

MEDIA AND INFORMATION LITERACY

First Quarter
Module 2

Responsible Use of Media and
Information





Republic of the Philippines
Department of Education
REGION VII, CENTRAL VISAYAS
SCHOOLS DIVISION OF SIKUIJOR

COPYRIGHT NOTICE

Section 9 of Presidential Decree No. 49 provides:

“No copyright shall subsist in any work of the Government of the Republic of the Philippines. However, prior approval of the government agency of office wherein the work is created shall be necessary for exploitation of such work for profit.”

This material has been developed through the initiative of the Curriculum Implementation Division (CID) of the Department of Education – Siquijor Division.

It can be reproduced for educational purposes and the source must be clearly acknowledged. The material may be modified for the purpose of translation into another language but the original work must be acknowledged. Derivatives of the work including the creation of an edited version, supplementary work or an enhancement of it are permitted provided that the original work is acknowledged and the copyright is attributed. No work may be derived from this material for commercial purposes and profit.

Borrowed materials (i.e. songs, stories, poems, pictures, photos, brand names, trademarks, etc.) included in this module are owned by their respective copyright holders. Every effort has been exerted to locate and seek permission to use these materials from their respective copyright owners. The publisher and authors do not represent nor claim ownership over them.
Published by the Department of Education

OIC-Schools Division Superintendent: *Dr. Neri C. Ojastro*
Assistant Schools Division Superintendent: *Dr. Edmark Ian L. Cabio*

Development Team of the Learning Module

Writer: Karen A. Jumalon

Evaluators: Anna-Liza S. Jimenez Susan A. Calibo Ivy Mae L. Dimagnaong Noel P. Paluray

Julieta A. Sarvida Roger B. Antipuesto Kenneth P. Llorente

Management Team: Dr. Marlou S. Maglinao
CID – Chief

Raul R. Abapo
Education Program Supervisor (EPS – TLE/TVL)

Edesa T. Calvadores
Education Program Supervisor (LRMS)

Printed in the Philippines by _____
Department of Education – Region VII, Central Visayas, Division of Siquijor
Office Address: Larena, Siquijor
Telephone No.: (035) 377-2034-2038
E-mail Address: deped.siquijor@deped.gov.ph

MEDIA AND INFORMATION LITERACY

First Quarter
Module 2

Responsible Use of Media and
Information

INTRODUCTION

This module is written in support of the K to 12 Basic Education Program to ensure attainment of standards expected of you as a learner.

This aims to equip you with essential knowledge on the Responsible Use of Media and Information

This includes the following activities/tasks:

- Expected Learning Outcome — This lays out the learning outcome that you are expected to accomplish at the end of the module.
- Pre-test — This determines your prior learning of the particular lesson you are about to take.
- Discussion of the Lesson — This provides you with the important knowledge, principles and attitude that will help you meet the expected learning outcome.
- Learning Activities — These provide you with the application of the knowledge and principles you have gained from the lesson and enable you to further enhance your skills as you carry out prescribed tasks.
- Post-test — This evaluates your overall understanding about the module.

With the different activities provided in this module, may you find this material engaging and challenging as it develops your critical thinking skills.



What I Need to Know

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

- ❖ discuss responsible use of media and information
(MIL11/12IMIL-IIIa-3)



What I Know

Pretest

Directions: Read and analyze the statements. Write the letter of your answer on your answer sheet.

1. What is the equitable distribution of technology and online resources?
 - a. Digital access
 - b. Digital security
 - c. Digital commerce
 - d. Digital communication and collaboration
2. What is the electronic buying and selling of goods and focuses on the tools and safeguards in place to assist those buying, selling, banking, or using money in any way in the digital space. Career and technical education use the tools of technology to show students the path for their future?
 - a. Digital access
 - b. Digital commerce
 - c. Digital security and privacy
 - d. Digital communication and collaboration

3. How do electronic precautions guarantee a smooth and safe navigation on the web?
 - a. Digital access
 - b. Digital commerce
 - c. Digital security and privacy
 - d. Digital communication and collaboration
4. When can you say that it is an electronic exchange of information?
 - a. Digital access
 - b. Digital commerce
 - c. Digital security and privacy
 - d. Digital communication and collaboration
5. What is an electronic standard of conduct or procedures and has to do with the process of thinking about others when using digital devices?
 - a. Digital law
 - b. Digital fluency
 - c. Digital etiquette
 - d. Digital health and welfare
6. What is an electronic responsibility for actions and deeds and has to do with the creation of rules and policy that address issues related to the online world?
 - a. Digital law
 - b. Digital fluency
 - c. Digital etiquette
 - d. Digital health and welfare
7. What is the process of understanding technology and its use?
 - a. Digital law
 - b. Digital fluency
 - c. Digital etiquette
 - d. Digital health and welfare
8. What is a physical and psychological well-being in a digital world?
 - a. Digital law
 - b. Digital etiquette
 - c. Digital health and welfare
 - d. Digital rights and responsibility
9. What are the requirements and freedoms extended to everyone in a digital world?
 - a. Digital law
 - b. Digital etiquette
 - c. Digital health and welfare
 - d. Digital rights and responsibility

10. What is an electronic, magnetic, optical, electrochemical, or other data processing or communications device, or grouping of such devices, capable of performing logical, arithmetic, routing, or storage functions and which includes any storage facility or equipment or communications facility or equipment directly related to or operating in conjunction with such device?
- Access
 - Alteration
 - Communication
 - Computer
11. When can you say that the instruction, communication with, storing data in, retrieving data from, or otherwise making use of any resources of a computer system or communication network?
- Access
 - Alteration
 - Communication
 - Computer
12. What do you call a transmission of information through ICT media, including voice, video and other forms of data?
- Access
 - Alteration
 - Communication
 - Computer
13. What is referred to as the process of making modification or change, in form or substance, of an existing computer data or program?
- Access
 - Alteration
 - Communication
 - Computer
14. What are the computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data so vital to this country that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters?
- Computer data
 - Computer system
 - Computer program
 - Computer infrastructure

15. What do you call a representation of facts, information, or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function and includes electronic documents and/or electronic data messages, whether stored in local computer systems or online?
- a. Computer data
 - b. Computer system
 - c. Computer program
 - d. Computer infrastructure
16. What is referred to as a set of instructions executed by the computer to achieve intended results?
- a. Computer data
 - b. Computer system
 - c. Computer program
 - d. Computer infrastructure



What's In

Media literacy, put simply, is the ability to identify different types of media and the messages they are sending. When we speak of media, it encompasses print media, such as newspapers, magazines and posters, and theatrical presentations, tweets, radio broadcasts, etc. Being able to understand these various forms of information with an ability to make sense of what is presented is key.



What' New



1. From what online game is this picture taken?

2. Has this game affected the lives of young people like you? In what way?

https://is4-ssl.mzstatic.com/image/thumb/Purple123/v4/b0/b4/3e/b0b43e4f-4a85-b105-fe37-4ea631a70c45/pr_source.jpg/643x0w.jpg



What Is It

RESPONSIBLE USE OF MEDIA AND INFORMATION

If you are a media and information literate person, you will possess some power over powerful media and information messages. You will have the ability to examine the content of media and information messages closely and see how their meanings are significant or otherwise with your life as a person and in your community as well.

You will also value the word ethics and its implications for the society. More often than not, we get lost in the flurry and frenzy of the media intrusion in our lives (Zarate, 2016)

Digital Citizenship

Digital citizenship can be defined as engaging in appropriate and responsible behavior when using technology. It encompasses digital literacy, ethics, etiquette, online safety, norms, rights, culture and more. A digital citizen is one who knows what is right and wrong, exhibits intelligent technology behaviors, and makes good choices when using technology. (<https://www.virtuallibrary.info/digital-citizenship.html>)

Responsible digital citizenship can be defined as the set of appropriate social norms and behavior with regard to the use of the internet. Evaluating the extent of responsible behavior on the internet involves looking into several domains of information technology behavior (Zarate, 2016).

Today, billions of people all over the planet interact using various technologies. This interaction creates a digital society that affords its citizens opportunities for education, employment, entertainment, and social interaction. As in any society, it is expected that digital citizens act in a certain way, according to accepted norms, rules, and laws. Most of today's students are entirely comfortable with technology, but are they using it appropriately? Do they understand their roles and responsibilities in digital society? (<https://www.virtuallibrary.info/digital-citizenship.html>)

Take a look at this picture describing a responsible digital citizen:



<https://www.virtuallibrary.info/uploads/2/6/9/3/26930678/published/6218195.png?1523065754>

Looking at the picture, can you consider yourself a responsible digital citizen?

Digital citizenship is the continuously developing norms of appropriate, responsible, and empowered technology use.

1. To lead and assist others in building positive digital experiences
2. To recognize that our actions have consequences to others
3. To participate in a manner for the common good

(<https://www.digitalcitizenship.net/nine-elements.html>)

Nine Themes of Digital Citizenship

1. **Digital Access** is about the equitable distribution of technology and online resources. Teachers and administrators need to be aware of their community

and who may or may not have access, not only in school but at home as well. Educators need to provide options for lessons and data collection, such as free access in the community or provide resources for the home.

2. **Digital Commerce** is the electronic buying and selling of goods and focuses on the tools and safeguards in place to assist those buying, selling, banking, or using money in any way in the digital space. Career and technical education use the tools of technology to show students the path for their future.
3. **Digital Communication and Collaboration** are the electronic exchange of information. All users need to define how they will share their thoughts so that others understand the message. For students struggling to understand their place in the world, technology can help them find their own voices and express themselves.
4. **Digital Etiquette** refers to electronic standards of conduct or procedures and has to do with the process of thinking about others when using digital devices. Teachers can include Digital Etiquette as part of the classroom rules or academic goals. Whether in the classroom or online, being aware of others is an important idea for everyone.
5. **Digital Fluency** is the process of understanding technology and its use. The better educated or “digitally fluent,” students are, the more likely they are to make good decisions online, like supporting others instead of making negative comments. Digital literacy includes the discussion of media literacy and the ability to discern good information from poor, such as “fake news” from real news.
6. **Digital Health and Welfare** refer to the physical and psychological well-being in a digital world. Technology provides many opportunities and enjoyment, but knowing how to segment use with the needs of ourselves and others is key to a healthy, balanced life. Educators, especially in 1:1 schools or classrooms need to ask the question of how much screen time is appropriate for students. Common Sense media have developed a guide on this topic.
7. **Digital Law** refers to the electronic responsibility for actions and deeds and has to do with the creation of rules and policy that address issues related to the online world. Just as in the real world, the online world has had to create structure to protect those using these digital devices from harm. Support for issues such as cyberbullying and sexting are available from School Resource Officers and other school council. Administrators need to come up with positive approaches to these issues in their schools and districts.

8. **Digital Rights and Responsibility** are those requirements and freedoms extended to everyone in a digital world. This area of Digital Citizenship is about helping students understand that when they are provided opportunities, such as the access to the Internet and use of online products, they need to be diligent in helping others as well, such as informing adults of potential problems. Educators must help students understand that protecting others, both online and in the real world are essential skills to have.
9. **Digital Security and Privacy** is the electronic precautions to guarantee safety. Viruses, worms and other bots can be passed along from one system to another just like an illness. When using devices in school or at home, understanding and being aware of attacks and how to prevent them are important skills for today and into the future. (<https://www.digitalcitizenship.net/nine-elements.html>)

The S3 Framework of Digital Citizenship (Safe, Savvy and Social)

Digital Citizenship classifies nine foundational elements in the following three guiding principles: Safe, Savvy and Social (or S3). The tenets of S3 are a way to support, as well as reinforce the framework of the themes of digital citizenship. Each theme/element encompasses three levels of support (Safe, Savvy and Social) which could (or should) be taught as soon as our children can first pick up a device and start to interact with it.

1. **Safety - Protecting Digital Citizens**
 - being protected from or unlikely to cause danger, risk, or injury to yourself or others
2. **Savvy - Creating Educated Digital Citizens**
 - wisdom and practical knowledge; the understanding to make good judgments
3. **Social - Respecting Yourself as a Digital Citizen**
 - creating cooperative and interdependent relationships and understanding of others

(<https://www.digitalcitizenship.net/nine-elements.html>)

Salient Features of Republic Act 10175 or the Cybercrime Prevention Act of 2012

AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES

CHAPTER I PRELIMINARY PROVISIONS

SECTION 1. Title. — This Act shall be known as the “Cybercrime Prevention Act of 2012”.

SEC. 2. Declaration of Policy. — The State recognizes the vital role of information and communications industries such as content production, telecommunications, broadcasting electronic commerce, and data processing, in the nation’s overall social and economic development. The State also recognizes the importance of providing an environment conducive to the development, acceleration, and rational application and exploitation of information and communications technology (ICT) to attain free, easy, and intelligible access to exchange and/or delivery of information; and the need to protect and safeguard the integrity of computer, computer and communications systems, networks, and databases, and the confidentiality, integrity, and availability of information and data stored therein, from all forms of misuse, abuse, and illegal access by making punishable under the law such conduct or conducts. In this light, the State shall adopt sufficient powers to effectively prevent and combat such offenses by facilitating their detection, investigation, and prosecution at both the domestic and international levels, and by providing arrangements for fast and reliable international cooperation.

SEC. 3. Definition of Terms. — For purposes of this Act, the following terms are hereby defined as follows:

- a) **Access** refers to the instruction, communication to, storing data in, retrieving data from, or otherwise making use of any resources of a computer system or communication network.
- b) **Alteration** refers to the modification or change, in form or substance, of an existing computer data or program.
- c) **Communication** refers to the transmission of information through ICT, media, including voice, video and other forms of data.

- d) **Computer** refers to an electronic, magnetic, optical, electrochemical, or other data processing or communications device, or grouping of such devices, capable of performing logical, arithmetic, routing, or storage functions and which includes any storage facility or equipment or communications facility or equipment directly related to or operating in conjunction with such device. It covers any type of computer device including devices with data processing capabilities like mobile phones, smart phones, computer networks and other devices connected to the internet.
- e) **Computer data** refers to any representation of facts, information, or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function and includes electronic documents and/or electronic data messages, whether stored in local computer systems or online.
- f) **Computer program** refers to a set of instructions executed by the computer to achieve intended results.
- g) **Computer system** refers to any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automated processing of data. It covers any type of device with data processing capabilities including, but not limited to, computers and mobile phones. The device consisting of hardware and software may include input, output and storage components which may stand alone or be connected in a network or other similar devices. It also includes computer data storage devices or media.
- h) Without right refers to either: (i) conduct undertaken without or in excess of authority; or (ii) conduct not covered by establishing legal defenses, excuses, court orders, justifications, or relevant principles under the law.
- i) **Cyber** refers to a computer or a computer network, the electronic medium in which online communication takes place.
- j) **Critical infrastructure** refers to the computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data so vital to this country that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters.

- k) **Cybersecurity** refers to the collection of tools, policies, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.
- l) **Database** refers to a representation of information, knowledge, facts, concepts, or instructions which are being prepared, processed or stored or have been prepared, processed or stored in a formalized manner and which are intended for use in a computer system.
- m) **Interception** refers to listening to, recording, monitoring or surveillance of the content of communications, including procuring of the content of data, either directly, through access and use of a computer system or indirectly, through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring.
- n) **Service provider** refers to:
1. Any public or private entity that provides to users of its service the ability to communicate by means of a computer system; and
 2. Any other entity that processes or stores, computer data on behalf of such communication service or users of such service.
- o) **Subscriber's information** refers to any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which identity can be established:
1. The type of communication service used, the technical provisions taken thereto, and the period of service;
 2. The subscriber's identity, postal or geographic address, telephone and other access numbers, any assigned network address, billing and payment information, available on the basis of the service agreement or arrangement; and
 3. Any other available information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.
- p) **Traffic data or non-content data** refers to any computer data other than the content of the communication, including, but not limited to, the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

CHAPTER II PUNISHABLE ACTS

SEC. 4. Cybercrime Offenses. — The following acts constitute the offense of cybercrime punishable under this Act:

(a) Offenses against the confidentiality, integrity and availability of computer data and systems:

(1) **Illegal Access.** — The access to the whole or any part of a computer system without right.

(2) **Illegal Interception.** — The interception made by technical means without right of any non-public transmission of computer data to, from, or within a computer system including electromagnetic emissions from a computer system carrying such computer data.

(3) **Data Interference.** — The intentional or reckless alteration, damaging, deletion or deterioration of computer data, electronic document, or electronic data message, without right, including the introduction or transmission of viruses.

(4) **System Interference.** — The intentional alteration or reckless hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, electronic document, or electronic data message, without right or authority, including the introduction or transmission of viruses.

(5) **Misuse of Devices.**

(i) The use, production, sale, procurement, importation, distribution, or otherwise making available, without right, of:

(aa) A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offenses under this Act; or

(bb) A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offenses under this Act.

(ii) The possession of an item referred to in paragraphs 5(i)(aa) or (bb) above with intent to use said devices for the purpose of committing any of the offenses under this section.

(6) **Cyber-squatting.** – The acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same, if such a domain name is:

- (i) Similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration:
- (ii) Identical or in any way similar with the name of a person other than the registrant, in case of a personal name; and
- (iii) Acquired without right or with intellectual property interests in it.

(b) Computer-related Offenses:

(1) **Computer-related Forgery.** —

- (i) The input, alteration, or deletion of any computer, data without right resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible; or
- (ii) The act of knowingly using computer data which are the product of computer-related forgery as defined herein, for the purpose of perpetuating a fraudulent or dishonest design.

(2) **Computer-related Fraud.** — The unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a computer system, causing damage thereby with fraudulent intent: Provided, That if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.

(3) **Computer-related Identity Theft.** – The intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical, without right: Provided, That if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.

(c) **Content-related Offenses:**

(1) **Cybersex.** — The willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration.

(2) **Child Pornography.** — The unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the Anti-Child Pornography Act of 2009, committed

through a computer system: Provided, That the penalty to be imposed shall be (1) one degree higher than that provided for in Republic Act No. 9775.

(3) *Unsolicited Commercial Communications*. — The transmission of commercial electronic communication with the use of computer systems which seek to advertise, sell, or offer for sale products and services is prohibited unless:

(i) There is prior affirmative consent from the recipient; or

(ii) The primary intent of the communication is for service and/or administrative announcements from the sender to its existing users, subscribers or customers; or

(iii) The following conditions are present:

(aa) The commercial electronic communication contains a simple, valid, and reliable way for the recipient to reject. Receipt of further commercial electronic messages (opt-out) from the same source;

(bb) The commercial electronic communication does not purposely disguise the source of the electronic message; and

(cc) The commercial electronic communication does not purposely include misleading information in any part of the message in order to induce the recipients to read the message.

(4) *Libel*. — The unlawful or prohibited acts of libel as defined in Article 355 of the Revised Penal Code, as amended, committed through a computer system or any other similar means which may be devised in the future.

SEC. 5. Other Offenses. — The following acts shall also constitute an offense:

(a) **Aiding or Abetting in the Commission of Cyber Crime**. — Any person who willfully abets or aids in the commission of any of the offenses enumerated in this Act shall be held liable.

(b) **Attempt in the Commission of Cyber Crime**. — Any person who willfully attempts to commit any of the offenses enumerated in this Act shall be held liable.



What's More

Independent Activity 1

Read and Study the topic on responsible use of media and information to answer the assessment below.

Independent Assessment 1

Learning with Errors

Directions: All statements are erroneous. Identify the word/ phrase that made the statement wrong.

1. If you are a media and information literate person, you have no power over powerful media and information messages.
2. Digital citizenship can be defined as engaging in inappropriate and responsible behavior when using technology.
3. A digital citizen is one who knows what is right and wrong, exhibits intelligent technology behavior, and makes poor choices when using technology.
4. Digital citizenship is the stagnant norms of appropriate, responsible, and empowered technology use.
5. Republic Act No. 10533 is also known as the “Cybercrime Prevention Act of 2012”.
6. Communication refers to the modification or change of information through ICT media, including voice, video and other forms of data.
7. Computer program refers to a set of instructions executed by the person to achieve intended results.
8. Cyber refers to a multimedia network, the electronic medium in which online communication takes place.
9. Cybersecurity refers to the collection of tools, policies, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the natural environment and the organization and user’s assets.
10. Adaptation refers to listening to, recording, monitoring or surveillance of the content of communications, including procuring of the content of data, either directly, through access and use of a computer system or indirectly, through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring.
11. Cybersex is the willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a sound system, for favor or consideration.

12. Data Interference is the unintentional or reckless alteration, damaging, deletion or deterioration of computer data, electronic document, or electronic data message, without right, including the introduction or transmission of viruses.



What I Have Learned

I learned that:

- ☐ There are many ways to become a responsible user of media and information.



What I Can Do

Directions: Answer each question/situation correctly and briefly. Do it in your notebook.

1. Discuss the responsible use of media and information.



Assessment

Post Test:

Directions: Read and analyze the statements. Write the letter of your answer on your answer sheet.

1. What is the equitable distribution of technology and online resources?
 - e. Digital access
 - f. Digital security
 - g. Digital commerce
 - h. Digital communication and collaboration

2. What is the electronic buying and selling of goods and focuses on the tools and safeguards in place to assist those buying, selling, banking, or using money in any way in the digital space. Career and technical education use the tools of technology to show students the path for their future?
 - a. Digital access
 - b. Digital commerce
 - c. Digital security and privacy
 - d. Digital communication and collaboration

3. How do electronic precautions guarantee a smooth and safe navigation on the web?
 - a. Digital access
 - b. Digital commerce
 - c. Digital security and privacy
 - d. Digital communication and collaboration

4. When can you say that it is an electronic exchange of information?
 - a. Digital access
 - b. Digital commerce
 - c. Digital security and privacy
 - d. Digital communication and collaboration

5. What is an electronic standard of conduct or procedures and has to do with the process of thinking about others when using digital devices?
 - a. Digital law
 - b. Digital fluency
 - c. Digital etiquette
 - d. Digital health and welfare

6. What is an electronic responsibility for actions and deeds and has to do with the creation of rules and policy that address issues related to the online world?
 - a. Digital law
 - b. Digital fluency
 - c. Digital etiquette
 - d. Digital health and welfare
7. What is the process of understanding technology and its use?
 - a. Digital law
 - b. Digital fluency
 - c. Digital etiquette
 - d. Digital health and welfare
8. What is a physical and psychological well-being in a digital world?
 - a. Digital law
 - b. Digital etiquette
 - c. Digital health and welfare
 - d. Digital rights and responsibility
9. What are the requirements and freedoms extended to everyone in a digital world?
 - a. Digital law
 - b. Digital etiquette
 - c. Digital health and welfare
 - d. Digital rights and responsibility
10. What is an electronic, magnetic, optical, electrochemical, or other data processing or communications device, or grouping of such devices, capable of performing logical, arithmetic, routing, or storage functions and which includes any storage facility or equipment or communications facility or equipment directly related to or operating in conjunction with such device?
 - a. Access
 - b. Alteration
 - c. Communication
 - d. Computer
11. When can you say that the instruction, communication with, storing data in, retrieving data from, or otherwise making use of any resources of a computer system or communication network?
 - a. Access
 - b. Alteration
 - c. Communication
 - d. Computer

12. What do you call a transmission of information through ICT media, including voice, video and other forms of data?
- Access
 - Alteration
 - Communication
 - Computer
13. What is referred to as the process of making modification or change, in form or substance, of an existing computer data or program?
- Access
 - Alteration
 - Communication
 - Computer
14. What are the computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data so vital to this country that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters?
- Computer data
 - Computer system
 - Computer program
 - Computer infrastructure
15. What do you call a representation of facts, information, or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function and includes electronic documents and/or electronic data messages, whether stored in local computer systems or online?
- Computer data
 - Computer system
 - Computer program
 - Computer infrastructure
16. What is referred to as a set of instructions executed by the computer to achieve intended results?
- Computer data
 - Computer system
 - Computer program
 - Computer infrastructure



References

Main Reference:

1. Zarate, Maria Jovita E., Media Information Literacy. Rex Printing Company, Inc., Quezon City, 2016

Online Sources:

1. Retrieved from: <https://yanahomeblog.files.wordpress.com/2018/08/blogg.jpeg> on July 30, 2020
2. Retrieved from: https://is4-ssl.mzstatic.com/image/thumb/Purple123/v4/b0/b4/3e/b0b43e4f-4a85-b105-fe37-4ea631a70c45/pr_source.jpg/643x0w.jpg on July 27, 2020
3. Retrieved from: Retrieved from: <https://www.virtuallibrary.info/digital-citizenship.html> on July 26, 2020
4. Retrieved from: <https://www.virtuallibrary.info/digital-citizenship.html> on July 28, 2020
5. Retrieved from: <https://www.digitalcitizenship.net/nine-elements.html> on July 28, 2020
6. Retrieved from: <https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/> on July 30, 2020