

A module
on
**LEADERSHIP FOR CYBER SAFETY AND SECURITY IN
SECONDARY SCHOOLS IN HARYANA**



National Centre for School Leadership



विद्यालय नेतृत्व अकादमी
राज्य शैक्षिक अनुसंधान एवं प्रशिक्षण परिषद्, हरियाणा
गुरुग्राम – 122001
School Leadership Academy
State Council of Educational Research & Training, Haryana, Gurugram
122001

LEADERSHIP FOR CYBER SAFETY AND SECURITY IN SECONDARY SCHOOLS IN HARYANA

Dr. Seema Sharma*

INTRODUCTION

The word “CYBER” denotes everything related to information technology (IT), a world of virtual reality, where there is no restriction and easy access. Cyber-crime is the crime committed by using virtual identity. Last decade is the witness of great technological advancement in all aspects of life. Education is one of them. From primary education to Higher education, from private institutions to government institutions, from schools to colleges, no area is untouched by technological intervention. The use of AVSAR App, EDUSAT and other digital platforms in Haryana has become mandatory for the government school students where they have to watch daily video lessons and attempt daily, weekly and mega surveys (tests) for regular assessments. This has now made the smartphones

compulsorily accessible to all the students from primary to secondary classes. When we cannot keep them away from technology, then we

surely need to teach them the advantages and disadvantages of using it. Technology offers the easiest mode of communication not only on personal level but also in teaching-learning processes. Students of all age groups are affected by the sweet-sour taste of this tool.

The smart devices in the hands of our adolescent and teenagers, is like a ticking bomb that can blow them off any time. Social Media is most arresting invention for our students. They can access anything at the click of a button and post any stuff on their social media account to draw attention of their peers, which may prove fatal for them. Children use social media to have fun, make and maintain friendships, share interests, explore identities and develop

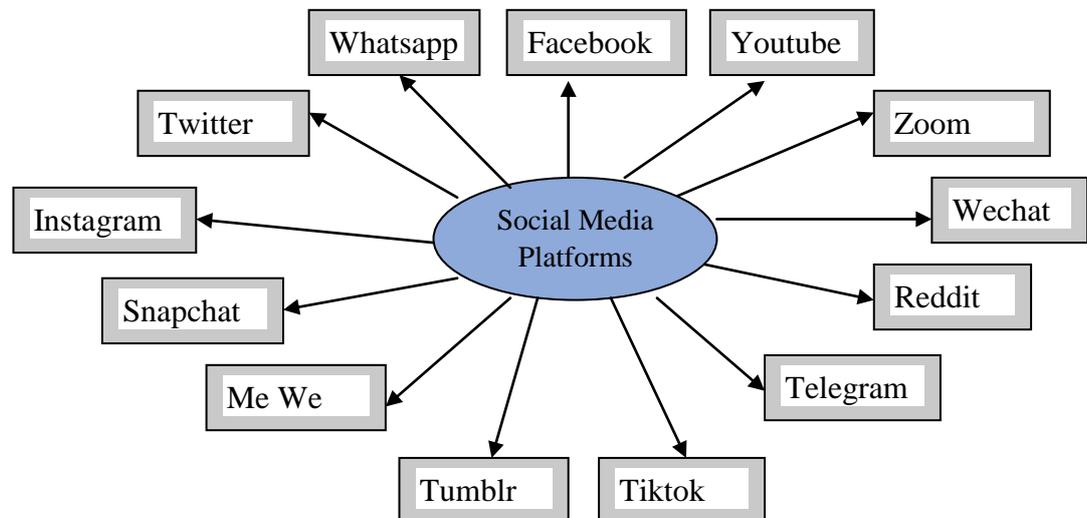
ARE YOU REALLY YOU?

- Some of your online “friends may not be who they say they are.
- Someone who tells you “she” is a teenager could be a 40-year old man posing as a teenager.



Gee, you sound really cute and we have the same birthday! We must be destined to meet!

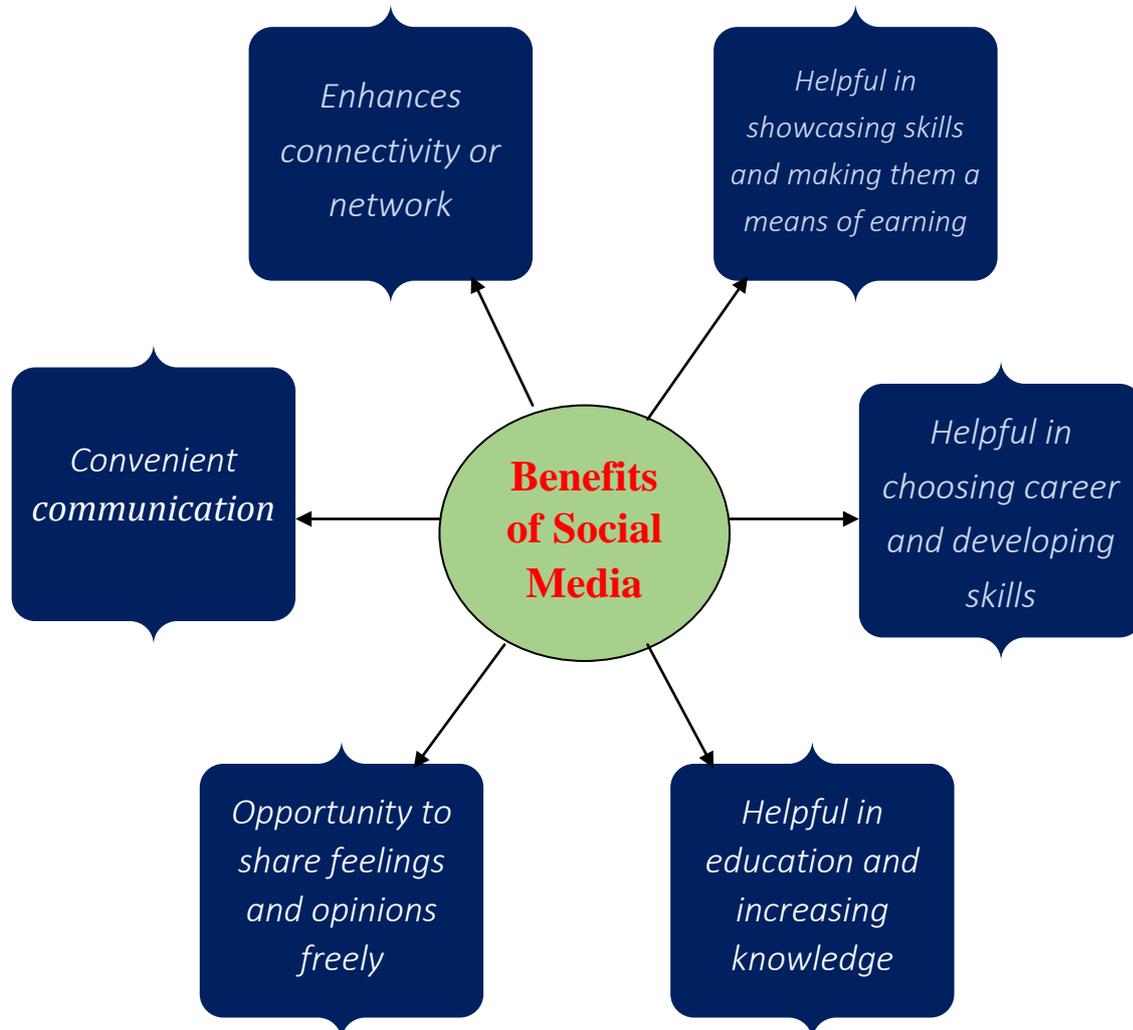
Well, I don't mind admitting I was homecoming queen and maybe we could celebrate our birthdays together.



Rule 1: Verify Your Connection

relationships with family. In their cyber space, they also get connected to wrong people - predators, cyber-bullies, drug-dealers and sexually abusive people, who can be very threatening.

Everyday newspapers and newchannels are covering cyber crime happening with youngsters. Savdhan India and so many other crime series are covering such cases to open the eye of people who are less aware about the cyber crime.



Virtual world is so alluring for students that they pay less attention to the advice of their elders. Cyber Security is now the most relevant concern in our schools, irrespective of age and gender. The more digitally connected students are, the more vulnerable they are to be cheated and victimized by the frauds and predators. Our secondary and senior secondary school students are at the greatest risk. They are the ones who are using a weapon without learning the rules of the war. It is, therefore, mandatory to teach them to safeguard their digital identities and activities lest they should find themselves duped. The more they share, the more they must care! [Cyber Self-Defence](#) is the need of hour in our schools. Therefore, it is the responsibility of a school leader to create such school environment where the knowledge of cyber-vulnerability, reporting of the crime and staying digitally safe may become a habit with them.

Rule2: Don't Privatize Your Social Life

This module is designed to develop an understanding about educating our students to be cyber safe and secure. They should be taught to make the constructive use of technology and neither harm anyone nor be harmed by it. Technology is a boon to the modern world, which has to be respected. Herewith, role of school leader regarding cyber safety and security of students is discussed.

TITLE OF THE MODULE

Leadership for Cyber Safety and Security in Secondary Schools in Haryana

OBJECTIVES

This module will enable school leaders to

- enlist the social media sites and apps popular among students
- know how students are using social media and cyber world
- discuss about the pros and cons of social media and cyber space for students
- identify the common cyber-crimes happening among teenagers
- enlist Do's and Dont's regarding cyber safety and security of students
- understand the causes and effects of cyber-crimes to students
- inculcate the cyber ethics among themselves and their students
- know about the role and responsibility of a school leader to guide students
- to make sure that each student is a cyber secure and cyber safe citizen



CYBER SECURITY AND SAFETY

Cyber security refers to the physical operation of the networks and computers over which the internet is delivered. If a hacker obtains remote control of your computer and alters lines of code in its operating system; if a company's network fails because hundreds of thousands or even millions of messages are directed at it by computers around the world; if a virus freezes all your data and criminals then contact you offering to unfreeze the data if you pay a ransom – those are all cybersecurity issues. The cyber world does offer security settings to safeguard our digital presence and stuff by putting passwords and screen locks. It is a part of the physical security of our devices. It helps us to keep our device safe even if it falls in others' hands. We can put security setting on our Email ids, social media account, posts on our social media, App settings and digital stuff saved on our devices, to keep it private.



Rule3: Avoid Posting Your Location

By contrast, **cyber safety** concerns the emotional and psychological impact of what you see, read and hear online. If a teenager receives Facebook or Instagram messages from people she knows at school, telling her she is stupid or ugly or she should kill herself – that is a cyber safety issue. If a child sees age-inappropriate sexual or violent content online – that is a cyber safety issue. If an adult finds that a former partner has posted pictures of him or her naked on social media or on a pornographic website – that is a cyber safety issue. What digital presence and what stuff is to be shared with whom is a safety issue. We can put a lock on everything we post on social media and Emails, but with whom we share our stuff is our choice.

Children, out of their lack of awareness and experience, make wrong choices and get connected to wrong people, share personal stuff and get cheated or victimized to a serious cyber-crime. Teenaged girls may sometimes fall in chatting or video calling with their boyfriends, even post their pictures and videos to get more likes/comments/shares, which may put them in a vulnerable situation. Even boys also post dirty stuff about the girls they know, to have their way with them or to flaunt their own masculinity among the peer groups. These children also bully each other on social media to exercise power over each other, without thinking about the after effects of it on any of them. Adolescents are going through an emotional conflict due to many reasons and when a stranger connects with them and appreciates them, they feel very happy and get attracted to that stranger who can be a fraud and abuse them later on. Hence, it is a matter of great concern for all of us.

WHAT HAPPENED	IS THE ACCOUNT HOLDERS' MONEY SAFE? 		
<ul style="list-style-type: none"> ▪ Fraudsters launched a malware attack and siphoned off ₹94.42 crore from Cosmos Bank on August 11 and 13 	<ul style="list-style-type: none"> ▪ The account holders' money is safe now and in the future, says the bank, as the proxy switch was operative on the payment gateway, not the 'Core Banking System' 		
HOW IT HAPPENED	WHO'S BEHIND IT?	<ul style="list-style-type: none"> ▪ The bank has appointed a professional forensic agency to investigate the attack 	<ul style="list-style-type: none"> ▪ banking and ATMs have been suspended
<ul style="list-style-type: none"> ▪ The fraudsters created a proxy switch to interact with the VISA and Rupay payment gateway ▪ They used the fake switch to approve 12,000 transactions at ATMs in 28 countries, and 2,800 transactions in India 	<ul style="list-style-type: none"> ▪ Experts suspect the hand of Lazarus, a group linked to the \$81 million heist in Bangladesh and the 2014 attack on Sony Pictures 	<ul style="list-style-type: none"> ▪ The servers, internet banking, mobile 	<p>WHAT'S NEXT?</p> <ul style="list-style-type: none"> ▪ The bank said it will take 3-4 days for the alternative switch to become operational

Cybercriminals and hackers easily get access to our students' most sensitive data and personal information. Phishers frequently trick their websites, email addresses, and social media profiles to gain access to personal information and to misuse them for their mean purposes. Popular services like free Wi-Fi, ATMs, and public computers can all lead to data compromise, financial loss, and identity theft just as it is important to learn about keeping one's belongings safe and secure in real life, similarly one needs to learn how to keep one's devices and digital stuff safe from on-site attackers. Physical security is the protection of people, property, and physical assets from people or actions that could cause damage or loss. But it is often overlooked in case of cybersecurity. And physical security in cyber space is all the more important. For this reason, the cyber security industry has now grown into a \$30 billion industry. All the firewalls in the world can't help you if an

Rule4: Avoid Over-Freuding On Social Media

attacker removes your storage media from the storage room in your device.

The attacker uses malicious software (Malware), to download viruses, worms, trojans and other harmful computer programs in our devices to get access to our sensitive information.

Some recent examples of Malware attacks:

CovidLock, ransomware, 2020 -It offers to give more information about the disease. Once installed, it encrypts data from our devices and denies access to data by the victim.

Lockergoga, ransomware, 2019 -It infected large corporations in the world by sending malicious emails, phishing scams and also credentials theft. It blocks victim's access to the system.

WannaCry, ransomware, 2017 - It attacked via phishing emails and encrypted Windows reaching more than 200,000 people across the world including hospitals, universities and large companies. It is not only institutions or corporations that are vulnerable to cyber-attacks, but individuals are targets too, often because they use insecure public networks and store personal information on their mobile phones like bank account details, PIN no., address, date of birth, sensitive personal information, which can be misused. Students can not only be taught about it, but can also be guided to become Cyber-attack professionals by obtaining a degree from some institute or doing a certified course online from NCERT/COURSERA/UDEMY. As cyber security professionals work to increase their knowledge of threats and cyber security information, earning an online cyber security master's degree can be invaluable.



Students can not only be taught about it, but can also be guided to become Cyber-attack professionals by obtaining a degree from some institute or doing a certified course online from NCERT/COURSERA/UDEMY. As cyber security professionals work to increase their knowledge of threats and cyber security information, earning an online cyber security master's degree can be invaluable.

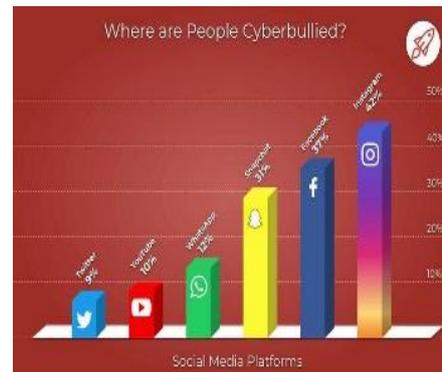
TYPES OF CYBER THREATS TO STUDENTS

Cyber-intelligence reports 2019 say that hackers increasingly targeted smart homes and internet of things (IoT) devices, such as smart TVs, voice assistants, connected baby monitors and cellphones. Hackers who successfully compromise a connected home not only gain access to users' Wi-Fi credentials/ Bluetooth, but may also gain access to their data, such as medical records, bank statements and website login information. In such case, all that is in the phone is in their hands.

- 1. Identity theft and invasion of privacy-** Personal or financial information is used to impersonate as you to commit fraudulent activities online. A type of crime in which your private information is stolen and used for criminal activities. You may receive a mail/message from an unknown source with a link and a note of winning a prize or lottery or gift. Don't click that link/contact number etc., or your personal information may get stolen.
- 2. Internet fraud-** Using internet services or software to beguile victims. This is done by accessing chat, website, Email etc. to create personal or financial havoc for you difficult to repair. Types of Internet frauds can be:

Rule5: Protect Your Account with a Strong Password

- **Deep-fakes** -We're now living in the virtual world of Deep-fakes, Deep-fakes are synthetic media in which a person appearing in an existing image or video is replaced with someone else. Anyone with a skill of digital manipulation can impersonate anyone and achieve his/her malicious goal.
 - **Viral hoaxes** -The kind of social media hoaxes that appeal to our emotions. Behind every cute, sensational, funny viral video that gets millions of views/likes/shares, there can be someone ready to trick us. This can also be intended to spread communal or political hatred, panic or national chaos. Students get easily beguiled by such Deep-fakes and Viral-hoaxes. They even keep forwarding such messages and videos without investigating their authenticity. The Indian Cyber-intelligence is getting more and more vigilant with each passing day and any creator/promoter of such activities is sued by law. A school leader needs to keep guiding his students regarding their responsibility in creating and forwarding such stuff.
3. **ATM fraud**-Using your ATM card or information connected to it without your knowledge.
 4. **Wire fraud**-An attempt to commit fraud with the aid of some form of electronic communication such as a telephone, computer or mobile etc. Even using charger, USB cable, Bluetooth etc. from an unknown source can also aid to it.
 5. **File sharing and piracy**-Illegal distribution or reuse of digital **files** that is traded over the internet. This crime applies to digital books, movies, PC games, hacked software, music etc.
 6. **Cyber Bullying**-Bullying or harassing or threatening someone by using electronic means. It is bullying using electronic means. Online bullying is very common among teenagers.
 7. **Fake IDs on social media**- When someone makes a fake ID on social media account to dupe or intimidate or blackmail others. Adolescents and teenagers are the most victimized by such fake IDs. This happens because of lack of awareness. Students should be made aware about online stranger danger, who stalk them and beguile them to their own end.
 8. **Child pornography**- Making/sharing a photo, film, video or image of a minor showing him/her taking part in a sexual activity or anything encouraging such activities online. Read more about it in POCSO Act (link shared in Ref.)
 9. **Hacking**- Hacking is the activity of identifying weaknesses in a computer device or a network to penetrate the security to gain access to any data or information stored in the device. Password cracking is one of the examples.
 10. **Intellectual Property Theft (IPT)**- It is the infringement of a trademark, patent, copyright. Reusing of someone's images/videos/textual content without giving credit to the owner, as if it is your own, falls into this category. Students explore their academic content online and sometimes copy-paste it on social media with their own



Rule6: Block/Report Unfriendly Connections

name. They need to understand that this is violation of intellectual property right.

11. Phishing- someone trying to get your personal information online through fake sites, spam emails, and other trickery.

MANAGING THE DIGITAL FOOTPRINT (Preventive Measures)

What is Digital Footprint?

Our Digital Footprint is the record of our online activity. It shows where we have been, the data we have shared, and the traces or links we have left behind. It is just like leaving our foot impression on a wet sand by the sea, by following which we can be tracked or caught. Whenever we sign up, log in, or hit send, we are leaving a digital impression behind. Unfortunately, these types of footprints aren't washed away by the tide. That's why it's so important to guide the students to make informed decisions about what to share.

How do our students leave Digital Footprints on social media?

- Using social media on their computer, mobile phone or other devices.
- Logging into sites with their social media credentials (like personal details/password).
- Connecting with family, friends or strangers.
- Sharing personal information, data, and photos with their connections.
- Joining a dating site or app, and chatting in personal chat-box.

These are just a few examples of the categories that make up their digital footprint and activities that make them vulnerable.

How can a school leader control it?

A school leader can guide the students repeatedly through assemblies by reminding them to take the following steps:

- It is our collective responsibility to ensure the authenticity of any content we forward. The one who sends any content that may spread communal violence, defame the governing bodies or is pornographic, is liable for punishment under cyber laws. Hence, think before forwarding a message.
- Be careful about what you share on social media in terms of personal photos, videos or

CASELET 1: Posting obscene videos on Instagram

Shikha is a school teacher in Faridabad. She teaches Hindi to classes 11-12. She has been taking online classes in WhatsApp group of each class due to Pandemic COVID-19. This calls for her active presence online on social media as well. She is very friendly with the children, so all her students, boys or girls, feel free to discuss their problems with her. One day while scrolling the posts on Instagram, she comes across an obscene video of a boy in her class whose name is Akshay. He seemed to have got his video shot by his friend, doing some intimate activities with his girlfriend. There are so many likes/ shares and comments on this post. This shocks Shikha to no end and she decided to guide Akshay. And through Akshay, she also wants to teach the same lesson of Cyber safety to the whole class.

Q.1 What should she do to make Akshay understand his mistake and rectify it without spoiling his self-esteem?

Q.2 Should she inform his parents and involve them? Why or why not?

Q.3 Should she talk in person to both the boy and the girl to sensitize them against such posts? Why or why not?

Rule7: Keep an Eye on Your Own Account

family information.

- Be careful about the one you connect with through social media account. Never connect with strangers or meet anyone in person whom you personally don't know
- Search your name and evaluate your reputation.
- Keep personal information private.
- Use the grandma rule when posting anything online. What if your grandma sees what you post on social media? Think and act accordingly!
- Protect your stuff by taking security measures on Apps
- Use pattern/ PIN locks
- Know and use your settings and security keys
- Lock your device and screen
- Always log out of public computers
- Use Incognito mode when using a public computer
- Safe Online activities
- Never do random chat with anyone
- Only chat with family and friends
- Never do anything on a webcam you don't want to see with your family
- Think before commenting on anything

READ TO DIGEST

For a Case of unsafe online activities, read at:

http://timesofindia.indiatimes.com/articleshow/83834939.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst_prime

DEALING WITH THE THREATS TO CYBER WELLNESS OF STUDENTS AS A SCHOOL LEADER

What can you do as a school leader?

1. Organize periodic workshops for the students by calling officers from the cyber cell, women cell, cyber-crime lawyers, social worker etc.
2. A school leader must be active on social media platforms or instruct teachers for it to keep a check on the regular social media activities being done by their students.
3. A school leader can make a Facebook page or a YouTube channel for the school to be handled by a team of students. This will put the digital energies of the students on a creative and constructive path. Even school's digital news board or magazine for students can also be introduced for this purpose. Such initiatives will help in deflecting the students from destructive form of Digital literacy and they will explore good content only.
4. **Organize a training program** for teachers and students for educating them to take the following steps to ensure cyber security-
 - Using a more secure firewall and authentic anti-virus for network and server which can block any unauthorized access from outside the network is perhaps the best idea.
 - Never leave your devices unattended in office, classroom, hotel room, meeting room etc. Always carry it with you or keep it at a secure place.
 - Never give your mobile or devices to a stranger. Learn to say 'No' just as you never allow any stranger to enter your house.
 - Keep servers and routers in a locked room and control access to it with a strong

Rule8: Be Especially Careful with Posts and Pictures

password.

- Always pick up your documents from printers, faxes, photocopiers and multi-functional devices promptly.
- Never keep the 'remember this password' box ticked for any website.
- Never store passwords in any file on common computers.
- Never download or click any link received from unknown sources.
- Always keep a backup of data stored in your devices lest you should lose access to it in case of Malware attack.
- Establish an incident management system in school to support the victims. Train and equip the team with relevant contact numbers, offices and other portals related to cyber cell. Report criminal incidents to law enforcement.

5. **Aware the teachers and students to do this before forwarding a content-**

- Evaluate the website sending it
- Investigate the source
- Who holds the copyright?
- What do they want you to believe?
- Detecting Lies and Staying True
- Don't be fooled by cool and professional looking websites
- Decipher the intent and investigate the source
- Compare at least 3 sources of information. Remember to include one source with an opposing viewpoint
- Always check the facts you find

READ TO DIGEST
Students Kidnap Classmate, Beat Him Up to Make "Viral Video"

The classmate alleged that the students shot the video of thrashing him to make it "viral on social media"

<https://www.ndtv.com/cities/4-students-kidnap-classmate-beat-him-up-to-make-viral-video-1926001>

6. **Appoint a group of students in school with a teacher as the supervisor.** Train the teachers to watch online activities of all students and counsel them as and when needed. In addition, guide them to:

- Know ways to deal with the bullies
- Block and report about the bully.
- Do not respond or retaliate
- Reach out to elders or officials for help
- Be civil and never bully
- Save evidences

Cyber Crime	Punishments
Cyber Stalking	3 years, or with fine up to 2 lakh
Cyber Pornography including Child Pornography	10 years and with fine may extend to 10 Lakh
Intellectual Property Crimes	3 years, or with fine up to 2 lakh
Cyber Terrorism	Imprisonment for a term, may extend to 7 years
Cyber Hacking	3 years, or with fine up to 2 lakh
Phishing	3 years, or with fine up to 2 lakh
Invading Privacy	2 years, or with fine up to 1 lakh

7. **Cyber Safety Law**-Make the participants aware about the cyber laws by sharing updated information about laws.
8. **Get parents involved** - Educating parents on the dangers of inappropriate usage and encouraging them to talk to their children about it is an effective way to ensure that students are safe online, both at school and at home.
9. **Provide resources to students** - It's unlikely that your students want to listen to an hour-long lecture on the dangers of the internet, so, provide them with resources like videos on internet safety and links/contact no. to report in case of complaints.
10. **Stick to private online communities** - The Facebook Guide for Teachers and The Twitter Guide for Teachers discuss ways in which to create private online learning communities for

Rule9: Be Judicious about what you share and consider any posting permanent

yourself and your students.

11. **Create Virtual Platform to help peers under your supervision:** Sometimes, children hesitate to convey their problems to elders, but they may share among a trusted peer group. Create a virtual platform, like google form, WhatsApp/Telegram group to allow students to discuss any discomfort they face online. Allow students to help each other under your guidance.
12. **Create pledges for your students** - A pledge is a great way to ensure that students continue online safety even after you have finished educating them about it. Having students sign pledges. The samples may be picked from "[Internet Safety Pledges](#)"

13. Sensitize the students

- Are you Uncomfortable online? Inform the trusted teacher/elder or the trusted peer group! This is exactly the same as we teach about ‘Good Touch/Bad Touch’.
- Threatened with harm/blackmailing or any other online crime? Inform the police about this. Contact your nearest Cyber-crime branch with the help of your trusted teacher or elders/parents.
- Don’t post any personal information online – like your address, email address or mobile number.
- Think carefully before posting pictures or videos of yourself.
- Keep your privacy settings as tight as possible
- Never share your passwords with anyone, not even your closest friend
- Don’t befriend anyone you don’t know
- Don’t meet up with people you’ve met online
- Think carefully about what you say before you post something online

14. Update the knowledge of the teachers and the students:

- What a phishing scam looks like.
- Get free anti-phishing add-ons
- Don’t give any information to any unsecured site.
- Keep changing your passwords.
- Install firewalls.

CASELET 2: Gaming Addiction

Mr. Rajesh Ahuja is the school head of a senior secondary school in Gurugram. He gets a complaint against a child Raman from class 8. His teachers complain that he keeps sleeping in the class, remains absent-minded and does not do his Homework properly. His performance is continuously going down. He also misbehaves in the class and his classmates are full of complaints about his violent behaviour. All the teachers have tried hard to set him right but in vain. Now they come to the Principal Mr. Ahuja and ask for his intervention as Raman has made up a gang of mischievous students who follow his behaviour. Mr. Ahuja plans to talk to his parents before talking to Raman. He calls his parents to the school. Raman’s father is a strict parent and complains that he gave Raman a smartphone as a gift on securing 3rd position in class 7. Raman was very happy, but these days he started playing some games on his phone and keeps spending 9-10 hours playing it. Sometimes he sits the whole night playing on it. His father had scolded him many times, even punished to mend his ways and focus on studies, but all in vain. Mr. Ahuja now understands the parents were as much at fault as Raman. So, he decides to counsel Raman as well as his parents.

Q.1 What advice should he give his parents to set Raman right without letting him know that they were teaching him a lesson?

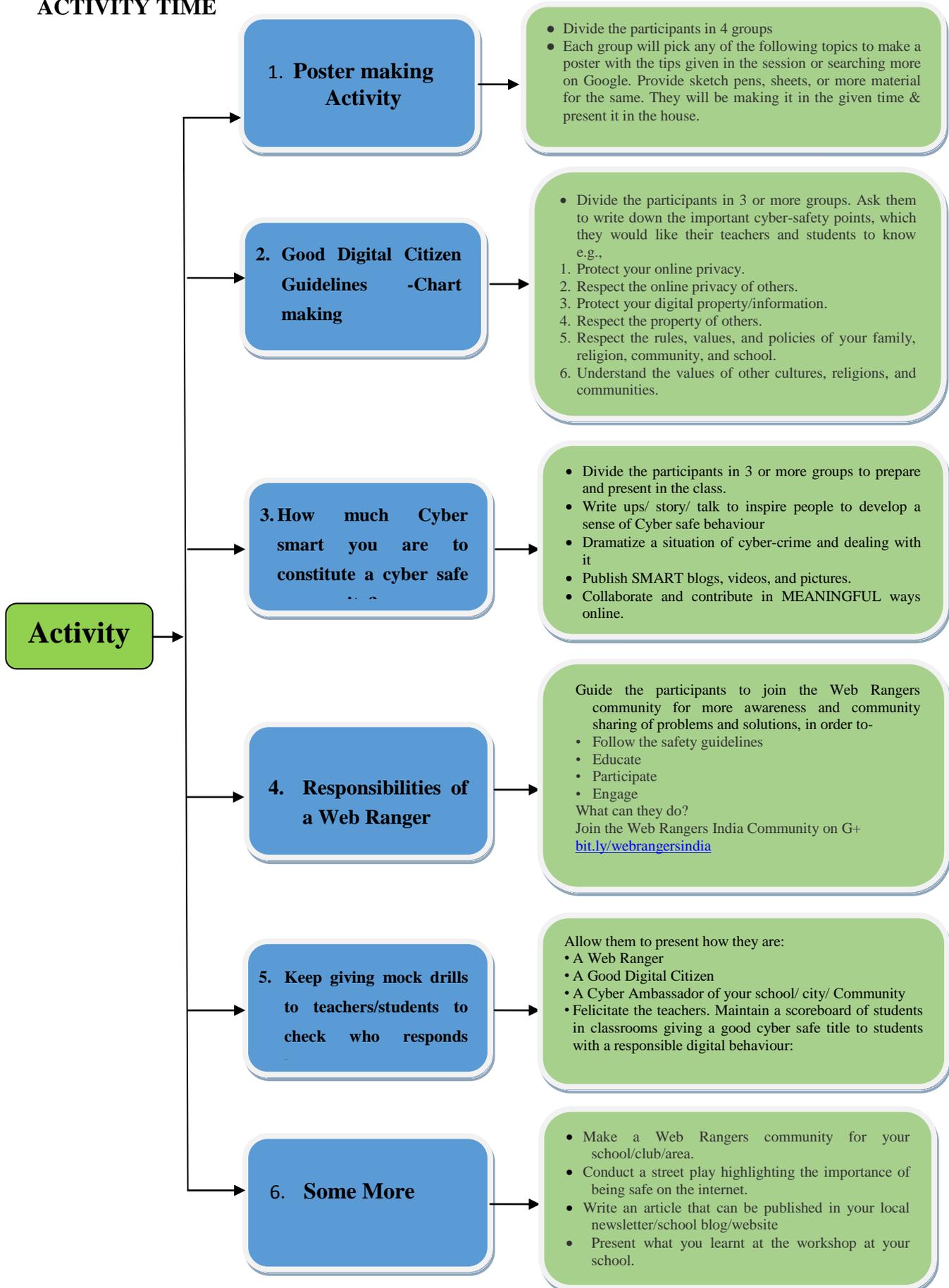
Q.2 Which method should he adopt to guide Raman, as he is a teenager and has become a violent child now?

Q.3 What Strategy is needed to rehabilitate Raman from his addiction?

Rule10: Be careful about strange wifi

- Don’t be tempted by those pop-ups.

ACTIVITY TIME



References:

1. https://niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf
2. <https://cybercrime.gov.in/>
3. https://itpd.ncert.gov.in/pluginfile.php/10327/mod_page/content/56/Final-%20session%20on%20Children%20%20POCSO-converted.pdf
4. <https://www.cert-in.org.in/>
5. <https://www.cyberswachhtakendra.gov.in/>
6. **Online Safety | National Government Services Portal**
https://services.india.gov.in/service/listing?cat_id=89&ln=en

*Dr. Seema Sharma, Senior Lecturer, DIET, Pali, Faridabad, Haryana.
MA (Eng), PhD (English), B.Ed.

Dr. Seema Sharma is specialised in ICT in teaching learning and school leadership. She is e-content creator as well as reviewer of English Subject for Haryana State. She has published various research papers in various national and international journals. She is excellent composer and a book of poems is credited in her account. She is also a regular poet of Indian Mythology in an International Journal.