

7

Digital Citizenship

Knowledge:

Students will be able to:

- Discuss the ethics and ethical issues in digital environments.
- Explain the importance of being safe, responsible, and respectful online.
- Define the key concepts of copyright, plagiarism, and piracy.
- Identify Improper use of computer resources.
- Steps to secure information privacy and confidentiality.
- The possible dangers of the internet and related security measures.

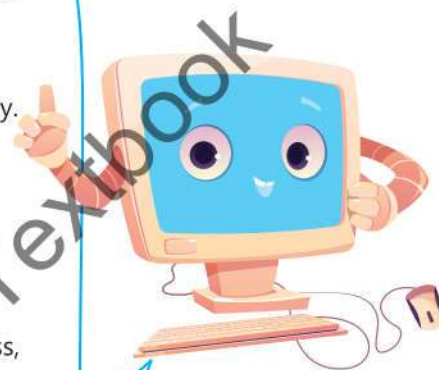
Students will know...

- Identify the purpose of major internet uses such as business, social networking, entertainment, information/news.
- Evaluate digital media bias and messaging.

Skills:

Students will be able to:

- Identify appropriate and inappropriate behaviour when navigating the digital environment.
- Identify threats and actively protect devices and networks from viruses, intrusion, vandalism, and other malicious activities.
- Describe and use safe, appropriate, and responsible practices (netiquette) when participating in online communities.
- Identify positive and negative impacts of using social media, both online and offline.



Introduction:

Societies are evolving with the passage of time. We use technology for communication instead of writing letters, sending faxes, or meeting with people. The Internet and smart devices have become an essential part of our daily routine.

The use of social media and the Internet is prevailing day by day. This massive increase in the use of digital means of communication resulted in increasing data security issues also. Let us also have a look at the safety aspects we need to consider to create a healthy cyber environment.

INTERNET

The Internet is also called 'the NET' or 'Network of Networks', which means International Network. It is a network used all over the world where users located at different locations can communicate and exchange information with each other. It is a collection of networks that are

connected and form a global network.

The Internet provides you the services of online shopping, electronic banking, advertisement, data sharing, communication, education, entertainment, etc. The Internet has transformed our lives and made us more digitised.



Advantages of Internet

The usage of Internet has increased over the years as it has many advantages. Let us discuss some of its advantages:

- **Treasure of Information**

Internet is a hub of information. We can search and access any type of information on any topic through the Internet. It is used extensively by people to do their projects and research.

- **Web Services**

Internet provides many useful services like chatting, email, video conferencing, etc. which help people to connect all around the world. Using these services, organisations can exchange information and conduct meetings with their employees which are located at different places.

- **Promoting Business**

Internet also helps companies to promote their products online through websites and social networking sites. It allows users to sell their products online. It also allows being in contact with the customer 24/7.

- **E-Learning**

Internet has changed learning from physical classroom to virtual classrooms. These days students can study by sitting at home in their comfortable timings. Internet is also used by teachers as well as students to collect information on various topics.

- **Entertainment**

Internet is used by people for entertainment. People can listen to music, watch movies, and play games on the internet. The Internet allows people to read newspapers and magazines online. There are various services on the Internet like Newsgroups and Blogs where people can contribute as per their interests.

- **Internet Banking**

Conventional banking systems are getting obsolete now. Customers use their credit and debit cards for payments. Cash is withdrawn from ATMs (Automated Teller Machines) which are available 24/7 all day and night. Mobile banking has taken the banking system to a high level. From your mobile phones, you can pay your bill,



Do You Know?

Blogs are virtual diaries created by people to share their hobbies, thoughts with like-minded people.

transfer money, pay for shopping, top up your mobile phone sim cards, and many more.

Disadvantages of Internet

The Internet has many advantages for users. But, as we know, excess of everything is bad. So, the internet has some disadvantages too.

• Violent Information

Several websites on the internet have violent videos and images. This type of content can disturb the mental health of children as well as adults.

• Wastage of Time

It is a waste of time as with the excessive use of internet, people get addicted to it and spend a lot of time surfing without any useful outcome.



Do You Know?

A librarian by the name of Jean Armour Polly came up with the term "internet surfing" in 1992.



• Virus and Spam Attacks

Internet has also increased the cases of virus attacks. Users can lose their data and programs in these virus attacks.

• Loss of Personal Information

We share our personal information over the internet that can be misused by cyber criminals to harm us.



Social Media

The website or program known as Social Media is where users can share their content. Additionally, it facilitates online conversations with other users. Millions of people all over the world are actively using it because of its enormous popularity and usefulness.



Advantages of Social Media

Social media has a lot of benefits.

- You can use it for educational purposes.
- You can use it for entertainment.
- It is easier to communicate and share information.
- You can create your brand and content to share original material to.
- It is easier to get updated information and news.

Disadvantages of Social Media

Social media also has several drawbacks, but fewer than its advantages. Some of its disadvantages include:

- It may also be the cause of a great deal of inefficiency.
- Lack of privacy can lead to identity theft, stalking, and other problems.
- As it is easy to get distracted from your work and loose focus when using social media, it may also be the cause of a great deal of inefficiency.
- It can be quite damaging to not know how to respond to negative feedback and to become easily distracted.
- Your shared data may be used against you after tempering it.

Digital Media Bias and Messaging

The idea that the media is reporting the news in a biased or partial way is known as media bias. When digital media looks to favour one point of view over another while covering the news, this is known as Digital Media Bias.



We could use the example of the difference between two news broadcasters that have very different audiences. They tend to be biased in what they report and how they report it due to ideological and political views.

Digital media is heavily used for messaging purposes as well. Many big platforms are used for messaging purposes as well. Some of them are:

- Twitter
- Instagram
- WhatsApp
- Facebook

Ethics and Ethical Use of Digital Environment

Ethics

At its simplest, ethics is a system of moral principles. They affect how people make decisions and lead their lives. Ethics is concerned with what is good for individuals and society and is also described as moral philosophy.



Digital Environment

The digital environment is an increasingly popular tool in family and child research that is argued to pose new ethical challenges. There are many issues in digital environments, such as:

- Participant Privacy



- Confidentiality
- Anonymity.

These concerns apply to internet research across all disciplines, not just those involving families and children.

Ethical Use of Digital Environment

If not handled ethically, using a digital environment can be dangerous. The following is a list of some ethical principles you should follow when using the digital environment:

- Be respectful
- Protect your reputation
- Protect your privacy
- Trustworthiness and honesty
- Doing good and preventing harm
- Avoidance of conflicts
- Fairness
- Accountability

Identify Improper Use of Computer Resources

Everything has its boundaries. When that limit is violated, both you and others are at risk. The following are some examples of inappropriate computer resource use:

- Actions that endanger people's life or harm their property.
- Actions that break the law.
- Uses that breach information confidentiality
- Actions that encourage others to break the law.



An employee using the company's computer for personal use could serve as an example. The company prohibits its employees from using the company's computer for personal benefit. A cyberbully is another example of the person who uses of computer resources improperly. He unlawfully stalks someone online and spreads hate against them using a computer.

Importance of Being Safe Responsible and Respectful Online

Users should place a high priority on online safety. The threats which can be faced online include your personal information to be in danger. It could be used against you if you are not careful. You as well as others can suffer harm from it. You can prevent a lot of potential harm from happening if you exercise caution.



Even though we communicate with each other online, we still need to show respect for others. We should be aware of the thoughts and feelings of others. It teaches us to show respect, and in doing so, will also be respected.

Cyber Crime with Preventive Measures

Cyber crimes are offences that are committed using computers and smart devices connected to the Internet. The victims of cybercrimes can be organisations or individuals. Most cybercriminals use e-mails, social media websites, or pirated software as a medium to trouble their victims.

It is important to remember that data once shared over the Internet is rarely deleted completely. Cybercriminals use this data unethically to trouble their victims.

Let us discuss some of the most used ways to commit cybercrimes.

E-mail Spoofing

When someone sends e-mails that appear genuine from a trusted e-mail ID but, in reality, they are not to be trusted. We call it E-mail Spoofing.

For example, a user may receive an email from a portal or social media platform where the spelling of the service provider or email ID has been slightly changed.

For example, `mailto:customer@tridentportal.com`.

Notice that the spelling of 'portal' is incorrect. These emails contain links that will direct the user to another web page where the user would be asked to enter information which means the user ends up providing personal credentials to cybercriminals. This is also called Phishing.



Do You Know?

The best defence against phishing assaults is human intellect and comprehension.

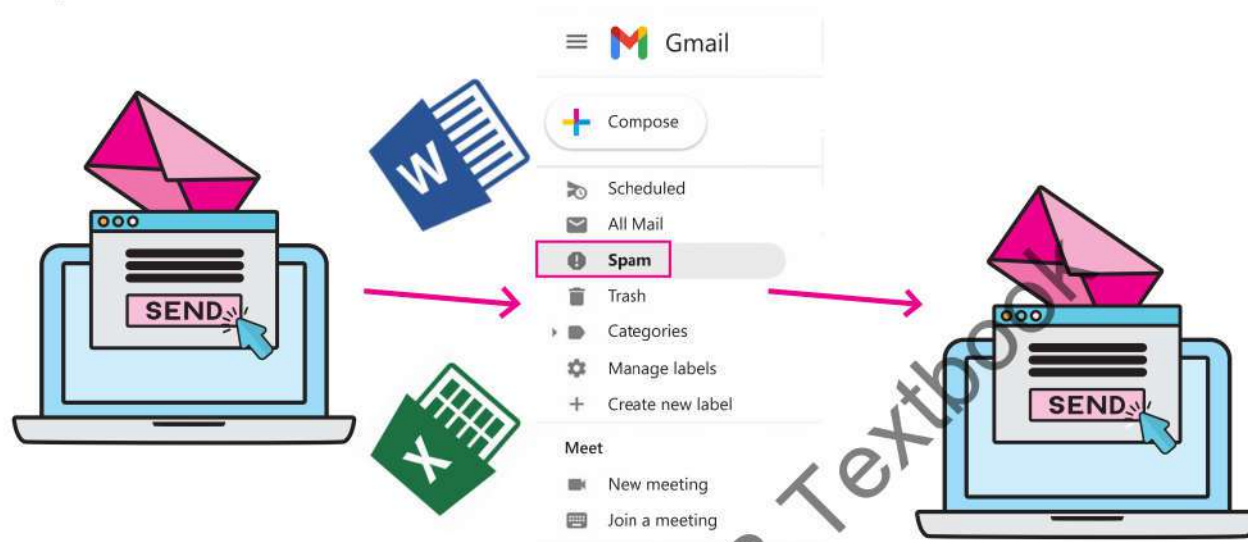


Spamming

It refers to the sending of bulk mail by an identified or unidentified source. Sometimes, certain businesses send bulk-advertising mail to many accounts at the same time. Some people intentionally send bulk mail to a user until the mail server runs out of disk space.

Some people send virus-infected applications and files through the internet via emails,

chats, games, etc. to get access to your smartphone and personal data. These emails may contain a document (Word or Excel file) with malware (a dangerous program that can impact your computer) attached to it. Opening such documents result in malware installed on your computer or mobile.



Using reputable websites to download files and not opening doubtful e-mails are some ways to counter these threats.

Some cybercrimes send emails informing the victim that they have won a lottery or a surprise gift. The cyber criminal then asks for personal details and bank details for transferring the winning amount. Cyber criminals may also ask the victim to deposit a small processing fee to lure the victim to transfer the winning amount.

From: Ansariakram641@gmail.com | Add to Address | [This is spam](#)
To: "Ansariakram641@gmail.com" <Ansariakram641@gmail.com>
Subject: When you report a conversation as spam, you also block the sender.
Date: Mon, 29 Apr 2018, 17:28: 01 IST
[X Go To Attachment\(s\) Download attachment](#)
Note: To help protect your privacy, images from this message have been blocked. [View images | What's this?](#)

Dear Winners,

Please, find the attachment form and fill out the required information and immediately send it back by email attachment to zxwerwaa, for your winning details.

These emails are not to be trusted and one must not reply with any personal information. Further, these must be immediately deleted from the email account to avoid accidental access in the future.

Measures to Avoid Spam

To avoid spam, we can take the following measures:

- Preview your message before opening them.

- Do not click any link in a spam email otherwise, you will invite many such emails in your inbox.
- Do not reply to a Spam email.
- Do not forward an email received from someone you do not know to a list of people.



E-mail account Hacking

It is another common method used by cybercriminals to trouble victims. Using malware or other tricks to obtain your email ID and password, cybercriminals can gain access to your critical information like social media accounts, bank accounts, etc. Cybercriminals may also send offensive emails to a victim's contacts via hacking.



Do You Know?

Cracking refers to the act of breaking into systems to steal or destroy data. Crackers may disturb applications by using malware or changing the program of the applications.

Measures to avoid Hacking

To prevent unauthorised access to your computer and internet we can take the following measures:

- Keep a password for your Wi-Fi connection and computer.
- Keep changing your passwords.
- Keep updating your operating system.
- Do not plug into devices you are not sure about.
- Always look at the green lock sign at the address bar of the window before accessing any website that states that the site you are visiting is secure.
- Always download trusted applications from the internet and check permission and authentication.



Cyber Troll

In internet slang, a troll is a person who starts quarrels or upsets people on the internet to distract and create discord by posting mean and unwarranted messages in an online community.



A cyber troll refers to a person who purposely posts opposing, sarcastic, demeaning, or insulting comments about something or someone.

Social Engineering

Social engineering is a technique used by cybercriminals to gain the information from individuals. Cybercriminals try to interact with the victims to understand their likes and dislikes to seek personal information and/or commit some harm to them.

Cyber Bullying

Cyber Bullying refers to the use of the Internet, e-mail, instant messaging, chat rooms, or social networks, such as Facebook, Twitter, etc. to harass, demean, embarrass or intimidate someone else.



Measures to prevent Cyber Bullying

- Remember never to share personal details such as age, address, date of birth, etc. with unknown people on social media.
- Restrict access to your data on social media platforms. For example, only your friends must be able to see any pictures on Facebook.
- Try avoiding friend requests from unknown people on social media.
- In case, any post hurts or upsets you, talk about it to your trusted set of people like family or friends instead of posting aggressive replies.
- If your parents/elders feel the need, they can also contact the local police station to complain about the cyberbully.
- Never install unwanted software and applications like online games, etc.



Do You Know?

Verbal harassment is the most frequent kind of bullying, followed by social harassment, physical bullying, and cyberbullying.

Online Transaction Fraud

Although at this age, as students, most of you may not be using banking services such as debit cards, credit cards, net banking, etc. yet it is important to be aware of this type of cybercrime.

Online transaction fraud refers to the illegal withdrawal or transfer of money from one bank account to another by a cybercriminal. Online transaction frauds generally take place when a cybercriminal steals a user's login credentials, bank account details, credit card details, etc.

Cybercriminals use many ways to cheat people online:

Cybercriminals may send emails from a fake account that can appear to be from a bank or credit card service provider.

Cybercriminals may also fake their identity and call people pretending to be bank employees to obtain a user's banking details.



Types of Online Transaction Frauds

Identity Theft: Sometimes, cybercriminals deliberately use another's identity to gain a financial advantage over someone else. Cybercriminals may also pose as someone else to obtain credit and other benefits in the other person's name.

Job Frauds: Cybercriminals portray incorrect details as an employer.

Banking Frauds: Some cybercriminals fraudulently obtain money from users for investment by posing as a bank or other financial institution.

Measures to Safeguard Ourselves from Online Fraud

We can safeguard ourselves from online fraud by keeping in mind the following points:

- Regularly update your banking passwords and Pin of the debit/credit cards.
- Be sure to check for the bank's security certificate details.
- Also, check for various signs such as green address lines, lock signs on websites, and HTTPS in the address bar to confirm you are visiting a secure bank website.
- Never share your bank and credit card details such as your online account password, card number, PIN, OTP, etc. with anyone.
- Always check the website URL starts with HTTPS. The website URL with HTTPS encrypts your data on the website and protects it from any kind of tampering.
- Avoid making online transactions using public Wi-Fi or a computer in a cyber cafe.
- Review the monthly statements of your bank account and credit cards to detect any unrecognised transactions.
- In case the credit/debit cards are stolen or lost, call the bank immediately and block your card/bank account.
- Never install pirated software on your mobile or computer. It is not only illegal but may also compromise the security of your devices.

Some rules we must remember while using Social Media:

- **Maintain Authenticity :** We must be honest about our identity. Never pretend to be someone else.
- **Always use a disclaimer :** While sharing personal views about something, we must make it clear that these are personal views.

- **Never pick fights on the internet:** We must convey our opinion carefully by choosing the right words.
- **Protect your identity :** Never list your full name, parent's details, home address or telephone number online.
- **Respect your audience :** Maintain good conduct, even on the Internet. Refrain from using slang, personal insults or obscene language.
- **Respect for other's feelings :** One must always be considerate and mindful of other's feelings on sensitive topics such as politics or religion.
- **Try to monitor comments :** One should prefer to monitor comments so as to maintain the quality of comments on a personal post/site.



Intellectual Property Rights

Intellectual property is a term that refers to the legal property rights of a person over creations of his/her mind, both artistic and commercial. Under Intellectual property Rights, the owners of the property are granted exclusive rights over their creation. These creations could be artistic, musical, or literary.

Intellectual property rights ensure that the creator's hard work is safe and protected from any unauthorised copying or piracy.

Types of Intellectual Property Rights (IPR)

There are three main types of Intellectual Property Rights:

- **Copyright :** It is the legal right given exclusively to the person for a fixed number of years to publish, and record the literary, artistic, musical, or musical use of his or her work. Copyright of work lasts even after the death of the originator.
- **Patent :** It is the right that gives an inventor the complete right to make, use, and sell his or her work for a specific time period. Usually, the validity period for a patent is 20 years.
- **Trademark :** It is a symbol, word or logo legally registered or established and used as representing a company or a product. Trademarks help to protect brand names, logos, and the design of the product. The validity period for a Trademark is 10 years and can be renewed after that.

Measures to Protect Intellectual Property Rights

We can take the following measures to protect Intellectual Property Rights:

- Do not share your business ideas with others.
- Have detailed drawings, descriptions, plans, and records that can prove it is your

creation.

- As soon as you have a business name and logo for your idea, you should register those Trademarks right away.

Plagiarism

It refers to the usage or imitation of the language and thoughts of another person projected as one's original work. It is considered a crime or fraudulent act.

Plagiarism as described by the Merriam-Webster dictionary is as follows:

- To steal and pass off ideas or words of another as one's own.
- To use another's production, without crediting the source.
- To commit literary theft.
- To present as new and original, an idea or product derived from an existing source.



Ways to Prevent Plagiarism

Some of the ways you can prevent plagiarism are:

- Use Citation-Citation refers to acknowledging the original writer and the source from where the material has been taken.
- Rephrase the matter.
- Use " " for statements quoted by another person.
- Encourage original ideas and use authentic resources.

VIRUS

A virus is a type of software or malware that spreads between several computers and corrupts data. It targets the computer's data and software. Its primary goal is to disrupt or interfere with the systems so that data can be corrupted or even leak.

Some indications of a virus attack are listed down below:

- Unwanted pop-ups that repeatedly appear
- Modifications to your desktop or files
- The system speed slows down and suddenly crashes. It can also make the computer shut down itself.
- You keep being logged out of your account.



- It sends out mass emails from your account to infect other machines with viruses.

Malicious activities are those that aim to compromise or corrupt the confidentiality of data or software in computers. There are numerous further varieties of malware and computer viruses. Some of the most common ones include:

Ransomware: It makes the victim's files inaccessible by disabling them. Once the ransom is paid, only then can they be accessed.

Spyware: It gathers information about the victims without their awareness. The information is then utilised to their benefit.

Malware for mobile devices: This malware harms mobile devices through phishing and other means.

Keyloggers: They record the victim's keystrokes. It gathers private information or sensitive data like passwords.

Cyber Safety

Cyber safety refers to the safe and responsible use of the Internet in order to safeguard one's personal information while not misusing anyone else's personal information.

We can take the following safety measures while using the Internet or computer:

- Install the most recent antivirus software on your computer.
- Use caution when entering your password on the internet.
- Do not respond to shady emails or strangers.
- Do not disclose your personal information to anyone online.
- Refuse friend requests from unfamiliar people.
- Always leave your privacy settings on.
- Be cautious when downloading.
- Be careful what you post on social media platforms.
- Encryption can be used to protect data privacy while transferring files between locations.



Ethical Hacking

Not all hacking is destructive. Some hackers use this technique for national security, creating safer systems, etc. This is known as ethical hacking. It is a legitimate practice to uncover potential data breaches and risks in a network or system. In order to find vulnerabilities that malicious hackers can exploit or eliminate, ethical hackers search the system or network.



Footprints are the impression we leave through a foot or walking on the ground while moving. In the same way, a digital footprint is a trail of data of a user that he leaves while using the Internet.

The information exchanged online through emails and attachments, uploading videos or images leave marks of personal information about you which is available to others online. When you allow cookies from websites, businesses might obtain your digital footprints. They may also be taken without your permission. Your data can be sold and utilised for gain if you provide them access. Cyberattacks may also emerge from this. A Digital Footprint is also known as Digital Dossier.

Some measures you can take to prevent digital footprints are:

- Beware of posting personal information online.
- Change your platform settings to private.
- Be mindful of what kind of feedback you can get when you share data
- Double-check before posting online to avoid accidental leakage of information.

Glossary

prevail	to become stronger or superior	hub	is a simple communication device.
surfing	looking or visiting websites on the internet	stalking	to follow someone illegally
confidentially	privacy	credentials	someone's background or general information
bulk	mass or size of something in large amount	lure	to attract someone into doing something
slang	informal terms or phrases		



LET'S HAVE A LOOK

- The Internet is also called 'the NET' or Network of Networks, which means International Network.
- Cyber Crimes are offences that are committed using computers and smart devices connected through the Internet.
- A virus is a type of software or malware that spreads between several computers and corrupts data.
- Cyber safety refers to the safe and responsible use of the Internet to safeguard one's personal information while not misusing anyone else's personal information.
- A digital footprint is a trail of data of a user that he leaves while using the internet.

Exercise

A. Multiple Choice Questions: Tick the correct answer.

1. The Internet is also called the network of:
a. networks b. computers c. mobiles d. tablets
2. Studying from home through the Internet is called:
a. i-Learning b. e-Learning c. c-Learning d. all of these
3. A Digital footprint is also known as:
a. Digital Diary b. Digital Dossier c. Database d. None of these
4. Why do hackers break into the other's computer system?
a. To steal important data b. To destroy the system
c. Both (a) and (b) d. None of these
5. Crimes that are committed through the internet are called:
a. Fiber crimes b. Internet crimes c. Cyber crimes d. None of these
6. Spamming refers to:
a. Sending an email from an unidentified source
b. Sending wrong information c. Sending bulk of information
d. None of these
7. We can adopt the following measures to avoid spam:
a. Preview your message before opening them b. Don't click on spam email
c. both a and b d. None of these
8. We can adopt the following measures to avoid email hacking:
a. Keep changing your passwords
b. Keep updating your operating system
c. Don't plug into devices you are not sure about
d. All of these

9. The technique used by cybercriminals to attain information from individuals is called:
a. Cyber bullying b. Cyber troll c. Social engineering d. All of these
10. Which of the following are not transaction fraud
a. Identity theft b. Cyber troll c. Banking fraud d. Job fraud

B. Write 'T' for True and 'F' for False in the boxes.

- | | |
|---|----------------------|
| 1. A digital footprint is an impression of a user that he leaves while using the Internet. | <input type="text"/> |
| 2. Always upload inappropriate content online. | <input type="text"/> |
| 3. Keep your privacy settings always off. | <input type="text"/> |
| 4. We should not use the content written by others without their permission. | <input type="text"/> |
| 5. Don't share your business ideas with others. | <input type="text"/> |
| 6. Don't install updated antivirus on your computer system. | <input type="text"/> |
| 7. Avoid friend requests from strangers. | <input type="text"/> |
| 8. Digital footprints are used to describe the traces that a person leaves when he uses the internet. | <input type="text"/> |

C. Answer the following short questions.

1. What is the Internet?
2. What is hacking?
3. Give any two examples of intellectual property rights.
4. Write two types to stop cyberbullying.
5. How can email spoofing be done?
6. What are the ways to prevent cyberbullying?
7. Describe the types of online transaction fraud.
8. What is the Internet? Write any three disadvantages of it.
9. What are digital footprints?
10. How can we avoid hacking?

D. Answer the following long questions.

1. What are Ethics? Write about the ethical use of the digital environment.
2. Write a detailed note on intellectual property rights.
3. Explain online transaction frauds in detail.
4. What is meant by social media? Write about its advantages and disadvantages as well.



Learning Activities

Application-based question.

Ayesha has got an email in her account. She is not sure whether the mail she has received is genuine or spam. Help her in identifying the spam.

(The activities below are neither listed in any particular order nor is this an exhaustive list. View them as recommendations)

• In-class Activity 1

Teachers can show videos on protecting your computer in class, and lead a discussion on ways to protect computers. Reflection questions can include (but not be limited to) What are some common ways in which computers can be protected? What happens when computers are not protected?

Suggested video: <https://www.youtube.com/watch?v=6mMZFoXbKqI>

• In-class Activity 2

Students will then work in groups to create a presentation that will teach parents how to protect their online identity and computer. Students can choose the tool they want to use to create their presentations:

They can: (1) record a skit with a video camera, (2) create an interactive lesson with Office Mix, (3) create a Sway, or (4) design a brochure using Word templates. (reference: Microsoft Digital Citizenship Module)

• In-class Activity 3

The teacher will place students in groups, and request each group to prepare a chart of ethical rules regarding the use of ICT. Students will present their posters, and the teacher can display posters in class.

• In-class Activity 4

The teacher can hold a debate, where two students can argue for and against the impact of using social media. The debate can include positives of social media, and students listening to the debate can vote for the winning debater. The teacher can ask reflection questions about the advantages of social media, such as connection to distant friends and relatives, selling goods & services, advertising revenue, learning more about culture and the world, entertainment, etc.

The teacher can also ask reflection questions related to the negative impact of social media, such as health consequences, addictive behaviour, sale of personal data, identify fraud, cyberstalking, etc.



Bibliography

- C., Christopher. 'Ethics - Introduction to Ethics: Ethics: A General Introduction.' Deepstash, 4 June 2021, <https://deepstash.com/article/73272/ethics-introduction-to-ethics-ethics-a-general-introduction>.
- Adhikary, Rajib. '(Cyber Safety-2) Confidentiality of Information.' MrRajib.com, 8 Sept. 2022, <https://mrrajib.com/cyber-safety-confidentiality-of-information/>.
- WELLS, NAOMI. What Does Citizenship Mean?: Digital Citizenship. ROSEN CLASSROOM, 2017.
- 'Ethics - Introduction to Ethics: Ethics: A General Introduction.' BBC, BBC, https://www.bbc.co.uk/ethics/introduction/intro_1.shtml.
- 'Touchpad Iprime Ver. 2.1 Class 7.' Google Books, Google, https://books.google.com.pk/books?id=r7mBEAAQBAJ&redir_esc=y.
- What Is Ethics? - King Edward VI School, Lichfield. <http://www.keslichfield.org.uk/wp-content/uploads/2020/04/What-is-ethics-2-RS-Resource.pdf>.
- School, Icfa Business. 'Ethics and Values,' Personal Effectiveness Management, <https://ebooks.ibsindia.org/pem/chapter/ethics-and-values/>.
- Health Resources and Services Administration (HRSA). 'Stop Bullying Home Page.' StopBullying.gov, 29 Mar. 2022, <https://www.stopbullying.gov/>.
- Worksheet No.: 2 Session: 2020-2021 - Ghsallahabad.org. <https://www.ghsallahabad.org/wp-content/uploads/2020/05/Class-7-Computer-WS-2.pdf>.
- Social Media Posting Can Have Dire Consequences. <https://www.northsidesun.com/opinion-columns/social-media-posting-can-have-dire-consequences>.



Answers

A: Tick the correct option.

1	a	2	b	3	b	4	c	5	c
6	a	7	c	8	d	9	c	10	b

B: True and False

1	T	2	F	3	F	4	T	5	T
6	F	7	T						