on.		
I back up important files to a secure location and delete the files I no longer need.		
I don't store sensitive data on USB drives.		

After completing the self-assessment checklist for cybersecurity, Count how many items the participant checked or ticked off on the checklist. This will provide an overall score indicating the level of adherence to cybersecurity best practices. Based on that, you can assess your level of cybersecurity risk.

- **Low Risk:** If the majority of items are checked off as "done," indicating a strong adherence to cybersecurity best practices. (12 checks or more)
- **Medium Risk:** If there is a mix of items checked off and unchecked, suggesting some gaps in cybersecurity measures. (8-11 checks)
- **High Risk:** If very few items are checked off as "done," indicating significant vulnerabilities and gaps in cybersecurity practices. (less than 7 checks)

DIGITAL THREATS AND SAFETY

Digital security refers to the resources employed to protect our online identity, data, and other assets. In simpler terms, it's like a shield that protects our digital world against malicious activities. There are many types of digital attacks, each with different goals and methods. Some of the most common digital attacks that compromise cybersecurity are malware and social engineering.

- Malware infiltrates devices through various methods, such as social engineering or exploiting vulnerabilities. Types include:

    1. **Trojan Virus** - deceives users by appearing as harmless files or software. It can create backdoors for attackers to access systems.
    2. **Ransomware** - encrypts or locks users' files or devices, demanding ransom payments for decryption.
    3. **Wipers** - intended to destroy data or systems by overwriting files or file systems.
    4. **Worms**- self-replicating malware that spreads across networks, exploiting vulnerabilities in operating systems.
    5. **Spyware**- secretly monitors users' activities, collecting sensitive information like passwords and financial details.

- Social engineering attacks exploit human psychology to manipulate individuals into performing actions or divulging sensitive information. Common social engineering techniques include:

- Phishing - sending fraudulent emails or messages to trick users into revealing personal information or clicking on malicious links.
- Malvertising - placing malicious code in online advertisements to infect users' devices.
- Drive-by Downloads - installing malware on users' devices when they visit compromised websites.
- Scareware - displaying fake warnings or alerts to scare users into downloading malware removal tools.
- Baiting - leaving infected USB drives or other devices in public places to lure users into connecting them to their devices.
- Pretexting - deceiving individuals by creating a false pretext to gain access to sensitive data.
- Honey Trap - assuming a fake identity online to establish relationships and gather sensitive information.
- Pharming - redirecting users to fake websites to steal personal data or credentials.

➤ Activity 3.1. STOP or GO: Digital Safety Simulation

In this activity, you'll have the opportunity to assess various online scenarios and determine whether they represent digital threats that you should stop or safe practices that you can go ahead with. By engaging in this activity, you'll gain a better understanding of how to navigate the digital world safely.

INSTRUCTIONS:

(Note that this can be converted into a online gamified version (like the use of Kahoot!, Slido, Mentimeter, Quizizz, or other tools)

- Read each scenario carefully.
- Decide whether the scenario represents a digital threat (STOP) or a safe online practice (GO).

SCENARIOS

1. You're browsing social media and see a friend's post offering free tickets to a concert you've been wanting to attend. All you have to do is share the post and tag five friends in the comments.

2. You're making an online purchase on a reputable website you've used before. The website uses two-factor authentication where a code is sent to your phone after entering your login credentials.

3. You're setting up a new online banking account. The bank's website requires you to choose a security question and answer. You decide to use your favorite childhood pet's name as the answer, as it's something you'll always remember.

4. You're participating in an online forum discussing a new software update. You download the update directly from the official website of the software developer.

5. You're on a public Wi-Fi network at a coffee shop and need to access your online bank account to check your balance. The connection isn't password-protected.

6. You receive a notification from your bank about a suspicious login attempt on your account from an unrecognized location. The notification allows you to confirm or deny the attempt.

7. You're a gamer and participate in online forums. A fellow gamer you've been chatting with for a while sends you a private message with a link to a new, unreleased game they claim to have early access to. They urge you to download it before it gets taken down.

8. You receive a text message from an unknown number claiming you've won a large sum of money in a contest you don't remember entering. The message asks you to reply with your personal information to claim your prize.

9. You're shopping online and find a great deal on a brand-name item on a website you haven't heard of before. The price seems too good to be true, but the website looks professional.

10. You're strong with your passwords and use different ones for each online account. However, you find it challenging to remember them all. A friend suggests using a password manager app to store your passwords securely.

ANSWER KEY:

1. **STOP.** While it might seem like a lucky opportunity, free concert tickets shared via social media are often scams. Sharing the post could spread malware or expose your friends' information. It's best to verify the offer's legitimacy through the official concert venue or artist's website.

2. **GO.** Two-factor authentication adds an extra layer of security to your online accounts, making it a safe practice.

3. **STOP.** Easily guessable answers like pet names or birthdays are vulnerable to social engineering attacks. Hackers might be able to gather this information about you from your online profiles. Choose a complex security question and answer that wouldn't be readily available online.

4. **GO.** Downloading updates directly from trusted sources minimizes the risk of malware.

5. **STOP.** Public Wi-Fi networks are notoriously insecure. Avoid accessing sensitive information like bank accounts or credit card details on public Wi-Fi. If you absolutely must check your balance, consider using your phone's mobile data instead.

6. **GO.** Banks often use security measures like notifications to alert users about suspicious activity. Confirming or denying the attempt is a safe action.

7. **STOP.** Downloading unauthorized software, especially from unknown sources, can be risky. It could be malware disguised as a game. Check the legitimacy of the download through the official game developer's website or trusted gaming communities before proceeding.

8. **STOP.** This is a smishing (SMS phishing) attempt. Legitimate contests won't require you to divulge personal information via text message.

9. **STOP.** Unusually low prices on unfamiliar websites are often scams. Research the website's reputation and compare prices with established retailers before making a purchase.

10. **GO.** Password manager apps can be a secure way to store complex passwords for different accounts. However, ensure you choose a reputable app with strong encryption and a good security track record.

ENSURING OUR DIGITAL SAFETY AND SECURITY

Safeguarding your personal information and assets from identity theft, online scams, malware, and fraud is very important in the digital age. The Philippines ranked 4th in Kaspersky's 2021 global rankings of countries most targeted by web threats globally as the country most targeted by web threats in 2021, and cyber threats detected in the country from 2017 to 2021 increased by 433 percent (National Defense College of the Philippines, 2023). To help you fortify your defenses, here are some digital security reminders:

1. **Set up alerts on your accounts** - take advantage of alerts offered by platforms to stay informed about your account activities and quickly detect unauthorized access.

2. **Protect your devices** - keep your software, operating system (also phone operating systems), and browser up to date to leverage security fixes and protect against malware. Install reputable antivirus software and only download applications from trusted sources like Google Play or the App Store.

3. **Secure your account log-ins** - avoid reusing passwords across multiple accounts and consider using a password manager to generate and store complex passwords securely. Enable Two-Factor Authentication for an extra layer of security.

4. **Think before you click or share-** to xercise caution when clicking on links or opening attachments in unsolicited emails or text messages. Report spam emails and avoid sharing Personally Identifiable Information (PII) unnecessarily, especially via unsecured channels like email or text.

5. **Practice digital security on the go** - to be wary of using public Wi-Fi hotspots, and if necessary, use a Virtual Private Network (VPN) for added security. If you can, avoid using publicly available charging cords or USB ports, especially in unsecured places, as they can pose risks of malware or data theft.

6. **Other tips to combat digital threats-** to create bookmarks for important banking and other websites, ensure your email provider has robust security features, and monitor your accounts (especially banking) for fraudulent activity.

Because many children and young adults are often more familiar with the internet than their parents or grown-ups, it's important to share these digital safety tips with them to help protect yourselves. Your parents or guardians may not always know the latest ways to stay safe online, so teaching them about securing accounts, being cautious with public Wi-Fi, and avoiding scams can help protect you and your family. This way, you can create a safer online experience for yourself, with their support and understanding.

➤ Checkpoint Question 3.1 What other steps can you take to ensure your digital safety and security?

ONLINE FRAUDULENT ACTIVITIES: DIGITAL SCAMS AND IDENTITY

In the previous section, different digital security threats have been discussed, including online scams, identity theft, and many more attacks on our digital security. In this section, we will look closely at the different kinds of online scams, how people get their identities stolen, and fraud. Have you been a victim of online fraudulent activities?

➤ Activity 3.2. Fraud Alert!

In this activity, we'll explore how online scams and identity theft can happen through various creative mediums. Online scams and identity theft are serious risks that can affect anyone using the internet, including young people like you. You will choose a creative format to depict a scenario where an individual has been scammed online or had their identity stolen.

INSTRUCTIONS:

1. Form four groups. Each group will receive materials such as large sheets of paper or poster board, markers, colored pencils, crayons, or any other creative supplies you might need.

2. Take some time to brainstorm ideas based on your knowledge of online scams and identity theft. Consider different scenarios, such as phishing emails, fake websites, or social engineering tactics.

3. Decide on a creative format for your project. You can choose from:

4. Skit: Write and perform a short skit that illustrates the scenario.

5. Song: Compose and perform a song that tells the story of the scam or identity theft.

6. Poster: Design a poster that highlights the key elements of the scam and how to avoid it.

7. Video: Record a short video reenacting the scenario.

8. Work together to create your project. You have 20 minutes to complete it.

9. Present your project to the class. The facilitator will then ask other groups to spot signs of the fraudulent activities and discuss how they could have been prevented.

ONLINE SCAMS

An online scam refers to deceptive and fraudulent activities conducted through the internet to exploit individuals for financial gain. These scams exploit vulnerabilities in the digital age and impact millions of people globally.

- **Job offer scams** - unsolicited emails offering fake job opportunities, where victims receive a check or money order for more than the agreed amount and are asked to return the difference, only to discover later that the original check was fake.

- **Lottery scams** - emails claiming the recipient has won a lottery they never entered, often requiring payment of fees to claim the prize, resulting in identity theft and financial loss.

- **Beneficiary scams** - emails from strangers requesting help to transfer large sums of money out of the country, promising a share of the profits but ultimately leading victims to make payments without receiving any returns.

- **Online dating scams** - scammers pose as romantic interests on dating apps or websites, building trust with victims before asking for money or redirecting items, often using fake identities and emotional manipulation.

- **Charity fraud scams** - fake donation sites and emotional pitches capitalize on public tragedies, soliciting funds that never reach the victims and exploiting people's goodwill.

- **Repair scams** - scammers impersonate tech support personnel, offering to fix PC issues remotely and install malware on victims' computers to gain access to personal information and files.

- **Social media scams**: - fraudsters use quizzes, fake profiles, and malicious links on social media platforms to gather personal information, spread malware, or deceive users into providing financial details.

- **Robocall scams** - automated calls impersonate legitimate organizations to deceive victims into providing personal or financial information or installing malware.

- **Messaging scams** - scammers use SMS, messaging apps, and social media to deceive victims into providing personal or financial information, often through fake delivery notifications, banking alerts, or prize notifications.

- **Online shopping scams** - fake retailer websites offer counterfeit or non-existent products at low prices, often disappearing after receiving payments, or using social media stores to lure victims into making purchases.

- **Cryptocurrency Scams** - exploiting the rise of digital currencies, these scams target inexperienced investors with fraudulent schemes.

IDENTITY THEFT

Identity theft, or identity fraud, occurs when an imposter obtains key pieces of personally identifiable information (PII), such as ID numbers (SSS, GSIS, PhilHealth, etc.) or driver's license numbers, to impersonate someone else. The identity thief then uses the stolen information to impersonate the victim, open fraudulent accounts, make unauthorized purchases, or engage in other criminal activities while posing as the victim. There are two main categories of identity theft:

1. **True-name identity theft -** the thief uses PII to open new accounts or obtain services in the victim's name.

2. **Account-takeover identity theft -** the imposter gains access to the victim's existing accounts and uses them for fraudulent activities.

Examples of identity theft include:

- **Financial Identity Theft -** this involves using stolen identity information to gain financial benefits, such as opening credit card accounts, accessing financial accounts, making purchases, or taking out loans.

- **Medical Identity Theft -** thieves use stolen identity information to obtain medical services or prescription drugs or file false insurance claims.

- **Online identity theft-** involves the theft of personal information through online channels, such as social media, phishing scams, and hacking, for fraudulent purposes.

Identity thieves often use social engineering techniques such as mail theft, dumpster diving, shoulder surfing, and phishing to obtain PII. Signs that your identity may have been stolen include unauthorized transactions, changes to your credit score, missing bills, false accounts or charges on your credit report, health plan rejections, IRS notifications of duplicate tax returns, and notifications of data breaches.

➤ Checkpoint Question 3.2 What do you think are some factors contributing to the prevalence of online scams among Filipinos?

PREVENTING ONLINE SCAMS AND IDENTITY THEFT

Cybercriminals employ various techniques to exploit vulnerabilities and deceive unsuspecting victims into divulging sensitive information or falling for fraudulent schemes. From phishing emails to fake websites and malware attacks, the ways of online fraud are numerous and constantly evolving. Therefore, it's essential for individuals to take proactive steps to protect themselves against these threats.

- **Be cautious with personal information** - avoid sharing sensitive personal information, such as ID numbers or financial details, unless it's necessary and you trust the recipient.

- **Be vigilant** - stay informed about common online scams and identity theft techniques. Familiarize yourself with red flags and warning signs to recognize potential threats.

- **Use strong passwords** - create unique, strong passwords for each online account and avoid using easily guessable information like birthdays or names.

- **Enable Two-Factor Authentication (2FA)** - use 2FA whenever possible to add an extra layer of security to your accounts. This typically involves receiving a code via text message or authentication app and entering your password.

- **Update software regularly** - keep your devices and software up-to-date with the latest security patches and updates to protect against vulnerabilities that scammers may exploit.

- **Use secure websites** - when making online purchases or entering personal information, ensure that the website is secure by looking for “https://” in the URL and a padlock icon in the address bar.

- **Beware of phishing emails** - be cautious of unsolicited emails, especially those requesting personal information or containing suspicious links or attachments. Avoid clicking on links or downloading attachments from unknown sources.

- **Verify requests for personal information** - if you receive a request for personal information, especially via email or phone, verify the sender’s identity independently before providing any sensitive data.

- **Monitor your accounts regularly** - routinely review your bank statements, credit card transactions, and credit reports for any unauthorized activity. Report any suspicious transactions to your financial institution immediately.

- **Use antivirus and antimalware software** - install reputable antivirus and antimalware software on your devices to detect and prevent malicious software that could compromise your security.

- **Secure your wi-fi network** - secure your home Wi-Fi network with a strong password and encryption to prevent unauthorized access to your internet connection.

- **Dispose of personal information securely** - shred or securely dispose of documents containing sensitive personal information before discarding them to prevent dumpster diving identity theft.

FALSE INFORMATION

In the digital age, access to information has never been easier. People can find news, articles, and updates on virtually any topic with just a few clicks. However, this accessibility

has also given rise to a concerning trend: the proliferation of fake news, disinformation, and misinformation.

- Fake news refers to deliberately fabricated stories presented as factual news, often to mislead readers or influence public opinion.
- Disinformation involves deliberately spreading false information with malicious intent, such as propaganda or political manipulation.
- Misinformation refers to the unintentional sharing or disseminating of false information, often due to a lack of fact-checking or critical analysis.

All of those are considered false information. These are news, stories, or hoaxes created to deceive readers deliberately. The rise of false information has become a great concern with the rise of the digital age. Our trusted sources of information are journalists, media outlets, the government, and other organizations with established credibility. With the internet, little regulation and standards have been enforced in publishing, sharing, and consuming information.

➤ Checkpoint Question 3.3. How would you differentiate between fake news, disinformation, and misinformation?

➤ Activity 3.3 Fact or Fiction?

We are constantly bombarded with information from various online sources. However, not all information is created equal. With the abundance of content available on the internet, it's essential to develop critical thinking skills to discern between fact and fiction. This activity will explore the importance of evaluating online content critically.

INSTRUCTIONS:

1. Divide into small groups.

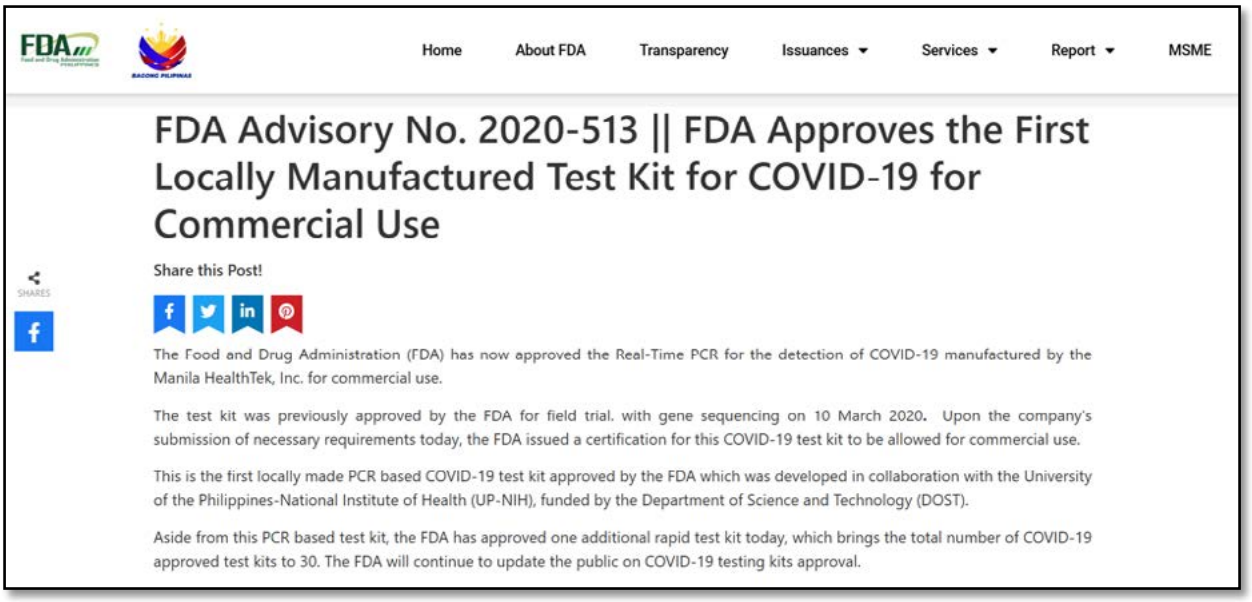
2. You will receive an online article or social media post. Some of these contain accurate information, while others may contain misinformation or false claims.

3. Your task is to carefully analyze the content provided and determine which pieces are factual and which ones are fictional.

4. During your analysis, discuss your reasoning behind your choices. Consider factors such as the credibility of the sources, the evidence provided, and any biases that may be present.

5. After analyzing the content, each group will be able to present their findings to the rest of the participants. Explain why you classified each piece of content as either fact or fiction.

Content 1: FDA Advisory No. 2020-513: FDA Approves the First Locally Manufactured Test Kit for COVID-19 for Commercial Use



Content 2: BSP warns banks on security risks

Sep 22, 2025 INQUIRER.NET Today's Paper

NEWS GLOBAL NATION BUSINESS LIFESTYLE ENTERTAINMENT TECHNOLOGY SPORTS OPINION

PROPERTY INDUSTRIES FINANCE CONSUMER & RETAIL TOURISM & TRANSPORTATION FOREIGN NEWS ECONOMY COMMUNICATIONS INDUSTRY MOVEMENTS

EDITORS' PICKS

BSP warns banks on security risks

Tetangco says banking system 'strong and stable'

By: Ben O. de Vera - Reporter / @bendeveraINQ Philippine Daily Inquirer / 12:18 AM April 04, 2016

Share:

Bangko Sentral ng Pilipinas. INQUIRER.net FILE PHOTO

DESPITE the entry of dirty money into a local bank and a remittance firm that sent shock waves to the financial system, the Bangko Sentral ng Pilipinas (BSP) maintained that the banking industry remained "strong and stable."

EDITORS' PICK MOST READ

NEWSINFO Signal No. 5 up over Babuyan Islands as Super Typhoon Nando rages

OPINION EDITORIAL: Credible probe to pacify the people

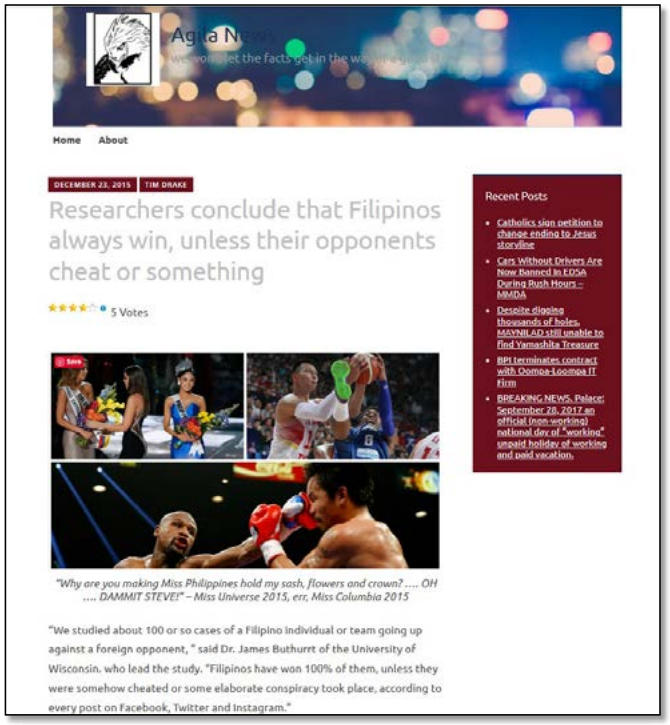
NEWSINFO Walang Pasok: Class suspensions on Sept. 22 due to Super typhoon Nando

NEWSINFO Protesters vow 'flood of cases' vs corrupt

SPORTS FIVB Men's World: Italy sweeps its way to quarterfinal round

NEWSINFO BOC vows to 'confront' corruption; pushes to change public perception

Content 3: Researchers conclude that Filipinos always win, unless their opponents cheat or something



Home About

DECEMBER 23, 2015 TIM DRAKE

Researchers conclude that Filipinos always win, unless their opponents cheat or something

5 Votes

"Why are you making Miss Philippines hold my sash, flowers and crown? .... OH .... DAMMIT STEVE!" – Miss Universe 2015, err, Miss Columbia 2015

"We studied about 100 or so cases of a Filipino individual or team going up against a foreign opponent, " said Dr. James Buthurrt of the University of Wisconsin. who lead the study. "Filipinos have won 100% of them, unless they were somehow cheated or some elaborate conspiracy took place, according to every post on Facebook, Twitter and Instagram."

Recent Posts

- Catholics sign petition to change ending to Jesus storyline
- Cars Without Drivers Are Now Banned In EDSA During Rush Hours – MMDA
- Despite digging thousands of holes, MAYNILAD still unable to find Yamashita Treasure
- BPI terminates contract with Oompa-Loompa IT Firm
- BREAKING NEWS: Palace: September 28, 2017 an official (non-working) national day of "working" unpaid holiday of working and paid vacation.

VARIOUS TYPES OF FALSE INFORMATION

We need to be aware of various types of false information. These are:

- **Clickbait** - these are stories created to attract more visitors to a websiteand earn more money from ads. They use exaggerated headlines to grab attention but often sacrifice truth or accuracy. You might come across clickbait headlines like “Shocking Secret Revealed: Local Celebrities Caught in Scandal!” which exaggerate to lure readers but often lack substance.

- **Propaganda** - stories made to mislead people, promote a biased viewpoint, or push a specific political agenda. During election season, political parties may spread propaganda to sway voters, such as distributing flyers with false promises or spreading rumors about opposing candidates. For example, a Facebook account claimed that 2022 presidential bet Vice President Leni Robredo is still facing sedition and other complaints before the Department of Justice due to “narco list” videos. But the cases had been thrown out in 2020.

- **Satire/Parody** - fake news stories created for entertainment or humor, not to be taken seriously. Examples include Adobo Chronicles or Showbiz Balita on Facebook. They may share satirical posts joking about current events or trending topics, aiming to entertain rather than inform.

- **Sloppy Journalism** - sometimes reporters publish stories without checking all the facts, leading to unreliable information. For instance, a local news outlet might publish a story without verifying facts, like reporting on a crime incident without confirming details or sources for the sake of releasing news first.

- **Misleading Headlines** - stories with partly true information can be twisted with misleading or sensational headlines, spreading quickly on social media. A news article may use a headline like “Metro Manila to be Flood-Free! Massive Budget Allocated!” to get more attention, when in reality, the story orthe news is about the government just allocating an additional budget forflood control projects in Metro Manila. Another example could be an online article with a headline like “Viral Video Exposes Makati Mayor Corruption Scandal!” might only have a small mention of corruption buried within, misleading readers into thinking it’s a major exposé.

- **Biased/Slanted News** - fake news confirming people's beliefs or biases, often appearing on social media feeds tailored to individual preferences. Some blogs or Facebook pages may cater to specific political leanings, selectively sharing news that aligns with their agenda and ignoring opposing viewpoints. You can think of it with a scenario wherein a politician, known for being tough on crime, is accused of involvement in a drug smuggling ring. A social media account with huge following posts "Politician X Exposed: From Drug Warrior to Drug Lord?", where they emphasize the accusations and portray Politician X as corrupt, without providing concrete proof.

- **Imposter Content** - fake news presented as if it's from a credible source, tricking people into believing false information. An example could be a website called "Pinoy Daily News" (designed to sound like a real Philippine news outlet) publishes an article claiming a popular Filipino celebrity has discovered a miraculous cure for a common disease plaguing the Philippines.

- **Manipulated Content** - real information or images altered to deceive, such as edited photos or videos used to create false narratives. In December 201, the Philippine Army admitted to releasing manipulated photos of alleged communist rebels surrendering themselves and their rifles to the military. It was pointed out online that the people in the photograph appeared to be floating.

With the proliferation of false information, how do we spot them? There are a number of things we can look out for when evaluating online content.

- Check if the social media account sharing the post is verified with a "blue badge" or check mark indicating authentication. While this doesn't guarantee reliability, it's often a sign of credibility.

- Examine the source of the story. Is it a recognized and trustworthy website? If unfamiliar, investigate the site's About section or the author's background for more information.

- Look beyond sensationalist or shocking headlines, which are common in fake news. Pay attention to headlines written in all caps or with excessive exclamation points.

- Fake news articles often contain grammatical mistakes or awkward language usage due to rushed or unprofessional writing.

- Verify the story with reputable news outlets. Confirm the existence and reliability of any sources cited in the article.

- Watch out for incorrect dates or altered timelines, which are common in false stories. Check the publication date to ensure the story is current and not outdated.

- Reflect on whether your personal beliefs influence your judgment of a news feature or report.

- Check for manipulated images or videos that may have been altered to deceive. Look for inconsistencies or unnatural elements in visual content that raise suspicion.

- Be aware of satirical sites that publish humorous or parody content. Check if the website is known for satire or creating funny stories before taking the story seriously.

- Research the author's credentials and reputation. Be cautious of articles authored by unknown individuals or those lacking expertise in the subject matter.

People may use false information for various reasons, including political gain, advertising revenue, as a joke or prank, or as a commentary (satire). Together, these pose significant challenges to society, threatening the integrity of democratic processes, undermining trust in media and institutions, and fueling social division and polarization. In this era of digital misinformation, it is more important than ever for individuals to critically evaluate the information they encounter, seek out reliable sources, and actively combat the spread of fake news.

➤ Checkpoint Question 3.3 What can governments, social media companies, news outlets, content creators, and regular users do to stop fake news online?

DIGITAL FOOTPRINT

Your online activities create a digital footprint that can affect your privacy and security. But what is a digital footprint? A digital footprint encompasses all your online activities, including social media posts, online purchases, account registrations, and more. These actions leave behind a trail of data that various entities, ranging from marketers to cybercriminals, can track and analyze. Understanding what comprises your digital footprint and how to safeguard it is crucial in protecting yourself from potential risks such as identity theft, fraud, and unwanted solicitation.

Sometimes, contributing to your digital footprint isn't always obvious, as websites and apps can track your activity without your explicit knowledge. For instance, websites may use cookies to monitor your behavior, and apps may collect data without your awareness. When you grant organizations access to your information, they may sell or share it with third parties, or it could be compromised in a data breach.

TYPES OF DIGITAL FOOTPRINTS

There are two main types of digital footprints: active and passive.

1. **Active Digital Footprint** - an active digital footprint occurs when you intentionally share information about yourself. This can include posting on social media, participating in online forums, or filling out online forms. Whenever you're logged into a website with a registered username or profile, your actions contribute to your active digital footprint.

2. **Passive Digital Footprints** - a passive digital footprint is created when information is collected about you without your awareness. This often happens when websites gather data about your browsing habits, such as how often you visit, where you're from, and your IP address. Additionally, social networking sites and advertisers may use your interactions, likes, shares, and comments to create profiles and target you with tailored content without your explicit consent or knowledge.

➤ Activity 3.4 My Online Trail

Much like footprints in the sand, our digital footprint can reveal much about us—to both intended and unintended audiences. Understanding the concept of a digital footprint is essential as it impacts our privacy, reputation, and even our security in the digital world.

INSTRUCTIONS:

1. Gather in your assigned groups. Each group will receive a large sheet of paper and markers.

2. Create a big footprint outline on the paper. Ensure the outline is large enough to fit various digital activities.

3. Brainstorm and list different online activities contributing to your digital footprint. Write each online activity on a separate sticky note.

4. Place the sticky notes inside the footprint outline, arranging them to represent the online activities of a fictional character or persona.

5. Once you have completed your digital footprint. Around the footprint, write ways on how the fictional character can ensure a secure and positive digital footprint.

6. Prepare to present it to the rest of the class. Explain the significance of online activities and their potential impact on the fictional character's digital life.

SECURING YOUR DIGITAL FOOTPRINT

While digital footprints can enhance your online experience by providing personalized content, they also pose risks such as compromised privacy, identity theft, and targeted scams. Cybercriminals can leverage your digital footprint to orchestrate sophisticated attacks, making it essential to manage your online presence effectively. Some examples of digital footprints are:

- Your search history
- Text messages, including deleted messages

- Photos and videos, including deleted ones
- Tagged photos, even those you never wanted online
- Online purchases and transaction histories
- Location data collected by mobile devices and apps
- Likes/loves on sites like Facebook and Instagram
- Browsing history, even when you are in “incognito” mode
- Cookies that websites collect
- Data collected by smart devices, such as fitness trackers, smart home assistants, and wearable technology

Your digital footprint represents your online trail and reputation—virtually all your actions are being monitored and recorded. But what exactly does this entail, and why is it significant? The digital footprint you generate holds importance because:

- It tends to be permanent once publicly accessible, particularly with content shared on social media platforms.
- It can influence your online reputation, which is nearly as crucial as your reputation in the physical world.
- Prospective employers often conduct background checks on potential hires by examining their online presence.
- Colleges and universities may review applicants’ social media activity before issuing acceptance letters.
- Your words, images, and videos can be misconstrued or manipulated for malicious intents.
- Malicious actors may disseminate your private messages to a wider audience, potentially harming friendships, relationships, and reputations.
- Cybercriminals might pilfer and exploit your personal information for phishing scams or fabricate fake accounts using your data.

To mitigate the potential risks associated with your digital footprint, consider the following measures:

- Conducting regular searches to monitor your online presence.
- Setting up alerts to receive notifications of online mentions.
- Tightening privacy settings on social media platforms and other online accounts.
- Exercising caution when sharing personal information online.
- Restricting mobile app permissions to minimize data exposure.

- Limiting the number of online accounts and using a password manager for enhanced security.
- Being mindful of linking accounts and granting permissions to third-party apps.
- Educating yourself on privacy policies and taking proactive steps to protect your personal data.

➤ Checkpoint Question 3.4 Should employers or schools check your social media history when deciding whether to hire or admit you? Why or why not?

➤ Activity 3.5 Docufilm Analysis: The Power of Privacy

For this activity, you will view the documentary "The Power of Privacy," which explores the challenges and opportunities of digital privacy in the 21st century.
Link to video: https://youtu.be/KGX-c5BJNFk?si=0Ed7ibLv8INVOojq

INSTRUCTIONS:

1. As you watch, note key points, arguments, and examples the film presents.
2. After watching, gather in groups to discuss the following questions:
   - How did the documentary make you feel about your own digital privacy? Did it change your perspective or behavior regarding how you share personal information online?
   - Based on the insights gained from the documentary, what steps will you take to enhance your digital privacy? Are there any specific practices or tools you plan to adopt to safeguard your personal information?

➤ MODULE 4
Understanding Cybercrime, Cyberbullying, and OSAEC

MODULE OVERVIEW:

In this module, we will delve into the legal aspects of cybercrime, focusing on the Cybercrime Prevention Act of 2012 (Republic Act No. 10175, signed into law on September 12, 2012, and upheld by the Supreme Court in 2014) (Republic Act No. 10175). We will explore the role of law enforcement agencies, such as the Anti-Cybercrime Group of the Philippine National Police, in addressing cybercrimes. Additionally, the module will cover the alarming issue of Cyberbullying and Online Sexual Abuse or Exploitation of Children (OSAEC).

MODULE OBJECTIVES:

At the end of this module, the learners can:

- Describe the legal framework surrounding cybercrime, including relevant legislation such as the Cybercrime Prevention Act of 2012 (Republic Act No. 10175, signed into law on September 12, 2012, and upheld by the Supreme Court in 2014) (Republic Act No. 10175).
- Identify cyberbullying and develop strategies for addressing it.
- Explain Online Sexual Abuse or Exploitation of Children (OSAEC).

Sub-Topics:

- The Republic Act No 10175 or the Cybercrime Prevention Act of 2012 (Republic Act No. 10175, signed into law on September 12, 2012, and upheld by the Supreme Court in 2014)
- Cyberbullying
- Online Sexual Exploitation and Abuse of Children and the Law

Materials Needed: pens/pencils, projector, screen, speakers, printed worksheets and scenario cards, poster boards, markers, adhesives

Topic	Activity	Description	Duration
Pre-Activity	Introduction to the Module	Overview of module objectives, introduction to the key legal frameworks, guidelines for addressing sensitive topics, and establishing a supportive environment for discussion.	10 mins
	Pre-Activity 4: Cybercrime Pre-Test	A multiple-choice quiz to assess learners' baseline knowledge on cybercrime definitions, real-life examples, and the relevant Philippine legislation, setting the stage for deeper discussions.	10 mins
The Philippine Cybercrime Law	Discussion	In-depth discussion of Republic Act No. 10175, covering key provisions like illegal access, data interference, and content-related offenses.	20 mins
	Activity 4.1 Red Flag or Green Flag	An interactive exercise where students analyze various scenarios to identify risky online behaviors (red flags) versus safe practices (green flags).	30 mins
	Discussion	Exploration of additional legal instruments and discussion on the roles and responsibilities of law enforcement agencies, including their collaboration with international bodies.	20 mins
Cyberbullying	Discussion	Presentation and discussion of current statistics and data on cyberbullying in the Philippines, examining demographic trends, mental health impacts, and the prevalence of cyber violence among youth.	10 mins

Topic	Activity	Description	Duration
	Activity 4.2 Video Analysis	Screening of the short video "George" followed by guided reflection; students discuss implications of the actions shown, touching on issues such as privacy, consent, and the impact of social media behavior.	15 mins
	Discussion	Discussion on the psychological, emotional, and physical effects of cyberbullying, along with exploration of proactive strategies to take action.	20 mins
	Activity 4.3: No to Bullies, Yes to Allies	Small-group campaign activity where students brainstorm and design a poster or campaign plan to raise awareness against cyberbullying.	30 mins
	Discussion	Discussion on how to report cyberbullying incidents, including practical steps, and available hotline numbers.	10 mins
Online Sexual Abuse and Exploitation of Children	Activity 4.4: Docufilm Analysis	Viewing of Atom Araullo's documentary on online sexual exploitation, followed by group analysis to identify key crimes, law enforcement responses, and measures implemented to protect victims.	30 mins
	Discussion	Examination of the Anti-OSAEC and Anti-CSAEM Act, clarifying legal definitions, its purpose, and the key entities involved in the enforcement of the law.	20 mins
	Activity 4.5 Policy Drafting Workshop	Groups draft a local policy or ordinance for an LGU or school based on RA 11930.	30 mins

Topic	Activity	Description	Duration
	Discussion	Discussion on the severity of online child sexual exploitation in the Philippines, analyzing statistical evidence, socioeconomic factors, and the challenges faced by law enforcement, as well as preventive strategies.	20 mins
	Activity 4.6 Guardians of the Digital Galaxy	Group project to design a poster that emphasizes the importance of reporting OSAEC, outlines digital safety practices, and encourages community action	25 mins
		ESTIMATED TOTAL HOURS	**5 hours**

IMPORTANT NOTE:

Given the sensitive nature of the topics covered in this module, facilitators should be aware of the following:

- These topics may trigger emotional distress among high school students. Be prepared to handle such reactions with empathy and care.
- Ensure you are trained in debriefing techniques to help students process the information and their feelings effectively.
- Be equipped with strategies to de-escalate any situations that may arise during discussions.
- Have information on support resources available for students who may need additional help, such as counseling services.
- Foster a safe and supportive environment where students feel comfortable expressing their thoughts and concerns.

➤ Pre-Activity 4 Cybercrime Pre-Test

Instructions

1. Answer the following questions to the best of your ability.
2. There is no need to guess if you are unsure. Be honest in your responses.

Why is cybercrime?

a. Crime committed using a computer
b. Crime involving theft of digital assets
c. Crime committed using internet
d. All of the above

Which of the following is an example of cybercrime?

a. Phishing
b. Jaywalking
c. Shoplifting
d. None of the above

What legislation in the Philippines addresses cybercrime?

a. 12. Republic Act No. 10175
b. 13. Republic Act No. 12345
c. Republic Act No. 9999
d. Republic Act No. 7777

What is the primary objective of the Cybercrime Prevention Act of 2012 (Republic Act No. 10175, signed into the law on September 12, 2012, and upheld by the Supreme Court in 2014)?

a. To regulate online shopping
b. To prevent and combat cybercrime
c. To combat cyberbullying
d. To promote internet freedom

Which agency is responsible for enforcing cybercrime laws in the Philippines?

a. Department of Information and Communications Technology (DICT)
b. Philippine National Police (PNP)
c. Central Intelligence Agency (CIA)
d. National Telecommunications Commission (NTC)

THE PHILIPPINE CYBERCRIME LAW

Republic Act No. 10175, also known as the Cybercrime Prevention Act of 2012 (Republic Act No. 10175, signed into law on September 12, 2012, and upheld by the Supreme Court in 2014), was enacted to address crimes committed against and through computer systems. It aligns with international standards, particularly the Budapest Convention (ratified by the Philippines in 2018 after its accession in 2016) on Cybercrime. The law aims to pre-empt, prevent, and prosecute cybercrimes, including offenses against data privacy, integrity, and availability, as well as content-related offenses such as cybersex and child pornography. While the law has faced legal challenges, it sanctions various content-related offenses and provides penalties for offenders, including imprisonment and fines.

As members of the public, here are the following features we must know about the law:

- Clear and consistent definitions of what cybercrime is
- Stronger punishments for people who commit cybercrimes
- More authority given to law enforcement authorities to catch cybercriminals
- Improved ways to coordinate efforts with other countries to fight cybercrime

The Cybercrime Prevention Act of 2012 (Republic Act No. 10175, signed into law on September 12, 2012, and upheld by the Supreme Court in 2014) outlines various provisions aimed at combating cybercrimes. Here's a brief description of each:

- **Illegal Access:** Unauthorized entry into a computer system or application.
- **Illegal Interception:** Unauthorized interception of computer data communication.
- **Data Interference:** Unauthorized tampering, deleting, or introducing viruses to computer data.
- **System Interference:** Unauthorized interference with computer system operations, including virus transmission.
- **Misuse of Devices:** Unauthorized use, sale, or distribution of gadgets or programs for cybercrimes.
- **Cybersquatting:** Malicious acquisition of domain names to harm others or profit unfairly.
- **Computer-related Forgery:** Unauthorized alteration of computer data for fraudulent purposes.
- **Computer-related Fraud:** Unauthorized access or alteration of computer data to cause damage.
- **Computer-related identity theft:** Unauthorized use or acquisition of personally identifiable information.
- **Cybersex:** Operating or facilitating lascivious activities via computer systems.
- **Child Pornography:** Unlawful activities involving child exploitation through computer systems.
- **Libel:** Defamatory acts committed using computer systems.
- **Aiding or Abetting:** Assisting or encouraging the commission of cybercrimes.
- **Attempt in the Commission:** Willful attempts to commit cybercrimes.
- **Coverage of Other Laws:** Application of cybercrime provisions to crimes committed via information and communication technologies.
- **Corporate Liability:** Holding juridical persons accountable for cybercrimes committed on their behalf or for their benefit.

➤ Activity 4.1 Red Flag or Green Flag? Recognizing Cybercrime Risks

The objective of this activity is to enhance awareness and understanding of cybercrime risks and legal violations outlined in the Philippine Cybercrime Law.

Instructions: (Note that this can be converted into a online gamified version (like the use of Kahoot!, Slido, Mentimeter, Quizizz, or other tools)

1. Read each scenario provided carefully and consider the actions described in the context of cybercrime.

2. Determine whether each scenario represents a "Red Flag" (potential cybercrime risk or legal violation) or a "Green Flag" (safe and legal online behaviors).
   a. Posting derogatory comments and false information about a classmate on social media to damage their reputation.
   b. Sharing personal login credentials for online banking accounts with a friend.
   c. Reporting suspicious online activity to relevant authorities.
   d. Downloading copyrighted movies or music from unauthorized websites.
   e. Using privacy settings on social media platforms to control who sees your information.
   f. Being cautious about clicking on unknown links or downloading attachments from unverified sources.
   g. Sharing intimate photos or videos of a former partner without their consent.
   h. Sending threatening messages to someone via email or messaging apps.
   i. Meeting up with a friend you've only known online for 2 weeks.

Answer key:

a. Red Flag, cyberbullying
b. Red flag, this exposes your friend to the risk of identity theft
c. Green flag
d. Red Flag, copyright infringement
e. Green flag
f. Green flag
g. Red Flag, this is a serious crime
h. Red flag, hate speech can be a crime
i. Red flag, safety concern - online predators can exist

OTHER LEGAL BASIS FOR CYBERCRIME

The legal framework for cybercrime in the Philippines primarily revolves around the Cybercrime Prevention Act of 2012 (Republic Act No. 10175, signed into law on September 12, 2012, and upheld by the Supreme Court in 2014) (Republic Act No. 10175). This act provides comprehensive provisions for detecting, investigating, and preventing cyber crimes. Key components of the Philippine legal framework for cybercrime include:

- **Cybercrime Prevention Act of 2012 (Republic Act No. 10175, signed into law on September 12, 2012, and upheld by the Supreme Court in 2014):** This legislation outlines various cybercrimes such as illegal access, data interference, cybersex, child pornography, and online libel, among others. It also defines penalties for these offenses.

- **Republic Act No. 9775 (Anti-Child Pornography Act of 2009):** Specifically addresses crimes related to child pornography and provides measures to prevent and combat such activities.

- **Revised Penal Code:** Some cybercrimes, such as libel committed through online means, are punishable under existing provisions of the Revised Penal Code of the Philippines.

- **International Cooperation:** The Philippines also participates in international agreements and conventions to combat cybercrimes, facilitating cooperation with other nations in investigating and prosecuting cyber offenders.

    - **Budapest Convention (ratified by the Philippines in 2018 after its accession in 2016) on Cybercrime (Council of Europe Convention on Cybercrime):** The Philippines signed the Budapest Convention on Cybercrime in September 2012. This convention provides a framework for international cooperation in combating cybercrimes, including offenses related to computer systems, data, and content. It promotes harmonization of laws, mutual legal assistance, and extradition among participating countries.

- **ASEAN Declaration to Prevent and Combat Cybercrime:** The Philippines, as a member of the Association of Southeast Asian Nations (ASEAN), participates in regional initiatives to prevent and combat cybercrimes. The ASEAN Declaration to Prevent and Combat Cybercrime serves as a guiding framework for cooperation among ASEAN member states in addressing cyber threats and promoting cybersecurity.

➤ Checkpoint Question 4.1. Is it justifiable for cybersecurity measures to take over freedom of speech and expression?

THE CYBERCRIME LAW ENFORCEMENT

The National Bureau of Investigation and the Philippine National Police are the law enforcement agencies for the Cybercrime Prevention Act of 2012 (Republic Act No. 10175, signed into law on September 12, 2012, and upheld by the Supreme Court in 2014). Both shall organize a cybercrime unit or center staffed by special investigators to handle cases involving violations of the Cybercrime Prevention Act of 2012 exclusively.

The Anti-Cybercrime Group (ACG) of the Philippine National Police (PNP) is crucial in combating cybercrime. The ACG is tasked with investigating and addressing various forms of cyber offenses, ensuring the safety and security of digital spaces, and promoting awareness about cyber threats. Their responsibilities include:

- **Investigation and Enforcement -** The ACG investigates cybercrimes such as hacking, online fraud, identity theft, and other information and communication technology offenses. They collaborate with other law enforcement agencies nationally and internationally to track down cybercriminals and bring them to justice.

- **Capacity Building and Training -** The ACG conducts training programs, workshops, and seminars to enhance the skills of law enforcement personnel in handling cybercrime cases.

- **Public Awareness and Education -** The ACG educates the public about safe online practices, emphasizing the importance of protecting personal information, avoiding phishing scams, and securing digital devices.

- **Collaboration with Other Agencies -** Given the global nature of cybercrime, the ACG collaborates with international law enforcement agencies, sharing information and expertise to combat cross-border cyber threats.

The Cybercrime Division of the National Bureau of Investigation (NBI) in the Philippines is a specialized unit tasked with investigating and combating cybercrimes within the country. The Cybercrime Division employs specialized personnel with expertise in digital forensics, cybercrime investigation techniques, and computer science to identify, track, and apprehend cyber offenders. Their primary tasks include:

- **Investigation and Detection -** The CCD investigates and detects various cybercrimes, including identity theft, online scams, hacking of bank accounts, phishing, cyber libel, and other offenses committed in the digital realm.

- **Forensic Analysis -** They conduct forensic analysis of digital evidence to trace the origin of cybercrimes, identify perpetrators, and build strong cases for prosecution.

- **Public Awareness and Education-** They raise awareness about cyber threats, safe online practices, & preventive measures through educational campaigns & workshops.

- **Collaboration with Other Agencies-** The CCD collaborates with other law enforcement agencies, both nationally and internationally, to share information, track down cybercriminals, and dismantle criminal networks.

- **Victim Assistance-** The CCD assists victims of cybercrimes by providing guidance, support, and helping them navigate legal processes.

REPORTING CYBERCRIME

To report cybercrime, we can reach out to the following:

Philippine National Police Anti-Cybercrime Group (PNP-ACG):
Walk-in: Anti-Cybercrime Group Building, Camp Crame, Quezon City, Manila
Complaint Action Center Hotline: +63 (8) 723-0401 local 7491
Viber: +63 961 829 8083
Facebook: facebook.com/anticybercrimegroup
Twitter: @pnpacg
Website: pnpacg.ph/main/contacts.html

Department of Justice (DOJ)
Walk-in: Office of the Cybercrime, DOJ, Ermita, Manila
Website: www.doj.gov.ph
E-mail: cybercrime@doj.gov.ph
Hotline: 526-2747/521-8345
Website: www.doj.gov.ph/reporting_cybercrime.html

➤ Checkpoint Question 4.2. How can young people help fight cybercrime, and what can schools and youth groups do to promote safe online behavior?

CYBERBULLYING

Cyberbullying refers to the use of digital technologies, such as social media, messaging platforms, gaming platforms, and mobile phones, to engage in repeated behavior aimed at intimidating, angering, or humiliating individuals who are targeted. Examples include spreading false information or sharing embarrassing photos/videos on social media, sending hurtful or threatening messages/images via messaging platforms, and impersonating someone to send mean messages through fake accounts. Unlike face-to-face bullying, cyberbullying leaves a digital trail, which can serve as evidence to address and prevent further abuse. Here are some facts and figures on cyberbullying in the Philippines:

1. Prevalence of Cyberviolence (UNICEF, 2019)
    - Data reveal that cyber violence affects almost half of the children aged 13-17 in the Philippines.
    - The prevalence of cyberviolence is nearly the same for both genders, with 44% of males and 43% of females experiencing it.
    - Verbal abuse over the internet or cell phone constitutes one-third of cyberviolence incidents, while a fourth involves sexual messages.
    - Interestingly, more females receive sexual messages, but twice as many males report having their nude bodies or sexual activities shown online, whether real or falsified.

2. Age Groups Affected (GMA Network, 2016)
    - A survey conducted in the Philippines revealed that 80% of teenagers experience cyberbullying through social media.
    - Even among younger children aged 7 to 12, 60% have encountered cyberbullying[2].

3. Regional Trends (Statista, 2019)
    - In 2019, the number of cyberbullying incidents was highest in Region 4-A, accounting for approximately 92.4 thousand victims.
    - The CARAGA region and the National Capital Region also witnessed significant cyberbullying or cyber libel occurrences.

➤ Activity 4.2. Video Analysis: 'George'

George' is a short video about cyberbullies. Let's take a look at the video and why it has been considered cyberbullying.

INSTRUCTIONS:

1. Watch the short video, George.
2. Reflect on the following questions:
    a. Was it wrong for Alex to film Derrick while he was rapping?
    b. Why was it wrong for George to post it on his Friendbook wall?
    c. Who can be considered as a cyberbully in the video?

EFFECTS OF CYBERBULLYING

When bullying happens online it can feel as if you're being attacked everywhere, even inside your own home. It can seem like there's no escape. The effects can last a long time and affect a person in many ways:

1. **Mentally** – feeling upset, embarrassed, stupid, even afraid or angry
2. **Emotionally** – feeling ashamed or losing interest in the things you love
3. **Physically** – tired (loss of sleep) or experiencing symptoms like stomach aches and headaches.

The feeling of being laughed at or harassed by others can prevent people from speaking up or trying to deal with the problem. In extreme cases, cyberbullying can even lead to people taking their own lives. Cyberbullying can affect us in many ways, and it's particularly prevalent and normalized in spaces like mobile gaming and social media, where anonymity and distance can embolden individuals to engage in hurtful behavior. However, it's essential to recognize that these challenges can be overcome, and people can regain their confidence and health with the right support and intervention.

➤ Checkpoint Question 4.3. Where do you think the line should be drawn between online teasing or joking and cyberbullying?

TAKING ACTION AGAINST CYBERBULLYING

Here are some steps you can take if you're experiencing cyberbullying or know someone who is:

1. **Tell someone:** It's important to speak up and tell a trusted adult if you're being bullied online. This could be a parent, teacher, school counselor, or another responsible adult. Don't suffer in silence; reporting the bullying is the first step toward stopping it.

2. **Work with your parents:** If you're worried about losing privileges like phone or computer use because of the bullying, communicate your concerns to your parents. Together, you can find a solution that addresses the bullying without punishing you.

3. **Seek support:** Talk to a school counselor, trusted teacher, or family member about what you're going through. If the bullying is taking a toll on your mental health, consider seeking therapy or counseling for additional support.

4. **Take a break:** Sometimes, stepping away from the situation can help you regain perspective and cope with the bullying. Turn off your phone or computer, engage in activities you enjoy, and spend time with supportive people who make you feel good about yourself.

5. **Resist the urge to retaliate:** It's natural to want to defend yourself when faced with cyberbullying, but responding to the bully can escalate the situation. Instead, focus on ignoring the bullying and avoiding further interaction with the bully.

6. **Save evidence:** If possible, save evidence of the bullying, such as screenshots or copies of mean messages. This documentation can be helpful if you need to report the bullying to social media platforms or authorities.

7. **Report the bullying:** Many social media sites have mechanisms for reporting abusive behavior, and service providers can block users who engage in cyberbullying. Don't hesitate to report instances of bullying to the appropriate authorities or platforms.

8. **Block the bully:** Take advantage of privacy settings and blocking features on your devices to prevent the bully from contacting you further.

9. **Practice online safety:** Protect your personal information and passwords, and be cautious about what you share online. Once something is posted online, it can be difficult to remove, so think carefully before sharing sensitive information or engaging with hurtful content.

If you're aware that a friend is engaging in cyberbullying behavior, it's important to address the situation sensitively but firmly. Here's what you can do:

1. **Have a private conversation:** Take your friend aside and talk to them about their behavior in a non-confrontational manner. Avoid blaming or shaming them, but express your concerns calmly and directly.

2. **Stand up for your principles:** Let your friend know their actions are unacceptable and go against your values. Make it clear that you cannot condone or support bullying behavior, even if it's coming from a friend.

3. **Explain the consequences:** Help your friend understand the serious impact that cyberbullying can have, not only on the victims but also on themselves and others around them. Emphasize the potential legal, social, and emotional consequences of their actions.

4. **Encourage empathy:** Encourage your friend to consider how their words and actions may hurt others. Empathy can help them recognize the human impact of cyberbullying and motivate them to change their behavior.

5. **Offer support:** Let your friend know that you're there to support them in making positive changes. Offer to help them find healthier ways to express themselves and resolve conflicts without resorting to bullying tactics.

6. **Seek help if necessary:** If your friend is unwilling to change their behavior or if the situation escalates, don't hesitate to seek help from a trusted adult, such as a parent, teacher, or school counselor. They can provide additional support and intervention as needed.

While these steps outline proactive measures to address cyberbullying, it's important to acknowledge that they might be easier said than done. Speaking up about bullying, whether you're the victim or a concerned bystander, can be challenging and intimidating. Many individuals may hesitate to report bullying out of fear of retaliation, embarrassment, or uncertainty about how others will react. Additionally, navigating conversations with parents or other adults about bullying can be complex, especially if there are concerns about potential consequences or misunderstandings. Furthermore, addressing bullying behavior in a friend requires delicacy, assertiveness, and courage to challenge harmful behavior within a relationship. Despite these challenges, it's crucial to recognize the importance of taking action against cyberbullying to promote safety, well-being, and respect in online communities.

Remember that addressing cyberbullying is essential for promoting a safe and respectful online environment for everyone involved. By speaking up and holding your friend accountable, you're taking an important step toward preventing further harm and fostering positive relationships.

➤ Activity 4.3. No to Bullies, Yes to Allies! A 'Campaign Against Cyberbullying' Activity

We must encourage everyone to act against bullying. In this activity, we will create a campaign poster to raise awareness about cyberbullying, promote empathy, and encourage students to take a stand against cyberbullying.

INSTRUCTIONS:

1. Form small groups (maximum of 6) and brainstorm ideas for a 'Campaign Against Cyberbullying.'

2. Develop a plan for your campaign, including objectives, target audience, key messages, and visual elements. Think about how you can promote your campaign through social media, school events, or presentations.

3. Use the materials provided to create posters and visual materials (can be digital) for your campaign based on your plan.

4. Present your campaign idea to the group, explaining your objectives, messages, and visual elements.

REPORTING CYBERBULLYING

In the Philippines, cyberbullying and online threats fall under the jurisdiction of the Anti-Cybercrime Law (Republic Act No. 10175). For minors, aside from RA 10627, or the Anti-Bullying act of 2013, Republic Act 7610 also known as Special Protection of Children Against Abuse, Exploitation and Discrimination Act can also be used. To address such incidents effectively, it's important to follow practical steps:

1. **Document the threats:** Keep a record of all cyberbullying incidents and threats. Take screenshots or preserve digital communication that serves as evidence.

2. **Report to the social media platform:** If cyberbullying occurs on Facebook or any other social media platform, report the issue to the platform's administrators. They have mechanisms in place to handle such situations and take appropriate action.

3. **File a Report with Law Enforcement:** Notify the Philippine National Police (PNP) Anti-Cybercrime Group or the National Bureau of Investigation (NBI) about the cyberbullying incident. They possess the technical expertise to trace IP addresses and conduct investigations.

4. **Consult a Lawyer:** Consider seeking legal advice from a lawyer who specializes in cybercrime cases. They can guide you through the legal procedures and assist in filing a case against the perpetrator. If you do not have access to a private lawyer, you can contact the Public Attorney's Office (PAO), which provides free legal assistance to those in need. PAO can help you understand your legal options and support you through the legal process.

5. **Prepare for the Investigation Process:** Understand that investigating cybercrimes can be complex and time-consuming. Be patient and cooperative throughout the process, providing authorities with all necessary documentation and information.

Here are hotlines you can reach for cyberbullying support:

- **NCMH Crisis Hotline:** Offers 24/7 support over the phone for individuals struggling with emotional and suicidal thoughts.

- **Tawag Paglaum Centro Bisaya:** A helpline available 24/7 for those dealing with emotional challenges and suicidal thoughts.

- **Bantay Bata Helpline 163:** Provides support over the phone from 7 AM to 7 PM, 7 days a week, for various concerns including bullying.

- **Makabata Helpline 1383:** A mechanism developed by the Council for the Welfare of Children (CWC), an attached agency of the DSWD, to provide immediate response, monitoring, and feedback via calls, electronic mail, and different social media platforms about all child rights and concerns.

- **DepEd Learners TeleSafe Contact Center Helpline** at (02) 8632-1372 and (02) 8637-2306, or via SMS at 0945-175-9777: To report incidents of abuse, exploitation, and bullying committed against learners in schools.

- **Kaibigan Chat Line** (a UNICEF x PYDN platform in Facebook)
  Refer to local organization, offices, or school's hotline if applicable.

➤ Checkpoint Question 4.4. What are some strategies that schools can implement to better support students who are affected by cyberbullying?

ONLINE SEXUAL ABUSE AND EXPLOITATION OF CHILDREN (OSAEC)

While the internet offers numerous advantages for children, it can also be the most dangerous place for them. Globally, the issue of online child exploitation is a cause for alarm, with millions of children subjected to coerced sexual activities or extortion for sexual purposes. Additionally, the proliferation of child sexual abuse materials on the internet is alarming, with hundreds of millions of such materials being shared and traded online.

➤ Activity 4.4. Docufilm Analysis

In this activity, we will focus on understanding how the Anti-OSAEC and Anti-CSAEM Law (Republic Act No. 11930, lapsed into law on July 30, 2022 and took effect on August 14, 2022) (Republic Act No. 11861) helps protect children and punish offenders in cases like the one shown in the documentary. This will give you a basic understanding of how the law works in real situations.

INSTRUCTIONS:

1. Watch Atom Araullo's documentary "Isang Ina, Ginamit ang Sariling Anak sa Online Sexual Exploitation".

2. Pay close attention to what the police and government authorities do to stop the abuse and protect the victims.

AS YOU WATCH, REFLECT ON THE FOLLOWING QUESTIONS:

1. What crimes did you see in the documentary?

2. How did the police and government protect the children in the documentary? Write down at least two actions the police or authorities took to protect the children in the film.

3. What do you think should be done or what actions can be taken to prevent and protect children from OSAEC and CSAEM?

RA 11930 or The Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse Or Exploitation Materials (CSAEM) Act Republic Act No. 11930, also known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act, was enacted to strengthen the protection of children against online exploitation and abuse. The law recognizes the importance of ensuring the physical, emotional, psychological, and moral well-being of children while promoting their safe access to digital technologies. It places strict regulations on the production, dissemination, and consumption of child sexual abuse or exploitation materials (CSAEM) and aims to hold offenders accountable, while also ensuring proper rehabilitation for victims.

OSAEC is defined as "the use of information and communication technology (ICT) as a means to abuse and/or exploit children sexually." This encompasses various forms of abuse and exploitation, including:

- **Production, Dissemination, and Possession of CSAEM -** creating, sharing, or holding materials that depict child sexual abuse or exploitation.

- **Online Grooming-** Engaging with children online to prepare them for sexual abuse or exploitation.

- **Sexual Extortion-** Coercing children into providing sexual content or engaging in sexual activities through threats or manipulation.

- **Sharing Image-Based Sexual Abuse-** Distributing images or videos of children in sexually abusive or exploitative situations.

- **Commercial Sexual Exploitation-** Engaging children in sexual activities for financial gain, including online prostitution.

- **Live-Streaming of Sexual Abuse-** Broadcasting sexual abuse of children in real-time over the internet.

- OSAEC is also referred to as online child sexual abuse or exploitation (OCSEA), and it includes cases where offline abuse is combined with an online component.

CSAEM is defined as "any representation, whether offline or through ICT, that depicts a child engaged in real or simulated sexual activities, or shows acts of sexual abuse or exploitation." This includes:

- **Visual, Video, Audio, or Written Representations:** Any form of media that depicts or describes sexual activities involving children.

- **Focus on Genitalia or Private Body Parts:** Materials that specifically highlight a child's genitalia or other private body parts in a sexual context.

- In the law, CSAEM may also be referred to as Child Sexual Abuse Material (CSAM).

PURPOSE OF THE ANTI-OSAEC AND ANTI-CSAEM ACT

- **Protection of Children -** the law aims to protect children from online sexual abuse and exploitation, promoting their physical, moral, spiritual, intellectual, emotional, psychological, and social well-being.

- **Rights and Safety -** it guarantees the protection of children from abuse or exploitation, regardless of the use of ICT, and ensures safe access to digital technologies.

- **Awareness and Understanding -** the law promotes children's understanding of their civil, political, cultural, economic, and social rights in the digital space.

KEY ENTITIES INVOLVED

- **National Coordination Center against OSAEC and CSAEM (NCC-OSAEC-CSAEM) -** develops and implements programs for prevention, support, and reintegration of child victims.

- **Inter-Agency Council Against Trafficking (IACAT) -** oversees NCC-OSAEC-CSAEM and coordinates efforts against OSAEC and CSAEM.

- **Department of Social Welfare and Development (DSWD) -** provides support and legal assistance, and assumes temporary protective custody of child victims.

- **Department of Justice (DOJ) -** offers legal support and assistance in protective custody matters.

- **Local Government Units (LGUs) -** pass ordinances, establish prevention programs, and provide rehabilitation and reintegration for victims.

- **Anti-Money Laundering Council (AMLC) -** shares information with NCC-OSAEC-CSAEM to combat OSAEC and CSAEM.

- **Congressional Oversight Committee -** monitors law implementation and recommends measures for effective enforcement.

➤ Checkpoint Question 4.5. How can laws be enforced starting at the community level? What roles should government, schools, community leaders, and youth groups play?

➤ Activity 4.5. Policy Drafting Workshop

In this activity, develop a draft policy or ordinance based on Republic Act No. 11930 for a local government unit (LGU), or your barangay, or the school you belong with. Keep in mind that what you will produce here can be an advocacy or lobbying document with the LGU, barangay, or school.

INSTRUCTIONS:

1. Divide yourselves into teams (3-5 members per team).
2. Each team is tasked with drafting a local ordinance or policy that aligns with the provisions of Republic Act No. 11930. The policy should include:
3. Objectives
4. Responsibilities of various local stakeholders
5. Procedures for reporting and responding to cases of online sexual abuse
6. Penalties for non-compliance
7. Support services for victims
8. Teams work together to create their policy draft. Each team presents their draft policy to the rest of the participants for feedback and discussion.
9. After each presentation, other teams review feedback and make revisions to their policies.

THE PHILIPPINE CRISIS OF ONLINE CHILD SEXUAL EXPLOITATION

In 2018, the Department of Justice Office of Cybercrime received 579,006 cyber tips for the online sharing, re-sharing, and selling of child sexual abuse images and videos. A survey by the International Justice Mission (IJM) found that nearly half a million (1 in every 100 Filipino) children were trafficked to produce new child sexual exploitation. Further, nearly a quarter of a million (1 in every 1,000) adult Filipinos trafficked children to produce these materials in 2022.

The Philippines has become the world's largest known source of online child sexual exploitation, with endemic poverty helping drive a surge in abuse, according to the IJM aid group's seven-year study. Parents and relatives were responsible for facilitating the abuse in nearly all cases.

According to the National Study on OSAEC conducted by De La Salle University with the Department of Social Welfare and Development and UNICEF Philippines, there are several reasons why this is happening to our children.

- Perpetrators around the world easily find willing Filipino adults who can pay to abuse and exploit children.
- Most Filipinos can speak and understand English.
- Children are usually left at home without the presence of their parents because they are away for work every day, and some even are abroad.
- Most families live below the poverty line and think this is an easy way to earn money. They think selling children online does not harm them because they are not "touched."
- The internet is easy to access.
- The issue is not openly discussed, and ignorance is feigned. This is not discussed with the family or on social media.
- Adults don't realize the lasting impact of this abuse on children.

➤ Checkpoint Question 4.6. How can the different entities such as the government, schools, parents, and youth groups protect children against OSAEC?

KEEPING CHILDREN SAFE FROM ONLINE SEXUAL ABUSE AND EXPLOITATION

Child Right's Network Philippines (CRN) and SaferKidsPH have shared valuable internet safety tips specifically designed to protect children from the harmful effects of online activities. As youth, it's important to take proactive steps to ensure the safety of younger individuals when they use the internet. Here are some practical tips you can follow to protect children:

- **Educate Them -** teach children about the importance of keeping personal information private online, not talking to strangers, and engaging in positive online activities.

- **Monitor Online Interactions -** keep an eye on children's online activities, guide them in safe interactions, and establish clear rules about internet usage.

- **Encourage Reporting -** let children know they can talk to you if they see anything inappropriate online and encourage them to report it promptly.

- **Set Boundaries -** establish clear rules about who children can interact with online and when they can use the internet to create a safe online environment.

- **Promote Positive Content -** encourage children to engage in positive online activities and avoid negative or harmful content, while also supervising downloads and teaching critical thinking skills.

As youth, you also need to protect yourself from OSAEC.

- Guard Personal Info and Privacy: Keep personal details private online, such as full names, addresses, or school names. Only share passwords with trusted individuals like parents or guardians to protect your online accounts. Take control of your privacy settings on social media to ensure only friends and family can see your content.

- Be Wary and Trust Your Instincts: Be cautious when chatting with strangers online and avoid meeting them in person without telling a trusted adult. Trust your instincts and log out if something feels off during an online chat. You don't have to keep talking to someone if you're not comfortable.

- Stay Positive and Safe: Ignore negative or inappropriate content online and keep your online space positive and safe.

- Speak Up and Report: If you see anything inappropriate online, report it immediately to help stop someone from getting hurt. Your actions can make a difference in keeping the online community safe.

- Stay Informed and Educate Others: Stay updated on the latest online safety practices and educate your friends and peers about the importance of protecting themselves from OSEAC. By spreading awareness and sharing knowledge, you contribute to creating a safer online environment for everyone.

To report cases of online child sexual abuse and exploitation, call:

- **Actionline Against Human Trafficking:** 1343 for Metro Manila and (02) 1343 for outside Metro Manila
- **MAKABATA Helpline** 1383
- **Philippine Red Cross:** 143
- **National Emergency Hotline:** 911
- **PNP Aleng Pulis:** 0919 777 7377
- **UP-PGH COVID-19 Bayanihan Operations Center:** 155 200
- Refer to local organization, offices, or school's hotline if applicable.

➤ Activity 4.6 Guardians of the Digital Galaxy: Poster against OSAEC

One effective way to combat OSAEC is by encouraging individuals to report any instances or suspicions of online abuse or exploitation they encounter. Reporting such cases can help authorities intervene and provide support to victims, ultimately holding perpetrators accountable for their actions. In this activity, you will have the opportunity to design a poster that effectively communicates the importance of reporting OSAEC and encourages people to take action against this form of exploitation.

INSTRUCTIONS:

1. Work in groups of three. Identify the key messages you want to convey through your poster. Consider emphasizing the importance of reporting suspicious online activities, raising awareness about the signs of OSAEC, and promoting the protection of children online.

2. Before designing your poster, consult with a parent or guardian about their views on online safety and reporting instances of online abuse or exploitation. Discuss their experiences, concerns, and any advice they may have regarding protecting children in the digital space.

3. Materials will be provided for the poster. Start to design your poster once you have decided on your layout, imagery, text, and overall messaging.

4. Stick your poster on the designated area: Guard

➤ **Checkpoint Question 4.7. As young people, who can also be subjected to OSAEC, how can we raise awareness among our peers about the risks of online exploitation and empower them to recognize and report suspicious activities to relevant authorities or helplines?**

➤ MODULE 5
Fostering Digital Well-being

MODULE OVERVIEW:

In an era where technology permeates every aspect of our lives, it is essential to assess its impact on our mental health and overall well-being. This module provides you with interactive tools and reflective exercises designed to help you navigate the digital landscape more mindfully. You will explore the benefits and challenges of digital technology, from understanding digital overload and its mental health effects to recognizing signs of internet and mobile gaming addiction, and learn strategies for fostering a balanced, healthy relationship with digital devices.

MODULE OBJECTIVES:

At the end of this module, the learners can:

- Evaluate the concept of digital well-being and understand its critical role in balancing digital and offline life.
- Analyze the mental health impacts associated with digital overload, including stress, anxiety, and physical symptoms.
- Identify warning signs and consequences of excessive digital use, with a focus on internet and mobile gaming addiction, and propose preventive measures.
- Develop and implement practical strategies and action plans, including family-based initiatives, to promote digital well-being.

Sub-Topics:

- Introduction to Digital Well-being
- Internet and Mobile Gaming
- Practicing Activities to Promote Digital Well-being

Materials Needed: pens/pencils, projector, screen, speakers, printed worksheets and scenario cards, poster boards, markers, adhesives

Topic	Activity	Description	Duration
Pre-Activity	Introduction to the Module	Overview of module objectives, introduction to the key topics such as digital well-being and internet and mobile gaming.	10 mins
	Pre-Activity 5: Digital Well-being Self-Assessment	A reflective exercise using a self-assessment tool to evaluate digital habits across six key areas by answering 18 questions and calculating scores to identify areas for improvement.	30 mins
Introduction to Digital Well-being	Discussion	Defining digital well-being, highlighting its benefits and warning signs of digital overload such as stress, eye strain, and reduced face-to-face interactions.	15 mins
	Activity 5.1: A Day in a Life of a Digital Citizen	Participants create a 24-hour visual schedule, mapping out their daily digital and non-digital activities to reflect on their current habits and identify opportunities for a healthier balance.	20 mins
	Discussion	Explore how excessive screen time and multitasking can lead to mental and physical strain, including symptoms like anxiety, irritability, and sleep disturbances.	15 mins
	Activity 5.2: Digital Balance Check-in	Involves reflective questions about gaming habits to evaluate if digital engagement, particularly gaming, is balanced with daily life priorities.	20 mins

Topic	Activity	Description	Duration
	Discussion	Discuss how moderate gaming can boost focus and socialization while also addressing potential negative effects such as low mood, social anxiety, and lack of motivation when gaming is excessive, along with strategies for maintaining a healthy balance.	20 mins
Practicing Digital Well-being	Discussion	Share best practices for managing digital habits and seeking positive content to enhance overall well-being.	15 mins
	Activity 5.3: A Better Day in the Life of a Digital Citizen	Encourages learners to design an ideal daily schedule that integrates digital well-being practices such as digital detox breaks, creative pursuits, and quality offline interactions.	20 mins
	Activity 5.4 Family Digital Well-being Action Plan (Take Home Activity)	A take-home activity that involves family participation to reflect on collective digital habits and collaboratively create an action plan with 2–3 targeted changes for fostering a healthier digital environment at home.	15 mins
		ESTIMATED TOTAL HOURS	**3 hours**

➤ Pre-Activity 5 Digital Well-being Self-Assessment

With the prevalence of smartphones, social media, and online platforms, it's essential to pause and reflect on our digital habits and well-being. This Digital Wellbeing Self-Assessment Tool was developed by Sentient Digital & Mind over Tech in 2021. It is designed as a reflective exercise to help you become more aware of how your technology use impacts your life, and to support you in creating a healthier relationship with digital devices.

INSTRUCTIONS:

1. Begin by visiting the website for the full set of instructions. https://www.cfcs.org.uk/app/uploads/2024/01/CFCS_DigitalWellbeingSelfAssessment.pdf

2. Read through the document carefully to understand the purpose of the assessment and the detailed process involved.

The self-assessment evaluates your digital habits across six key areas:

- Wellbeing (W)
- Boundary (B)
- Communication (Cm)
- Focus (F)
- Connection (Cn)
- Purpose (P)

3. There are 18 questions in total. Your response to each question should be a number between 0 (Never/Not at all) and 10 (Always/Completely).

4. For each question, locate the six corresponding columns. Each column is labeled with one of the six areas and includes either a '+' or '–' sign:

5. '+' indicates that the chosen number should be added.

6. '–' indicates that the chosen number should be subtracted.

7. Write your number in the appropriate column for each question. After answering all questions, add up the three numbers in each column. For any score written in a box marked with a '–', subtract that value.

8. Your final score for each area will be between 0 and 20. Use the guide in the document to interpret your results. Review your results and identify areas where improvements can be made.

INTRODUCTION TO DIGITAL WELL-BEING

Digital well-being refers to the state of maintaining a healthy and balanced relationship with technology and digital devices. It encompasses various aspects, including physical, mental, and emotional well-being, in the context of digital interactions. Digital well-being involves being mindful of one's digital habits, managing screen time effectively, and prioritizing activities that promote overall wellness. It is a complex concept involving how technology affects us individually and as a society.

- From a personal perspective, it's about understanding the good and bad sides of using digital devices and finding ways to use them to make us feel good. For example, managing screen time and being mindful of technology use.

- From a societal or organizational standpoint, providers of digital systems, services, and content must ensure that these are well-managed, supported, accessible, and fair for all users. Additionally, they must empower and enhance the capabilities of users so that everyone engaging with their offerings can do so in a manner that supports and enhances their well-being.

What could be the warning signs of excessive use of devices?

- Experiencing eye strain symptoms such as watering, tiredness, blurred vision, or headaches.
- Engaging more in digital communication than in face-to-face interactions.
- Feeling anxious when unable to access digital devices.
- Experiencing stress or overwhelm due to information overload.
- Comparing oneself to others frequently.
- Having trouble sleeping or experiencing disruptions in sleep patterns.
- Decreased frequency of face-to-face conversations with friends and family.
- Feeling emotionally disconnected from close relationships.
- 22. Finding that internet use hinders completion of offline tasks.
- 23. Feeling overwhelmed by internet or social media usage.

➤ Activity 5.1. A Day in a Life of a Digital Citizen

As our reliance on digital devices continues to grow, it becomes increasingly important to reflect on the impact of our digital habits on our overall well-being. By creating a visual representation of your daily routines, you can gain insight into your digital habits, identify areas for improvement, and strive for a healthier balance between digital engagement and offline activities.

INSTRUCTIONS:

1. Draw a clock that displays all 24 hours of the day.

2. Reflect on your typical daily routine, including both digital and non-digital activities. Consider how you spend your time on digital devices, such as smartphones, computers, and tablets, and activities that do not involve technology.

3. Use the clock template to visually represent your daily schedule. Divide the clock into segments corresponding to different activities throughout the day.

4. Label each segment with specific activities, indicating whether they are digital or non-digital. For example, you may allocate time for waking up, eating meals, attending classes or work, exercising, socializing, studying, using social media, watching TV, and sleeping.

5. Be honest and accurate in depicting your daily habits and routines. Include both productive and leisure activities, as well as any breaks or downtime.

6. Once you have completed your visual schedule, take a moment to reflect on your digital habits and overall balance between digital and non-digital activities.

7. Share your completed visual schedule with a small group, discussing your observations and insights about your digital life.

MENTAL HEALTH IMPACTS OF DIGITAL OVERLOAD

Digital overload occurs when individuals spend excessive time-consuming media through screens, such as smartphones, computers, or TVs. This prolonged exposure can overwhelm the brain's ability to process information effectively, leading to various mental health issues.

Digital overload can result from:

- **Spending too much time on your devices:** If you spend excessive time online without taking regular breaks, you can face digital burnout.

- **Consuming too much information:** The constant availability of information from countless sources can overwhelm your brain. Sometimes, your mind needs a break from all that input.

- **Media multitasking:** Using multiple devices at a time (like checking social media while watching a Netflix show) can overwhelm your brain. Research shows that people who media multitask perform poorly on tasks that require focus.

Symptoms of using too many digital devices:

- **Irritability:** Feeling easily annoyed or angered.
- **Anxiety:** Experiencing increased nervousness or worry.
- **Vision Problems:** Suffering from eye strain, blurred vision, and dry eyes1.
- **Sleep Difficulties:** Having trouble falling or staying asleep.
- **Mood Swings:** Undergoing rapid changes in mood.

➤ Checkpoint Question 5.1. What factors contribute to the frequency of individuals looking down at their phones in various social settings?

INTERNET AND MOBILE GAMING

Internet and mobile gaming offer engaging adventures, social connections, and cognitive challenges. When enjoyed in moderation, gaming can be a positive and enriching part of your digital life. However, it is essential to maintain a balanced approach so that gaming enhances your wellbeing without overshadowing other important areas of life. Benefits of moderate gaming include:

- **Cognitive and Social Gains:** Moderate gaming has been linked to improved focus, strategic thinking, multitasking, and emotional regulation.

- **47. Stress Relief and Connection:** Enjoyable gaming experiences can provide stress relief and foster online communities and friendships that complement real-life relationships.

Excessive gaming, sometimes referred to as Internet Gaming Disorder (IGD) or video game addiction, is characterized by compulsive and excessive use of online games or applications. This behavior can interfere with daily responsibilities, self-care, relationships, academic performance, and work productivity. People experiencing gaming addiction may find it difficult to control their gaming habits and might even show withdrawal symptoms when they are not gaming.

Signs and Symptoms of Gaming Addiction:

- **Poor Performance -** Neglecting school, work, or household responsibilities due to gaming.

- **Withdrawal Symptoms -** Experiencing sadness, anxiety, or irritability when unable to game.

- **Increased Time Investment -** Needing more gaming time to achieve the same level of enjoyment.

- **Coping Mechanism -** Relying on video games as the primary way to handle negative moods or life challenges.

➤ Activity 5.2 Digital Balance Check-In

Internet and mobile games have become integral to modern entertainment, offering a wide range of experiences, from action-packed adventures to brain-teasing puzzles. We all love crushing levels and conquering quests in our favorite mobile games. But sometimes, it's good to take a break from the action and check in with ourselves. This activity is like a Digital Balance Check-In to see how mobile games fit into your life.

INSTRUCTIONS:

1. Grab your paper and answer these questions truthfully:

2. How many hours, on average, do you spend playing internet or mobile games each day?

3. Are there any important things you sometimes forget to do (homework, chores, hobbies, hanging out with family) because you're gaming?

4. Do you have specific time each day for internet and mobile games, or do you play whenever you have a free moment?

5. How do you feel when you can't play internet or mobile games for a while? (Bored? Anxious? Restless?)

Psychological Benefits and Challenges of Gaming

Moderate gaming can support mental skills such as focus, strategic thinking, and emotional regulation. On the positive side, moderate gaming has been associated with benefits such as socialization, improvement in focus, multitasking, working memory, cognition, and emotional regulation. Some studies have even suggested that gaming can have mental health benefits, such as mitigating symptoms of depression and anxiety. Many studies suggest that when gaming is balanced with other activities, it can boost socialization, working memory, and even help mitigate feelings of depression or anxiety. However, being mindful of our habits is key:

- While gaming can be uplifting, too much may lead to neglecting other life areas, potentially causing low mood or diminished motivation.

- Gaming offers online communities and friendships, but real-life interactions are also essential for emotional fulfillment.

- Enjoyable gaming experiences contribute to stress relief, yet diversifying your coping strategies can strengthen your resilience.

- A balanced digital life nurtures relationships at home and in your community, ensuring that digital interactions complement rather than replace face-to-face connections.

In the Philippines, we have a reality that over 95.8% of internet users between the ages of 16 to 64 are gamers, making it the country with the highest number of gamers worldwide. The psychological effects of excessive gaming can be both positive and negative, depending on factors such as the frequency and intensity of gaming, as well as individual differences in mental health and personality traits.

Excessive gaming can have profound and wide-ranging negative effects on mental health, including:

- **Depression:** Neglect of social relationships and healthy habits may lead to feelings of sadness and hopelessness.

- **Social Anxiety:** Relying heavily on online interactions can result in withdrawal from fulfilling real-life social experiences.

- **General Anxiety:** Using gaming as an escape may prevent individuals from addressing underlying issues, worsening anxiety.

- **Lack of Motivation:** Excessive gaming can crowd out other interests and responsibilities.

- **Poor Emotional Regulation:** Difficulty managing emotions can lead to increased aggression and further mental health challenges.

- **Interpersonal Conflict:** Toxic online environments and aggressive behavior in games may strain relationships.

- **Suicidal Thoughts:** In severe cases, when gaming becomes the sole focus, individuals may experience thoughts of self-harm.

➤ Checkpoint Question 5.2. Should the internet and video games be banned at a certain age? Should school children and youth be allowed to play internet and video games?

STRATEGIES FOR FOSTERING A HEALTHY DIGITAL RELATIONSHIP WITH GAMING

Excessive gaming can have detrimental effects on mental health and overall well-being. To prevent addiction and maintain a healthy relationship with gaming, consider the following strategies:

- **Establish boundaries on gaming time:** Set clear limits on how much time you spend playing video games each day. By doing so, you can prevent excessive immersion in gaming and ensure that you allocate time for other important aspects of life, such as work, school, socializing, and physical activity.

- **Promote diverse interests and activities:** Explore a variety of hobbies and activities beyond gaming. Engaging in diverse interests fosters a well-rounded lifestyle and reduces the likelihood of becoming overly fixated on video games. Whether it's sports, music, art, or outdoor activities, finding alternative outlets for leisure can enrich your life and provide balance.

- **Converse about gaming addiction:** Have open and honest discussions with your parents, friends, and trusted peers about the risks of gaming addiction. Share your concerns and listen to their perspectives. By raising awareness and encouraging dialogue, you can collectively support each other in maintaining a healthy balance between gaming and other activities.

- **Distinguish between healthy gaming and addiction:** Educate yourself about the differences between normal gaming habits and addictive behavior. Learn to recognize warning signs such as neglecting responsibilities, withdrawal symptoms when not gaming, and impaired social functioning. By understanding the nuances of gaming addiction, you can identify potential red flags early on and take proactive steps to address them.

PRACTICING DIGITAL WELL-BEING

Practicing digital Well-being involves prioritizing self-control and using digital devices intentionally to benefit your physical and mental health, relationships, learning, safety, and work-life balance. But how can we practice digital well-being?

- **BE CONSCIOUS:**
    - **Monitor Your Digital Habits:** Keep track of how much time you spend using digital devices and how you spend that time. Use features available on smartphone applications to monitor your usage patterns.
    - **Identify Distractions:** Recognize what distracts you from your work or personal life when you're online.
    - **Monitor Mood Impact:** Pay attention to how engaging with digital devices and online content affects your mood and energy levels. Reduce time spent on activities that negatively impact your mood and replace them with uplifting alternatives.
    - **Embrace Boredom:** Instead of mindlessly scrolling through social media, engage in productive activities such as reading articles, watching videos, or conversing with friends.
- **BE INTENTIONAL:**
    - **Set Time Limits:** Establish and stick to specific time limits for using digital devices. Utilize reminders or alarms to help you adhere to these limits effectively.
    - **Take Breaks:** Follow the 20-20-20 rule to reduce eye strain. Take a 20-second break every 20 minutes to focus on something at least 20 feet away.
    - **Maintain Good Posture:** Be mindful of your posture while using digital devices to prevent strain on your spine and alleviate discomfort.
    - **Establish Internet Bedtime:** Avoid using digital technology before bedtime to improve sleep quality. Activate 'do-not-disturb' settings to prevent interruptions during sleep hours and promote restful sleep.

- **Seek Positive Content:** Follow websites or social media accounts that share positive and accurate content to uplift your mood and enhance your mental well-being. Utilize content restriction features to filter out negative content.

- **Ground Yourself in Reality:** Remember that social media often presents an idealized version of life. Take time to reflect on your own experiences and maintain perspective.

➤ Activity 5.3A Better Day in the Life of a Digital Citizen

As our reliance on digital devices continues to grow, it becomes increasingly important to reflect on the impact of our digital habits on our overall well-being. By creating a visual representation of your daily routines, you can gain insights into your digital habits, identify areas for improvement, and strive for a healthier balance between digital engagement and offline activities.

INSTRUCTIONS:

1. Get a blank clock template that displays all 24 hours of the day, similar to the one used in Activity 5.1.

2. Reflect on the concepts of digital well-being, digital overload, and the impact of technology on your overall well-being that were discussed in previous activities.

3. Consider the digital habits and behaviors that contribute positively to your well-being and those that may detract from it. Think about incorporating practices that promote digital well-being into your daily routine.

4. Using the clock template, visually represent your ideal digital well-being schedule. Divide the clock into segments corresponding to different activities throughout the day, focusing on digital activities that contribute positively to your well-being.

5. Label each segment with specific activities that promote digital well-being, such as mindfulness meditation, taking digital detox breaks, engaging in creative pursuits, spending quality time with loved ones offline, or participating in outdoor activities.

6. Be intentional and realistic in depicting your digital well-being practices, ensuring that they align with your personal values and goals.

7. Once you have completed your digital well-being schedule, take a moment to reflect on how it differs from your typical digital habits and routines. Consider the potential benefits of incorporating these practices into your daily life.

➤ Activity 5.4 (Take Home Activity) Family Digital Well-being Action Plan

Digital devices play a big role in our lives, and sometimes it's helpful to pause and think about how we use them. In this activity, you and your parents will reflect on your digital habits and create an action plan for a healthier balance.

INSTRUCTIONS:

1. Gather your parents or guardian (and better yet the entire family) and set aside a specific time when everyone is available. Choose a quiet, comfortable space free of distractions.

2. Take a few minutes to think about your day-to-day digital activities. Write down the types of activities you do on your phone, computer, or tablet (for example, social media, gaming, homework, or chatting with friends).

3. Note moments when you felt distracted or disconnected, as well as times when technology helped you or made you feel good.

4. Together with your parents, choose 2–3 areas where you'd like to see a change. Write these areas down as "Opportunities for Change."

5. For each area you want to improve, decide on one specific action you can take. Create a simple action plan list with the steps you both agree on.

➤ MODULE 6
Exploring Artificial Intelligence

MODULE OVERVIEW:

Artificial Intelligence (AI) is here. In this module, we will delve into the fascinating realm of AI to understand its significance, applications, and implications. We'll delve into its different types, explore its advantages and disadvantages, and discuss the ethical considerations for responsible AI use.

MODULE OBJECTIVES:

At the end of this module, the learners can:

- Define artificial intelligence, identify its various applications, and the opportunities and challenges it presents.
- Explain the responsible use of AI, including behavioral, ethical, and legal considerations.
- Evaluate the potential contributions of AI applications in education

SUB-TOPICS:

- Artificial Intelligence
- Advantages and Disadvantages of AI
- Ethics and Responsible Use of AI: Behavioral, Ethical, and Legal Considerations

MATERIALS NEEDED: projector, whiteboard/flip chart, markers, timer, slips of paper, hat or bowl, printed role cards/scenario handouts

MODULE FLOW: (Estimated duration may vary depending on the delivery and size of the group.)

Topic	Activity	Description	Duration
Pre-Activity	Introduction to the Module	Overview session introducing the module's objectives, key topics in AI, its applications, and ethical, behavioral, and legal considerations.	10 mins
	Pre-Activity 6: AI or Not	Students decide whether given statements reflect current AI capabilities.	10 mins
Artificial Intelligence	Discussion	Guided conversation to clarify AI definitions, examine real-world examples, and distinguish between advanced machine learning and general AI.	10 mins
	Activity 6.1: My Day, My AI	Reflective activity where students list daily tasks and identify AI involvement, then share their findings to highlight AI's pervasive role.	20 mins
	Discussion	Exploration of technologies powering AI today (machine learning, deep learning, NLP, etc.)	20 mins
Advantages and Disadvantages of AI	Discussion	Balanced discussion weighing AI benefits (efficiency, reduced errors, personalization) against drawbacks (job displacement, ethical issues).	20 mins

Topic	Activity	Description	Duration
	Activity 6.2: Where's the AI?	A charades-style game where teams act out various AI applications drawn from slips of paper, encouraging creative thinking about AI uses.	30 mins
	Discussion	Discussion on how AI is applied across various sectors (healthcare, finance, transportation, etc.) and its transformative effects on these fields.	20 mins
Ethics and Responsible Use of AI	Discussion	In-depth discussion covering human-AI interaction, privacy, bias, legal liability, and the need for regulation to address societal challenges.	20 mins
	Activity 6.3: Ethics Challenge	Roleplaying exercise with groups (School Security, Student Representatives, Parents, Tech Experts, Ethics Committee) debating an AI security system.	90 mins
	Discussion	Concluding discussion on responsible AI principles, examining frameworks for transparency, accountability, and fairness in AI development.	20 mins
		ESTIMATED TOTAL HOURS	4 hours and 30 minutes

➤ Pre-Activity 6 AI or Not?

Are you curious about how Artificial Intelligence (AI) is used in our world? In this activity, we'll test your knowledge and see if you can tell the difference between what AI can already do and what's still in the realm of science fiction!

INSTRUCTIONS:

1. Take a close look at each statement below and decide whether it represents something AI can currently do (AI) or something that's still under development (Not AI Yet).

a. AI can draw a picture of a funny monster you describe.
b. AI can play your favorite song when you ask it to.
c. AI can clean your room, make your bed, and prepare your food.
d. AI can help you learn a new language.
e. AI can teleport you anywhere in the world.

Answer Key:

a. AI - generative AI can create new images
b. AI - virtual assistants can use music streaming services
c. Not AI Yet - robots for home cleaning are still quite limited
d. AI - some language learning apps use AI
e. Not AI Yet - teleportation is still science fiction!

ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI) is a term used to describe computer systems that can perform complex tasks that were previously only possible for humans, such as decision making, problem-solving and reasoning. Today, AI is used to describe a wide range of technologies that power many of the services and products we use in our daily lives. These include apps that recommend TV shows and chatbots that provide real-time customer support. However, it's important to note that not all these technologies qualify as artificial intelligence in the traditional sense. Despite this, the term is used frequently due to its widespread usage and applicability in various fields.

UNDERSTANDING ARTIFICIAL INTELLIGENCE

While the term AI is often used to describe different technologies, some argue that much of the technology used today actually constitutes highly advanced machine learning that is simply a first step towards true artificial intelligence or "general artificial intelligence" (GAI). There are philosophical disagreements over whether "true" intelligent machines actually exist. However, when most people use the term AI today, they are referring to machine learning-powered technologies such as ChatGPT or computer vision that enable machines to perform tasks that were previously only possible for humans, such as generating written content, steering a car, or analyzing data. Some of the most common examples of AI in use today include:

- **ChatGPT:** Uses large language models (LLMs) to generate text in response to questions or comments posed to it.
- **Google Translate:** Uses deep learning algorithms to translate text from one language to another.
- **Netflix:** Uses machine learning algorithms to create personalized recommendation engines for users based on their previous viewing history.
- **Tesla:** Uses computer vision to power self-driving features on their cars.

➤ Activity 6.1My Day, My AI: A Personal Inventory

In today's digitally-driven world, artificial intelligence (AI) plays an increasingly prominent role in shaping our daily experiences. From using social media to completing homework assignments, AI tools are all around us, often making our lives easier without us even realizing it. This activity is a quick and engaging way to identify the AI tools and technologies you use throughout your day.

INSTRUCTIONS

1. Take a moment to think about the tasks and activities you do regularly, both at school and at home. These could include things like studying, communicating with friends, playing games, shopping online, or even watching videos.

2. Now, think about each of these tasks and activities and consider if there are any AI tools or technologies involved. For example, do you use virtual assistants like Siri or Google Assistant to set reminders or answer questions? Do you notice personalized recommendations when you watch videos or shop online?

3. Once you've identified some AI tools, share your findings with your classmates. Discuss the different tools you've come across and how they enhance your daily tasks.

4. After the sharing, let's think about the following questions:
   - How does it feel to realize that AI is so prevalent in your daily life?
   - Are there any AI tools that surprised you?

➤ Checkpoint Question 6.1. How do you feel about the possibility of truly intelligent machines in the future? What benefits or challenges do you think such advancements might bring to society?

CURRENT AI TECHNOLOGIES

In the ever-evolving field of Artificial Intelligence (AI), a range of powerful technologies are shaping the way we interact with machines. These current AI technologies are transforming industries and daily life by enabling machines to learn from data, understand human language, and interpret the visual world. This explosion of AI capabilities is fostering new applications and pushing the boundaries of what machines can achieve.

- **Machine Learning (ML):** The foundation of many AI applications. ML systems learn and improve from data. They can be trained on labeled data (inputs with desired outputs) or through finding patterns in unlabeled data.

- **Deep Learning:** Inspired by the human brain, it uses artificial neural networks for complex tasks like image recognition. Example is image recognition software trained on massive datasets of labeled images to identify objects in new pictures.

- **Natural Language Processing (NLP):** Enables machines to understand and process human language. Like teaching a computer to speak our tongue. NLP is used in chatbots and virtual assistants that understand your voice commands.

- **Speech Recognition (Automatic Speech Recognition, ASR):** A subfield of NLP that deals with converting spoken language into text. It's crucial for applications like voice assistants and dictation software. Speech recognition involves capturing audio, converting it to a digital format, analyzing the sounds, and translating them into words.

- **Computer Vision:** Equips machines with the ability to interpret and analyze visual information. Self-driving cars use computer vision to perceive their surroundings.

- **Generative AI:** The creative side of AI, allowing machines to generate entirely new content. It can create realistic images, compose music, or write creative text formats.

➤ Checkpoint Question 6.2. How often do you use these AI technologies in your day-to-day activities? Are you using them quite often?

ADVANTAGES AND DISADVANTAGES OF AI

While Artificial Intelligence (AI) promises a future filled with automation, efficiency, and groundbreaking advancements, it's not without its challenges.

1. ADVANTAGES OF AI:

a. **Increased Efficiency and Productivity:** AI can automate repetitive tasks, streamline processes, and work 24/7, leading to increased efficiency and productivity for businesses.

b. **Reduced Errors and Risk:** AI can minimize human error and take on risky tasks, improving safety and accuracy in various fields.

c. **Data Analysis and Insights:** AI can analyze vast amounts of data to identify patterns and trends, providing valuable insights for businesses and organizations.

d. **Unbiased Decision-Making:** AI can make decisions based on data without human biases, potentially leading to fairer outcomes in areas like loan approvals or job applications. (Note: This depends on the training data used to create the AI)

e. **Reduced Costs:** In the long run, AI can reduce costs by automating tasks and improving efficiency.

f. **Enhanced User Experience:** AI personalizes services and recommendations, creating a more user-friendly experience.

g. **Innovation and Progress:** AI can drive innovation in various fields, leading to new discoveries and advancements.

2. DISADVANTAGES OF AI:

a. **Job Displacement:** AI automation may lead to job losses in certain sectors as machines take over tasks previously done by humans.

b. **Data Privacy Concerns:** AI systems rely heavily on data, raising concerns about data privacy and potential misuse of personal information.

c. **Lack of Creativity and Emotion:** AI currently lacks human creativity and emotional intelligence, which are crucial for tasks requiring innovation or human interaction.

d. **Potential Bias:** AI algorithms can perpetuate biases if trained on biased datasets. Careful monitoring and quality checks are necessary.

e. **Degradation and Outdatedness:** AI systems can degrade over time or become outdated if not regularly updated and maintained.

f. **Limited Learning:** Most AI systems require human intervention to learn and improve; they may not learn from their own experiences as effectively as humans.

g. **Ethical Concerns:** AI raises ethical concerns about data privacy, responsible development, and potential misuse.

➤ Activity 6.2. Where's the AI?

This activity will challenge you to think about how you understand AI and its applications in various aspects of our lives. By playing a game of charades, you will try to guess where AI can be used.

INSTRUCTIONS:

1. Divide the class into two teams. As a class, brainstorm a list of different applications of AI in various fields like healthcare, transportation, entertainment, and more.

2. Write each application on a separate slip of paper. Fold the slips of paper and place them all in the hat or bowl.

3. Each team will take turns acting out applications of AI. Each team will get 3 minutes and guess as many applications as they can.

4. One member from the playing team picks a slip of paper, reads it silently, and then acts out the application for their team to guess. Remember, no sounds allowed – gestures and facial expressions are key!

5. Then another member from the playing team will pick another slip of paper to act out.

6. The team with the most points at the end wins. Remember that the words or phrases do not need to be exactly guessed as long as it describes what the actor is trying to act out based on the slip of paper.

APPLICATIONS OF ARTIFICIAL INTELLIGENCE

With these advantages and despite the challenges, AI technologies find applications across diverse sectors, driving innovation, efficiency, and productivity. A lot of sectors and industries can benefit from AI tools and technologies. Some notable applications of AI are:

- **Healthcare:** AI is revolutionizing healthcare by enabling early disease detection, personalized treatment plans, medical imaging analysis, drug discovery, virtual health assistants, predictive analytics for patient outcomes, and robotic surgeries.

- **Finance:** In the finance sector, AI powers algorithmic trading, fraud detection and prevention, credit scoring, risk assessment, customer service chatbots, personalized financial advice, and compliance monitoring.

- **Transportation:** AI is transforming transportation through autonomous vehicles, traffic management systems, predictive maintenance for vehicles and infrastructure, route optimization, ride-sharing algorithms, and smart logistics solutions.

- **Retail:** In retail, AI is utilized for demand forecasting, inventory management, personalized product recommendations, virtual shopping assistants, supply chain optimization, and customer sentiment analysis.

- **Manufacturing:** AI-driven robotics, predictive maintenance, quality control, supply chain optimization, smart factories, autonomous equipment operation, and adaptive manufacturing processes are revolutionizing the manufacturing industry.

- **Education:** AI is enhancing education through personalized learning platforms, intelligent tutoring systems, automated grading and assessment, adaptive learning algorithms, language translation tools, and virtual classrooms.

- **Entertainment:** AI technologies are reshaping the entertainment industry through content recommendation algorithms, personalized content creation, virtual reality experiences, gaming AI, emotion recognition in content consumption, and music and video production tools.

➤ Checkpoint Question 6.3. What should be the extent of the use of AI in education and learning? Should it be banned or restricted?

ETHICS AND RESPONSIBLE USE OF AI

AI is rapidly transforming our world, bringing significant advancements across various fields. However, alongside its benefits, AI raises critical questions about its responsible use. Let us explore the behavioral, ethical, and legal considerations surrounding AI development and implementation.

1. BEHAVIORAL CONSIDERATIONS:

   a. **Human-AI Interaction:** How will people behave differently in the presence of AI? Will trust in AI lead to over-reliance, or will there be a fear of losing control?

   b. **Addiction and Dependence:** Could certain AI applications become addictive, especially those designed for entertainment or social interaction?

   c. **Privacy and Transparency:** Will people feel comfortable interacting with AI if they don't understand how it works or how it uses their data?

   d. **Human Oversight:** AI systems should be designed with human oversight and control mechanisms.

2. ETHICAL CONSIDERATIONS:

   a. **Bias in AI:** AI algorithms can perpetuate existing biases present in the data they are trained on. This can lead to discriminatory outcomes in areas like loan approvals, hiring, or facial recognition.

   b. **Algorithmic Justice:** AI used in legal systems needs to be fair and unbiased to avoid perpetuating discrimination in areas like risk assessment.

   c. **Privacy and Surveillance:** The proliferation of AI-driven surveillance technologies raises concerns about individual privacy, data security, and the potential for mass surveillance and government overreach.

   d. **Job Displacement:** Automation through AI may lead to job losses in certain sectors. Strategies for retraining and upskilling the workforce will be crucial.

   e. **Autonomous Weapons:** The development of autonomous weapons systems powered by AI raises ethical questions about the delegation of lethal decision-making to machines, accountability for actions, and the potential for unintended consequences and escalations in conflicts.

3. LEGAL CONSIDERATIONS:

a. **Liability and Responsibility:** Determining who is responsible for AI actions is complex. Clear legal frameworks are needed to address liability in cases of malfunction or misuse.

b. **Regulation of AI:** Governments are grappling with how to regulate AI development and use it to ensure safety, security, and ethical implementation.

c. **Data Privacy:** AI systems often rely on collecting and analyzing vast amounts of personal data. This raises concerns about data privacy and potential misuse of information.

➤ Checkpoint Question 6.4. What do you think are the different considerations we need to address with regards to the use of AI in education?

➤ Activity 6.3. Ethics Challenge: Roleplaying for Responsible Use

With the different challenges in the use of AI, ensuring that we use it responsibly is critical. This role-playing activity explores the ethical and responsible use of AI through a simulated scenario. Get ready to step into different roles and champion your assigned positions.

INSTRUCTIONS:

1. Divide into 5 groups.

2. Take a look at the following scenario:

3. Your school board is debating the implementation of a new AI-powered security and attendance system. This system uses facial recognition technology to identify students entering and leaving the school and can also monitor student movement within hallways.

4. Each group will be assigned a role to play, with details different roles and their objectives.

a. **School Security Team:** You are responsible for ensuring the safety and well-being of students and staff. Convince the board of the system's effectiveness in deterring crime and improving school safety. Address concerns about accuracy and potential misuse.

b. **Student Representatives:** You represent the student body and advocate for student rights. Highlight potential privacy concerns regarding facial recognition technology and data collection. Champion for a school environment that fosters trust and openness.

c. **Parents' Association:** You represent the concerns of parents regarding their children's privacy and safety. Voice concerns about data security, potential misuse of information, and the overall impact on the school climate. Advocate for open communication and parental involvement in decision-making.

d. **Tech Experts:** You are a team of technology professionals specializing in AI and facial recognition systems. Analyze the technical aspects of the system and potential challenges with accuracy, bias, and data security.

e. **Ethics Committee:** You are a committee tasked with evaluating the ethical implications of new technologies in the school setting. Consider the ethical principles of fairness, transparency, and accountability.

You will be given 10 minutes to research and reflect on your assigned role. Discuss potential arguments and perspectives and their implications in schools.

6. Each group presents their viewpoints and engages in a dialogue with other groups. Remember to stay in character and defend your positions.

7. After the roleplaying, think about the following questions:

   a. What were the key challenges faced by each group?

   b. Did any perspectives change during the role-playing?

   c. What are some key takeaways regarding responsible AI use in schools?

RESPONSIBLE USE OF AI

Responsible AI is a set of principles and declarations used to regulate the development and governance of artificial intelligence systems. It ensures that AI models are efficient, compatible with regulations, consider ethical and societal implications, track and mitigate bias, build trust, and minimize negative effects. Major tech giants like Google, Microsoft, and IBM have called for AI to be regulated and built their own governance frameworks and guidelines. With the responsible use of AI, we could potentially address the considerations we have mentioned above.

- **BEHAVIORAL**
    - Ensuring transparency and human oversight.
    - Designing AI that complements human capabilities
    - Fostering public education and awareness about AI technologies.
- **ETHICAL**
    - Developing ethical guidelines for AI development and deployment.
    - Investing in research on bias mitigation and fair AI algorithms.
    - Respecting privacy when designing AI technologies.
    - Designing AI systems that are transparent and accountable.
    - Addressing job displacement with upskilling programs and potential policy solutions.
    - Regulating autonomous weapons.
- **LEGAL**
    - Developing legal frameworks for AI responsibility.
    - Strong data privacy laws and enforcement mechanisms are needed.

In a landmark achievement, UNESCO established the world's first global standard for AI ethics – the Recommendation on the Ethics of Artificial Intelligence, adopted by all 193 Member States in November 2021. This framework prioritizes the protection of human rights and dignity, emphasizing core principles like transparency and fairness. Crucially, it recognizes the importance of human oversight in AI development and deployment.

- **Respect, protection and promotion of human rights and fundamental freedoms and human dignity:** AI systems should be designed and used in a way that upholds human rights, freedoms, and inherent dignity. This includes avoiding bias, discrimination, and harm to individuals and communities.

- **Living in peaceful, just and interconnected societies:** AI should contribute to peaceful, just, and interconnected societies. This means fostering collaboration, solidarity, and care for others, while promoting peaceful relations and a healthy environment.

- **Ensuring diversity and inclusiveness:** AI development and use should be inclusive and consider the needs of diverse populations. This means ensuring participation from all groups and avoiding restricting personal choices or experiences.

- **Environmental and ecosystem flourishing:** AI development and use should consider the environmental impact and strive for sustainability. This means minimizing the environmental footprint of AI systems and protecting ecosystems.

➤ Checkpoint Question 6.5. Should AI technologies continue to flourish and be developed?

➤ MODULE 7
Advocating Digital Responsibility

MODULE OVERVIEW:

From Module 1 to 6, you have learned a lot of concepts and skills in becoming a responsible digital citizen. Now, we must pass on the knowledge. This module equips you to become a champion for digital responsibility. From understanding the importance of digital responsibility to learning how to intervene in potential online threats, this module aims to empower you to become advocates for positive digital citizenship.

MODULE OBJECTIVES:

At the end of this module, the learners can:

- Analyze the importance of digital responsibility and its impact on peers.
- Apply strategies for promoting digital responsibility and becoming digital heroes.
- Create effective promotional materials to raise awareness of digital responsibility.

Sub-Topics:

- Becoming a Digital Responsibility ChampionAdvantages and Disadvantages of AI
- Strategies for Promoting Digital Responsibility Among Peers
- Transitioning from Online Bystander to Digital Hero

Materials Needed: printed assessment sheets, writing materials, projector, whiteboard/flip chart, markers, poster boards, colored pencils, paper for worksheets, timer

Module Flow: (Estimated duration may vary depending on the delivery and size of the group.)

Topic	Activity	Description	Duration
Pre-Activity	Introduction to the Module	Introduce the module's objectives and outline the importance of digital responsibility, setting the stage for becoming a digital champion.	10 mins
	Pre-Activity 7: Am I A Champion?	Participants read and rate digital responsibility statements to assess their strengths and areas for growth as future digital champions.	20 mins
Becoming a Digital Responsibility Champion	Discussion	wA conversation on what it means to be a digital responsibility champion and how ethical online behavior can positively influence peers.	15 mins
	Activity 7.1: DigiChamp Persona Activity	In small groups, design a DigiChamp persona by creating a unique character with a name, appearance, personality, and key digital responsibility skills, then share and reflect on the qualities of a digital champion.	45 mins
	Discussion	Explore why practicing digital responsibility is crucial, including its impact on fostering a respectful, safe, and informed online community.	20 mins
Strategies for Promoting Digital Responsibility	Discussion	Discuss actionable strategies to promote digital responsibility, discussing methods such as leading by example, peer mentorship, and social media advocacy.	20 mins

Topic	Activity	Description	Duration
	Activity 7.2: Digital Responsibility Action Plan	Reflect on personal digital habits and set SMART goals; complete an action plan outlining specific step, timelines, and required resources to improve and promote responsible online behavior.	45 mins
From Oline Bystander to a DigiChamp	Discussion	Discuss the transition from a passive online bystander to an active digital hero, focusing on interventions, support strategies, and the importance of speaking up against negative online behavior.	20 mins
	Activity 7.3: Digital Responsibility Awareness Campaign	In groups, develop a mini-campaign to raise awareness about a chosen digital responsibility issue, design promotional materials (e.g., social media posts, videos, or infographics), and present the campaign for feedback and discussion.	
		ESTIMATED TOTAL HOURS	**4 hours**

➤ Pre-Activity 7Am I A Champion?

This activity will help you assess your strengths and areas for growth as a champion for digital responsibility.

INSTRUCTIONS:

1. Read each statement carefully, reflecting different digital responsibility aspects.
2. Rate yourself honestly on a scale of 1 (Never) to 5 (Always).

Statements	
I think twice before sharing personal information online. (Data Privacy)	
I verify the source of information before sharing it online. (Combating Misinformation)	
I treat others online with respect, even if I disagree with them. (Respectful Communication)	
I avoid spreading rumors or gossip online. (Preventing Cyberbullying)	
I am mindful of how much time I spend online and set healthy boundaries. (Digital Wellbeing)	
I speak up if I witness cyberbullying or online harassment happening. (Promoting Safety)	
I am comfortable explaining the importance of digital responsibility to others. (Advocacy)	

Statements	
I actively learn about new online threats and safety measures. (Continuous Learning)	
I use technology in a way that is productive and contributes positively to my life. (Responsible Technology Use)	
I encourage others to think critically about the information they encounter online. (Critical Thinking Promotion)	
Total	

3. Once you've rated yourself on all statements, add up your scores.

    a. **41-50 points:** Congratulations! You demonstrate strong digital responsibility and leadership qualities. Keep inspiring others with your positive online behavior.

    b. **31-40 points:** You're on the right track! You have a solid foundation in digital responsibility. Consider areas where you can further develop your skills and confidence as a champion.

    c. **21-30 points:** There's room for growth in your digital responsibility journey. Review the statements where you scored lower and explore resources to learn more about those specific aspects.

    d. **Below 20 points:** Don't worry, everyone can learn! Use the provided resources to gain a deeper understanding of digital responsibility and how you can become a champion.

BECOMING A DIGITAL RESPONSIBILITY CHAMPION

The digital world offers incredible opportunities, but it also comes with challenges. As you may have learned, digital responsibility entails using technology ethically, safely, and respectfully. As a Digital Responsibility Champion, you play a crucial role in promoting safe, ethical, and informed technology use in your community.

In today's digital landscape, where technology plays an increasingly pervasive role in our daily lives, digital responsibility is more important than ever. It influences how we interact with others online, the content we share, and the impact of our digital footprint. By practicing digital responsibility, individuals can help mitigate risks such as cyberbullying, online harassment, and data breaches, contributing to a more inclusive, respectful, and secure online community.

As you play your role as digital responsibility champions, continue to build your knowledge and skills in digital responsibility. Digital technology and its applications continue to improve and develop so you need to stay abreast with the current digital landscape, current trends, and its impact.

➤ Activity 7.1. DigiChamp Persona Activity: Design Your Digital Hero!

This activity will help you explore the characteristics and qualities that make someone a champion for digital responsibility. Unleash your creativity and design your very own DigiChamp, a digital responsibility champion persona!

Instructions:

1. Make groups of 3-5 members. Each group will make a DigiChamp Persona.

2. A DigiChamp persona is a fictional character who embodies the qualities and characteristics of a champion for digital responsibility.

3. Create your character.
   a. **Name:** Give your DigiChamp a cool and memorable name!
   b. **Appearance:** Sketch or describe your DigiChamp's appearance. How do they dress? Do they have any special gadgets or tools?

c. **Personality:** Describe your DigiChamp's personality. Are they outgoing and social? Analytical and tech-savvy? Creative and expressive?

4. Instead of superpowers, DigiChamps have exceptional digital responsibility skills. Identify the qualities that a DigiChamp has and write it around your character or in any way you prefer.

5. Share your DigiChamp creation with the larger group and reflect the qualities of a digital responsibility champion.

WHY DIGITAL RESPONSIBILITY MATTERS

In today's digital world, where technology is integrated into almost every aspect of our lives, being a responsible digital citizen is crucial. It's not just about protecting yourself online, but also about fostering a positive and healthy online environment for everyone you interact with, including your peers. Here's why digital responsibility matters and how it can impact them:

1. Leading by Example: As you responsibly navigate the online world, you become a role model for your peers. By practicing respectful communication, creating thoughtful content, and critically evaluating online information, you encourage others to do the same, fostering a more positive and inclusive online space.

   a. **Combating Cyberbullying and Online Harassment:** Digital responsibility entails treating others online with respect and empathy. Refusing to engage in cyberbullying or online harassment, and speaking up if you witness such behavior, helps create a safer online environment for your peers and discourages hurtful actions.

   b. **Promoting Source Credibility and Avoiding Misinformation:** Responsible digital citizens critically assess the information they encounter online. By verifying sources and avoiding the spread of misinformation, you assist your peers in navigating the vast online landscape more effectively, shielding them from scams, fake news, and harmful content.

   c. **Building Healthy Online Habits:** Digital responsibility involves setting boundaries with technology. By modeling effective online time management and encouraging

balanced digital habits, you can inspire your peers to adopt practices that promote a healthier lifestyle.

d. **Fostering Digital Privacy Awareness:** Understanding and respecting online privacy is crucial. By being mindful of the information you share online and educating your peers about responsible data sharing, you empower them to safeguard themselves and their personal information.

➤ Checkpoint Question 7.1. How will your actions and behavior affect or influence your peers?

By embodying digital responsibility, you contribute to a better online experience for everyone around you. Your peers will be more likely to:

- Feel safer and more respected online.
- Develop critical thinking skills for evaluating online information.
- Practice responsible online behavior and communication.
- Become aware of the importance of digital privacy.

STRATEGIES FOR PROMOTING DIGITAL RESPONSIBILITY

Now that you've explored the importance of digital responsibility and assessed your champion potential, let's dive into actionable strategies to promote positive change online. To apply strategies for promoting digital responsibility and becoming digital heroes, individuals can engage in various actions aimed at fostering a safer and more ethical online environment.

1. **Lead by Example:** Demonstrate responsible online behavior in your daily interactions. This includes being respectful, critical of information you share, and mindful of your online privacy.

2. **Educational Campaigns:** Organize workshops, seminars, or awareness campaigns to educate peers about the importance of digital responsibility. Provide information on topics such as online safety, privacy protection, and ethical online behavior.

3. **Peer Mentorship Programs:** Establish peer mentorship programs where experienced individuals can guide and support their peers in practicing digital responsibility.

4. **Community Engagement:** Engage with online communities or social media groups dedicated to promoting digital responsibility. Participate in discussions, share resources, and collaborate with others to amplify the message of responsible online behavior.

5. **Social Media Advocacy:** Utilize social media platforms to advocate for digital **r**esponsibility. Share informative posts, tips for staying safe online, and resources for dealing with common digital challenges.

6. **Collaboration with Schools and Institutions**: Collaborate with schools, universities, and other educational institutions to integrate digital responsibility into different school activities and programs inside and out of the classroom.

7. **Online Safety Tools and Resources:** Promote the use of online safety tools and resources that can help individuals protect themselves online.

8. **Advocacy and Policy Change:** Advocate for policy changes and regulations that promote digital responsibility at the local, national, and international levels. Support initiatives aimed at combating cyberbullying, online harassment, and digital discrimination, and work towards creating a safer online environment for all users.

➤ Activity 7.2. Digital Responsibility Action Plan

Becoming a digital responsibility champion means not only embodying these values ourselves but also inspiring others to do the same. In this activity, we will explore actionable strategies for promoting digital responsibility and becoming digital heroes in our communities and online networks.

Instructions:

1. Take a few moments to reflect on your own digital habits and behaviors. Consider areas where you excel in practicing digital responsibility and areas where you could improve.

2. Based on your self-reflection, identify one or two specific goals related to promoting digital responsibility that you would like to focus on. Ensure that your goals are specific, measurable, achievable, relevant, and time-bound (SMART). For example, "I will practice active empathy in all online interactions by responding thoughtfully to comments and messages within 24 hours."

3. Once you have identified your goals, brainstorm actionable steps you can take to achieve them. Consider both short-term and long-term actions that align with your goals.

Goals	Actionable Steps	Timeline	Resources Need (If any)

FROM ONLINE BYSTANDER TO A DIGICHAMP

In the digital world, it's all too easy to witness harmful behavior online and choose to do nothing. However, by transitioning from being a passive bystander to an active digital hero, you can play a crucial role in protecting your internet peers from various threats.

As you have learned, the internet can be a fantastic place for connection, learning, and entertainment. But just like the real world, it also has its share of negativity and threats. In this digital landscape, bystanders play a crucial role in creating a safer and more positive environment for everyone. Imagine you witness someone being bullied in a school hallway. Would you simply walk by, or would you do something to help? The same concept applies online. Bystanders have the power to shift the dynamics of a negative situation.

Unfortunately, the bystander effect can sometimes occur online. People may hesitate to intervene for fear of getting involved, social awkwardness, or not knowing what to do. But remember, even a small act of courage can make a big difference. So, how can you transition from a bystander to a digital hero who protects your online peers from threats? Here are some strategies:

1. **Recognize the Signs:** Be aware of potential online threats like cyberbullying, harassment, or the spread of misinformation. Understanding the signs can help you

identify situations where intervention might be necessary.

2. **Don't Be Silent:** If you see someone being targeted online, don't stay silent. Speak up in a safe and respectful way. You can offer support to the victim, or directly call out the negative behavior.

3. **Report It:** Many social media platforms and online communities have reporting mechanisms for bullying and harassment. If you're uncomfortable intervening directly, report the incident to the appropriate authorities.

4. **Be a Positive Voice:** Sometimes the best way to combat negativity is to drown it out with positivity. Promote kindness and respect in your online interactions. Encourage others to do the same.

5. **Empower Others:** Help your peers understand the importance of digital responsibility. Share resources and tips on online safety and bystander intervention.

➤ Checkpoint Question 7.2. How can you make sure that we spread the knowledge and skills of becoming a responsible digital citizen with our peers?

➤ Activity 7.3. Digital Responsibility Awareness Campaign

The digital world is full of incredible possibilities for connection, learning, and fun. But just like the real world, it also has its challenges. This is where YOU come in! In this activity, you'll step into the role of a digital responsibility champion and create a mini-campaign to raise awareness of a specific digital responsibility issue.

INSTRUCTIONS

1. Group yourselves according to your preference for developing a campaign for Digital Responsibility.

2. Think about the different aspects of digital responsibility. What issue resonates with you the most? Here are some ideas to get you started:
   a. Cyberbullying and online harassment
   b. Misinformation and fake news
   c. Oversharing and online privacy

d. Digital addiction and healthy online habits
e. Responsible online gaming and social interaction

Remember that you can choose an issue outside of the list above.

3. Define your target audience. Who are you trying to reach with your campaign? This will help you tailor your message and platform.

4. Create your key message. What key message do you want to convey about your chosen issue? Focus on the benefits of positive digital behavior.

5. Choose a platform. Choose a platform where your target audience spends their time online. Will you create a social media post, a short video, an infographic, or a combination?

6. Once you have decided on your ideas, begin designing and creating your promotional materials. Use poster boards, markers, colored pencils, or digital design software to bring your ideas to life.

7. After completing your materials, each group will present their work to the group. Explain your design choices, messaging, and intended impact. Listen to feedback and constructive criticism from other participants during the presentations. You will also give feedback to other groups.

As we conclude the DigiChamps modules on instilling digital responsibility in children, it's essential to reflect on the journey we've embarked on together. Throughout this module, we've delved into various aspects of the digital world, empowering you with knowledge and skills to navigate it responsibly.

As you continue your journey beyond this module, remember that digital responsibility is not just a concept but a way of life. By practicing empathy, critical thinking, and ethical behavior in your digital interactions, you can make a meaningful impact on the digital world and inspire others to do the same.

Congratulations on completing the DigiChamps module and thank you for your commitment to promoting digital responsibility. Together, we can create a safer and more responsible digital future for all!

SOURCES OF CONTENT FOR THE ENTIRE MODULE SET

10 Rights of a Child - Resource Hub - Consuelo Alger Zobel Foundation. (n.d.). Resource Hub - Consuelo Alger Zobel Foundation. https://consuelo.org/resources/resource/10-rights-of-a-child/

4 Types of AI: Getting to know Artificial Intelligence. (2024). Coursera. https://www.coursera.org/articles/types-of-ai

Adair, C. (2022). Video games and mental health: How gaming affects your mental health. Game Quitters. https://gamequitters.com/how-gaming-affects-your-mental-health/

Applications of artificial intelligence (AI) | Google Cloud. (n.d.). Google Cloud. https://cloud.google.com/discover/ai-applications

California State University, San Bernardino (2017). Cybersecurity Checklist. https://www.csusb.edu/sites/default/files/upload/file/Personal%20Security%20Checklist.pdf

Cassetto, O. (2023). Cybersecurity Threats: Everything you Need to Know. Exabeam. https://www.exabeam.com/information-security/cyber-security-threat/

China, C. R. (2024). Breaking down the advantages and disadvantages of artificial intelligence. IBM Blog. https://www.ibm.com/blog/breaking-down-the-advantages-and-disadvantages-of-artificial-intelligence/

Cleveland Clinic. (n.d.). Video game addiction. Cleveland Clinic. https://my.clevelandclinic.org/health/diseases/23124-video-game-addiction

Copeland, B. (2024). Artificial intelligence (AI) | Definition, Examples, Types, Applications, Companies, & Facts. Encyclopedia Britannica. https://www.britannica.com/technology/artificial-intelligence/Alan-Turing-and-the-beginning-of-AI

Cyberbullying: What is it and how to stop it. (n.d.). UNICEF. https://www.unicef.org/end-violence/how-to-stop-cyberbullying

Digital wellbeing. (n.d.). JISC. https://digitalcapability.jisc.ac.uk/what-is-digital-capability/digital-wellbeing/

Ethics of Artificial Intelligence | Internet Encyclopedia of Philosophy. (n.d.). https://iep.utm.edu/ethics-of-artificial-intelligence/

Ethics of artificial intelligence. (2024). UNESCO. https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

Fake news and Misinformation: Identifying Fake News. (n.d.). University of Maine. https://libguides.library.umaine.edu/fakenews/

Fran. (2021). What is digital citizenship? | The basics for teachers - FutureLearn. FutureLearn. https://www.futurelearn.com/info/blog/what-is-digital-citizenship-teacher-guide

Gavin, T. (2021). How to Protect Children from Online Sexual Exploitation (OSEC) - Virlanie Foundation, Inc. Virlanie Foundation, Inc. https://virlanie.org/how-to-protect-children-from-online-sexual-exploitation-osec/

Gravino E., Villanueva MC. (2021). R.A. No. 10175: The Cybercrime Prevention Act: The Net Commandments. Philippine Legal Research. https://legalresearchph.com/2021/12/05/r-a-no-10175-the-cybercrime-prevention-act-the-net-commandments/

Implementing rules and regulations of the Anti-OSAEC law signed. (n.d.). https://www.ijm.org.ph/articles/implementing-rules-and-regulations-of-the-anti-osaec-law-signed

IBM Data and IM Team. (2023). Understanding the different types of artificial intelligence. IBM Blog. https://www.ibm.com/blog/understanding-the-different-types-of-artificial-intelligence/

Iringan, J. L. L., III. (2022). The rise of Internet Gaming Disorder during the pandemic in the Philippines. BPS Clinic. https://www.bofillpsychologicalservices.org/post/the-rise-of-internet-gaming-disorder-during-the-pandemic-in-the-philippines

Journalism, Fake News, and Disinformation (2018). United Nations Educational, Scientific and Cultural Organization. https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf

Kyoto Review (2022) Mobilizing yet polarizing: Social media youth engagement in the 2022 Philippine elections - Kyoto Review of Southeast Asia. Kyoto Review of Southeast Asia.

https://kyotoreview.org/issue-36/social-media-youth-engagement-in-the-2022-philippine-elections/

Law Summary: Republic Act No. 11930. (n.d.). Jur. https://jur.ph/law/summary/anti-online-sexual-abuse-or-exploitation-of-children-osaec-and-anti-child-sexual-abuse-or-exploitation-materials-csaem-act

Learn about OSAEC - SaferKids PH. (2020). SaferKids PH. https://www.saferkidsph.org/learn-about-osaec/

Library Guides: News: Fake News, Misinformation & Disinformation. (n.d.). University of Washington Bothell and Cascadia College. https://guides.lib.uw.edu/bothell/news/misinfo
Lim, L. (2023). What are my digital rights and responsibilities? Rumie-learn. https://learn.rumie.org/jR/bytes/what-are-my-digital-rights-and-responsibilities/

Loução, I. (2023). The Digital Age: Navigating the pros and cons of technology's impact on society. Medium. https://medium.com/@isabelloucao18/the-digital-age-navigating-the-pros-and-cons-of-technologys-impact-on-society-b516abba5226

Lu, J. (2023) 10 ground rules of being a responsible social media user! | LinkedIn. https://www.linkedin.com/pulse/10-ground-rules-being-responsible-social-media-user-jet-l%C3%BC/
Lutkevich, B. (2024). Identity Theft. Security. https://www.techtarget.com/searchsecurity/definition/identity-theft

McGarrigle, J. (2022). Explained: What is Fake news? | Social Media and Filter Bubbles. Webwise.ie. https://www.webwise.ie/teachers/what-is-fake-news/

Microsoft. (2022). What is Netiquette? Microsoft 365. https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-netiquette

National Defense College of the Philippines. (2023, March 28). PHILIPPINE CYBERSECURITY IN RETROSPECT (2016-2021) - NDCP. NDCP. https://ndcp.edu.ph/philippine-cybersecurity-in-retrospect-2016-2021/#:~:text=Similarly%2C%20the%20Philippines%20ranked%204th,increased%20tremendously%20at%20433%20percent.

National Study on online Sexual Abuse and exploitation of Children in the Philippines. (2021, July 1). De La Salle University- Social Development and Research Center, Department of

Social Welfare and Development – Inter-Agency Council Against Child Pornography, and UNICEF Philippines. https://www.unicef.org/philippines/reports/national-study-online-sexual-abuse-and-exploitation-children-philippines

Nine elements of digital citizenship. (n.d.). Digital Citizenship. https://www.digitalcitizenship.net/nine-elements.html

OECD legal instruments. (n.d.). https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389

Online bullying remains prevalent in the Philippines, other countries. (2019). UNICEF. https://www.unicef.org/philippines/press-releases/online-bullying-remains-prevalent-philippines-other-countries

Protecting yourself from identity theft online - Microsoft Support. (n.d.). https://support.microsoft.com/en-us/office/protecting-yourself-from-identity-theft-online-6019708f-e990-4894-9ca7-fdb53ee70830

Republic Act No. 11930. (n.d.). https://lawphil.net/statutes/repacts/ra2022/ra_11930_2022.html

Republic Act No 11930 Implementing Rules and Regulations Ceremonial Signing | Inter-Agency Council Against Trafficking. (n.d.). https://iacat.gov.ph/?p=6341

Respicio, A. H. (2023). Cyber bullying investigation Philippines. RESPICIO & CO. https://www.respicio.ph/features/cyber-bullying-investigation-philippines

Respicio, A. H. (2023). Cybercrime Prevention Act of 2012 (Republic Act No. 10175, signed into law on September 12, 2012, and upheld by the Supreme Court in 2014) (R.A. 10175). RESPICIO & CO.

Responsible AI: Ways to avoid the dark side of AI use. (2022) .AltexSoft. https://www.altexsoft.com/blog/responsible-ai/

Rights and responsibilities - Digital Citizenship Education (DCE) - www.coe.int. (n.d.). Digital Citizenship Education (DCE). https://www.coe.int/en/web/digital-citizenship-education/rights-and-responsibilities

Saymon, M. S. A. (2023). Navigating the digital world: foundations and frontiers. Medium. https://medium.com/@saymonsale/navigating-the-digital-world-foundations-and-frontiers-16e517fedcc4

Scale of Harm: Estimating the Prevalence of Trafficking to Produce Child Sexual Exploitation Material in the Philippines. (2022). International Justice Mission. https://www.ijm.org.ph/articles/findings-of-scale-of-harm-prevalence-study-released

Seasus. (n.d.). Digital Well-Being | HDPD. https://hpdp.gov.mt/hpu/digital_well_being

Social media in the Philippines. (2023). Statista. https://www.statista.com/topics/6759/social-media-usage-in-the-philippines/#topicOverview

Start Smarter. (2022). The advantages and Disadvantages of digitalisation. https://startsmarter.co.uk/the-advantages-and-disadvantages-of-digitalisation/

Statista. (2019). Number of cyberbullying incidents Philippines 2019 by region. https://www.statista.com/statistics/1136192/philippines-number-cyberbullying-incidents-by-region/

Statista. (2021). Children who uses social media weekly Philippines 2021, by age group. https://www.statista.com/statistics/1314741/philippines-weekly-user-of-social-media-among-children-by-age-group/

Sternlicht, A. (n.d.). Video games, Mental health, and Addiction – the good, the bad, and the ugly: Family Addiction Specialist: addiction counselor. https://www.familyaddictionspecialist.com/blog/video-games-mental-health-and-addiction-the-good-the-bad-and-the-ugly

Strategies to help protect your digital footprint | Morgan Stanley. (n.d.). Morgan Stanley.https://www.morganstanley.com/articles/digital-footprint-protection-strategies#:~:text=Cybercriminals%20can%20use%20your%20%22digital,and%20tightening%20your%20privacy%20settings.

Takumi, R. (2016). 80% of young teens in PHL experience cyberbullying –survey. GMA News Online. https://www.gmanetwork.com/news/lifestyle/parenting/560886/80-of-young-teens-in-phl-experience-cyberbullying-survey/story/

Talkwalker. (2019). Social media statistics in the Philippines. Social media statistics in the Philippines. from https://www.talkwalker.com/blog/social-media-statistics-philippines

Teach for Philippines (n.d.) Embedding Teaching with Technology. https://teachforthephilippines.com/wp-content/uploads/2022/10/teacher_workbook-3.2.pdf

The Policy Circle. (2022). Digital landscape - the policy circle. https://www.thepolicycircle.org/brief/digital-landscape/

Top online scams and how to avoid internet scams. (n.d.). Kaspersky https://www.kaspersky.com/resource-center/threats/top-scams-how-to-avoid-becoming-a-victim

Totally Awesome. (2021). Zoomers Digital Insights Philippines 2021. https://totallyawesome.tv/wp-content/uploads/2021/10/Zoomers-Digital-Insights-Philippines-2021-converted.pdf
Types of AI explained. (2024). Cloud Academy. https://cloudacademy.com/blog/types-of-ai/

UNICEF. (2017). The state of the world's children 2017: Children in a digital world. https://www.unicef.org/media/48601/file

Wang, J. L., Sheng, J. R., & Wang, H. Z. (2019). The association between mobile game addiction and depression, social anxiety, and loneliness. Frontiers in Public Health, 7. https://doi.org/10.3389/fpubh.2019.00247

What are the advantages and disadvantages of artificial intelligence (AI)? (n.d.). Tableau. https://www.tableau.com/data-insights/ai/advantages-disadvantages

What are web threats? (n.d.). www.kaspersky.com. https://www.kaspersky.com/resource-center/threats/web

What is a digital footprint? And how to protect it from hackers. (n.d.). www.kaspersky.com. https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint

What is a digital footprint? And how to protect it from hackers. (n.d.). www.kaspersky.com. https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint

What is artificial intelligence? Definition, uses, and types. (2024). Coursera. https://www.coursera.org/articles/what-is-artificial-intelligence

What is digital citizenship? (n.d.). https://blog.avast.com/what-is-digital-citizenship-avast
Youth First (2020). Using social media responsibly. https://youthfirstinc.org/using-social-media-responsibly/