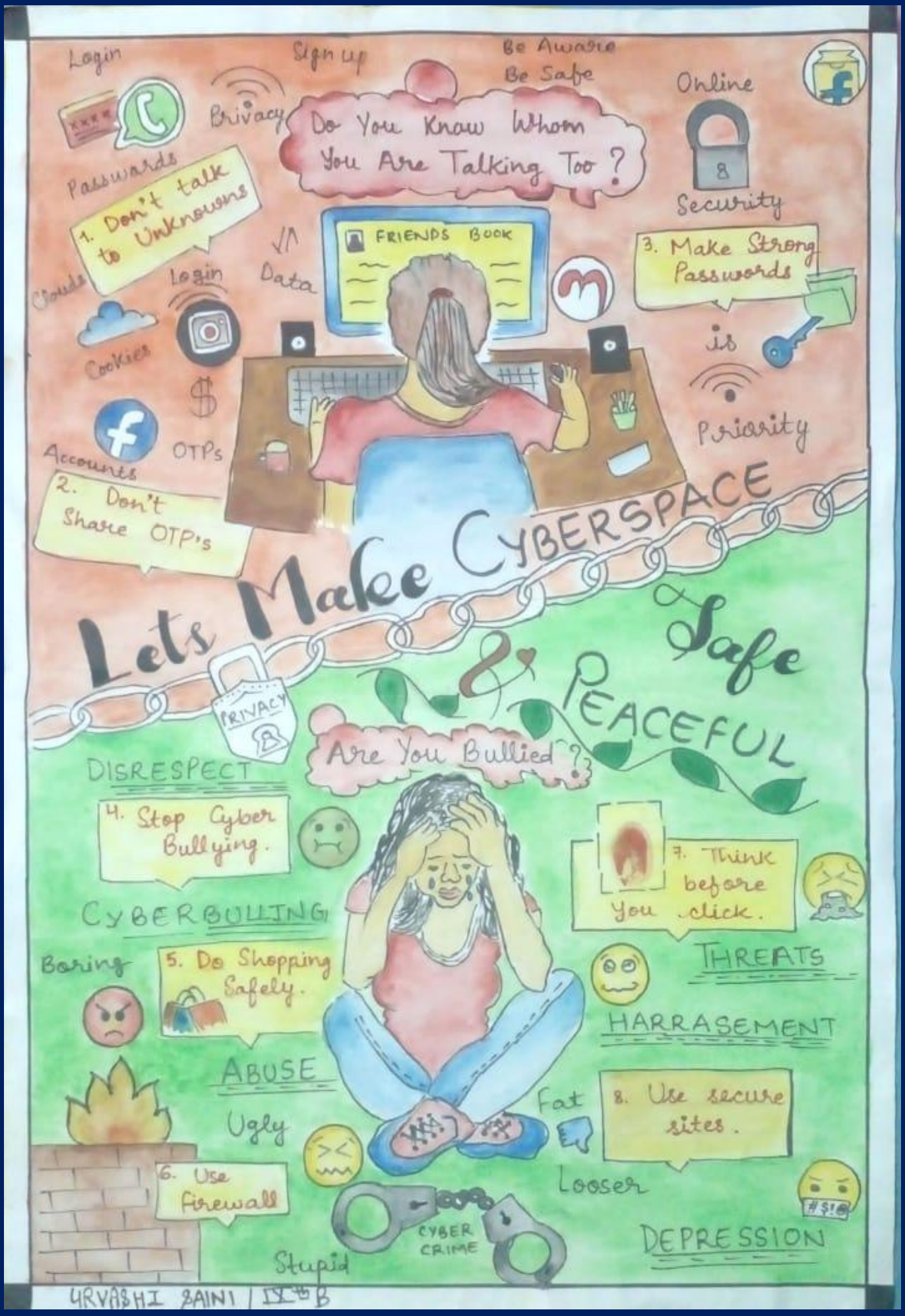

CYBER
SAFETY
MANUAL

WHY CYBER SAFETY?

In today's digital age, the internet plays a major role in education, communication and entertainment. While it offers countless opportunities, it also presents serious risks. Cyber safety is the practice of protecting oneself from online threats and using digital platforms responsibly, ethically and securely.

Being cyber-safe is not just about avoiding danger; it is about becoming a responsible digital citizen.


Login
Sign up
Be Aware
Be Safe
Online
Privacy
Do You Know Whom You Are Talking Too ?
Passwards
1. Don't talk to Unknowns
Security
FRIENDS BOOK
Data
Cloud
Login
3. Make Strong Passwords
is
Cookies
Priority
Accounts
OTPs
2. Don't Share OTP's
Lets Make CYBERSPACE
Safe
&
PEACEFUL
PRIVACY
Are You Bullied ?
DISRESPECT
4. Stop Cyber Bullying.
7. Think before you click.
CYBERBULLING
THREATS
Boring
5. Do Shopping Safely.
HARRASEMENT
ABUSE
Fat
8. Use secure sites.
Ugly
6. Use Firewall
Looser
#$!@
CYBER CRIME
DEPRESSION
Stupid
URVASHI SAINI / IX-B

CYBER SAFETY: DO'S AND DON'TS

❖ Personal Information & Privacy

- Do protect your personal information such as your address, phone number, name of your school, passwords, and financial details. Don't share passwords, PINs, or OTPs with anyone.
- Do use strong, unique passwords for different accounts and change them regularly. Don't use simple or predictable passwords.
- Do enable two-factor authentication (2FA) whenever available.
- Do review privacy settings on social media platforms and limit who can view your content.
- Do log out of accounts when using shared or public devices. Don't save login credentials on any public or shared devices.
- Do store sensitive information securely and encrypt files when possible. Don't reveal your real-time location or travel plans online.

Cyber Security

Protect your data
protect yourself

Cyber Security means protecting computers, mobile devices and online data from threats like viruses and hackers.

Some Common Cyber Threats Are :

Phishing → Fake messages that steal your information.

Malware → Viruses that damage your device.

Safety Tips

- Use strong unique passwords
- Dont click on unknown links
- Keep your software updated
- Avoid public Wi-fi.

Charvi Kiraula
IX - B

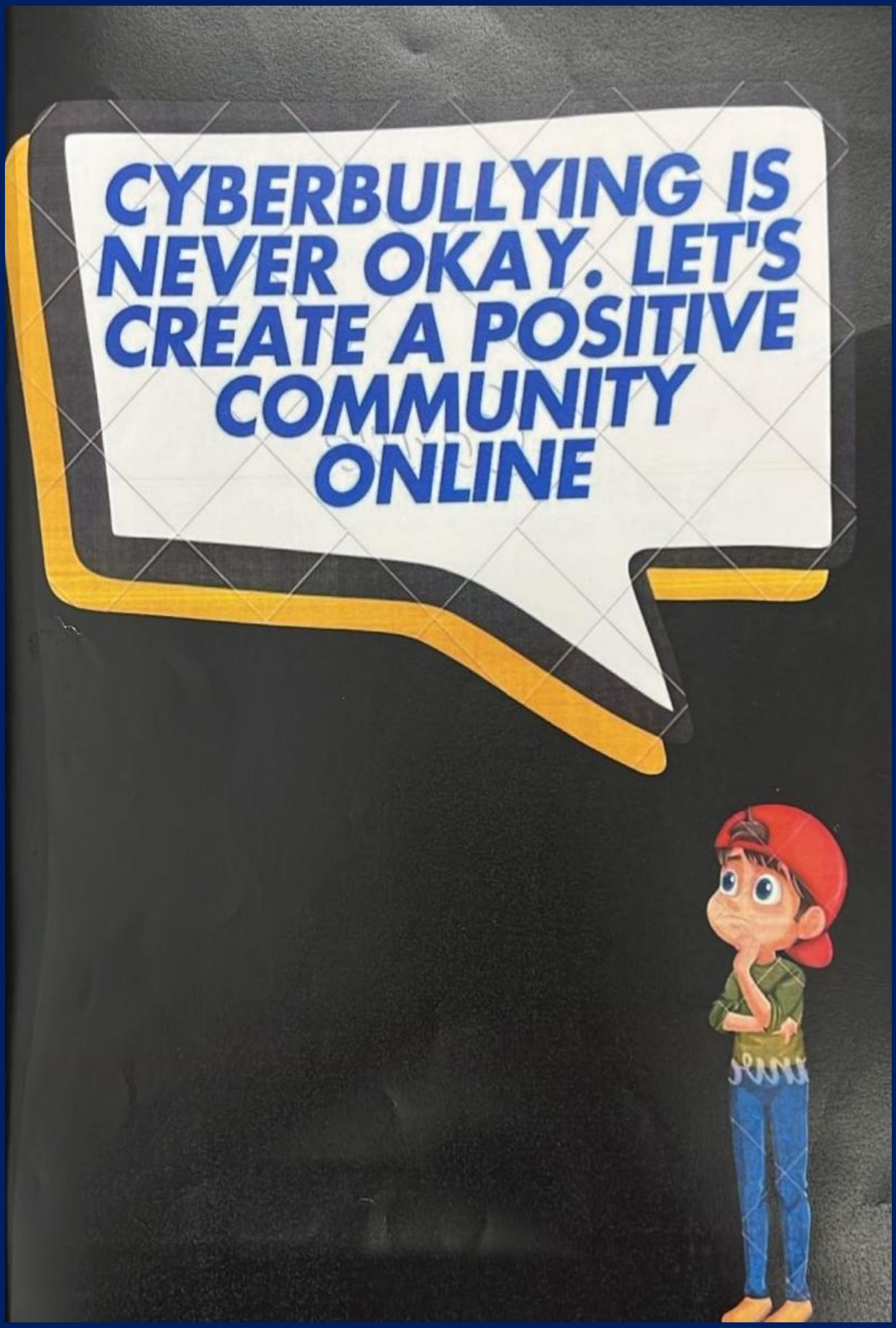
❖ Digital Awareness & Responsibility

- Do think critically before posting or sharing any content online.
- Do understand that your digital footprint is permanent and may affect future academic or career opportunities.
- Do verify information before forwarding messages, news or images. Don’t spread rumours, misinformation, or fake news.
- Do acknowledge sources and give proper credit for online content. Don’t violate copyright laws or use pirated software.
- Do use the internet for productive learning and skill development. Don’t engage in cyber harassment, hate speech, or abusive behaviour.
- Do maintain academic honesty while using digital resources.
- Do practice ethical online behaviour and respect digital laws. Don’t normalise inappropriate online behaviour.


Cyber-Bullying:-
By:- Ayansh Wadhwa
IX-A
Hey everyone, thanks for coming together today. I thought it'd be good to talk about cyberbullying—it's becoming such a serious issue.
Totally agree. I read that over 37% of young people between the ages of 12 and 17 have been bullied online. That's huge.
And it also causes serious mental health issues—depression, anxiety, even led to suicide in some cases.
We have to find ways through which we can stop it.
Supporting victims and reporting abuse can make a big difference, even if it seems small.
Absolutely, and we should speak up when we see bullying—silence will not stop the bully.
We need to educate people about digital responsibility and respectful communication.
We must try to warn people about this issue.
By taking these measures, we can stop Cyber-bullying.
We must keep our accounts private and only accept requests from people we know.

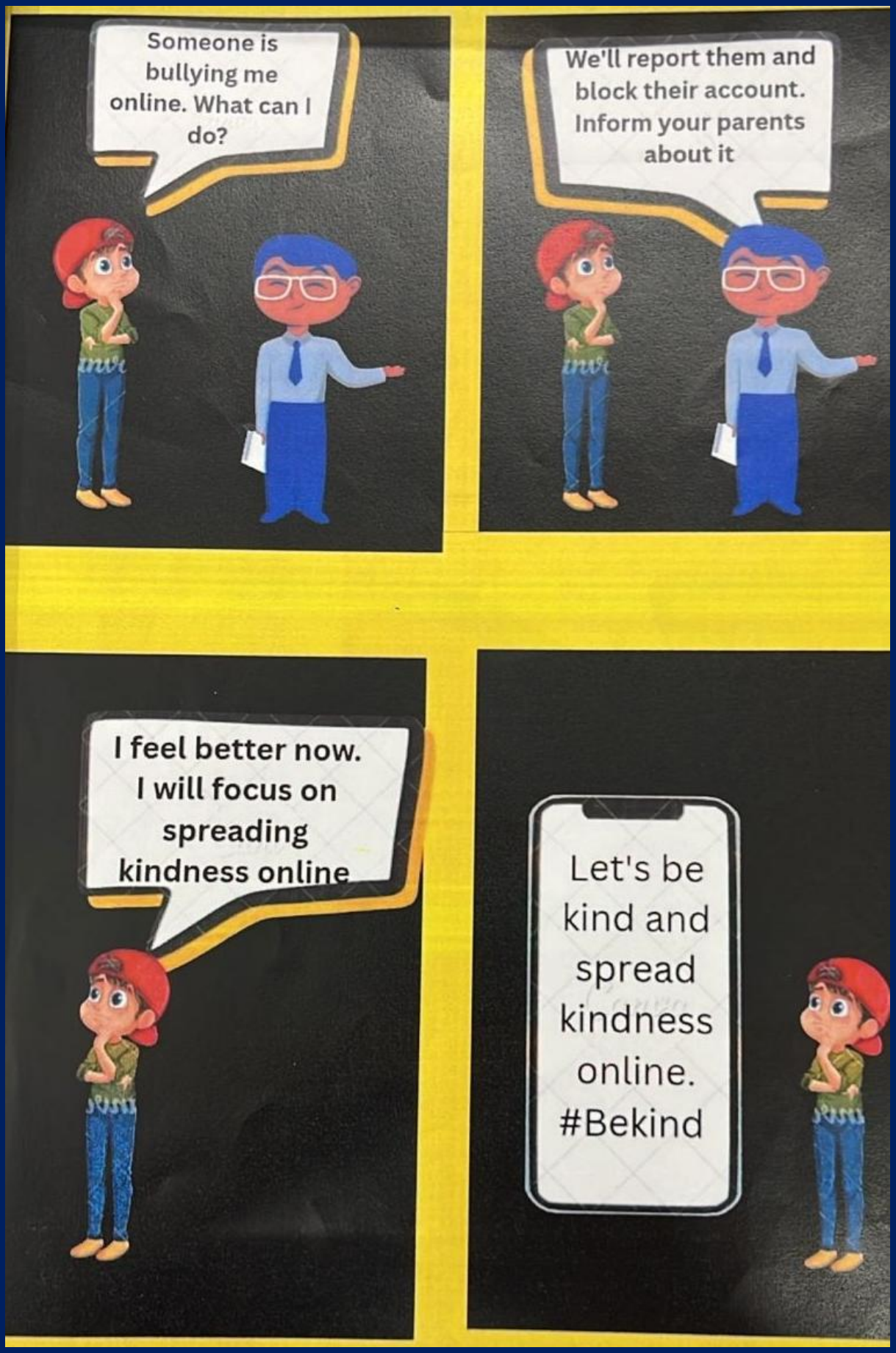
❖ Social Media & Online Communication

- Do communicate respectfully and practice good digital etiquette. Don’t accept friend or follow requests from strangers.
- Do ask for consent before posting photos, videos, or personal information of others. Don’t reveal private conversations or screenshots publicly.
- Do use appropriate language in online discussions and comments. Don’t post or forward explicit or offensive material.
- Do block, mute, or report users who display abusive or suspicious behaviour.
- Do communicate clearly and responsibly in group chats and forums. Don’t overshare emotions, conflicts, or personal problems online.
- Do pause and reflect before responding to controversial messages.
- Do promote positivity and responsible digital citizenship online. Don’t trust viral content without verification.


CYBERBULLYING IS NEVER OKAY. LET'S CREATE A POSITIVE COMMUNITY ONLINE

❖ Cyberbullying & Online Safety

- Do recognise different forms of cyberbullying, including trolling and harassment. Don’t shame, ridicule, or threaten others online.
- Do save screenshots and records of abusive messages or posts.
- Do report cyberbullying to parents, teachers, or school authorities promptly. Don’t ignore persistent online abuse or threats.
- Do support classmates who are victims of online harassment. Don’t stay silent when you witness cyberbullying.
- Do stand up against bullying without using offensive language.
- Do seek counselling or professional help if online abuse affects mental health. Don’t hesitate to speak to your elders or your parents.
- Do help create a respectful and inclusive online environment.


Someone is bullying me online. What can I do?
We'll report them and block their account. Inform your parents about it
I feel better now. I will focus on spreading kindness online
Let's be kind and spread kindness online. #Bekind

❖ Online Scams & Security

- Do remain alert to phishing emails and fake messages. Don’t ignore security alerts or any sort of warning.
- Do check sender details and URLs before clicking on links. Don’t click on unknown links or pop-up advertisements.
- Do delete suspicious emails or messages immediately.
- Do update operating systems, apps, and antivirus software regularly. Don’t download software from unofficial sources.
- Do use secure and trusted websites for transactions or downloads. Don’t share bank or payment details online.
- Do monitor online accounts for unusual or unauthorised activity. Don’t use unsecured public Wi-Fi for sensitive activities.
- Do report scam attempts to a trusted adult or platform administrators.

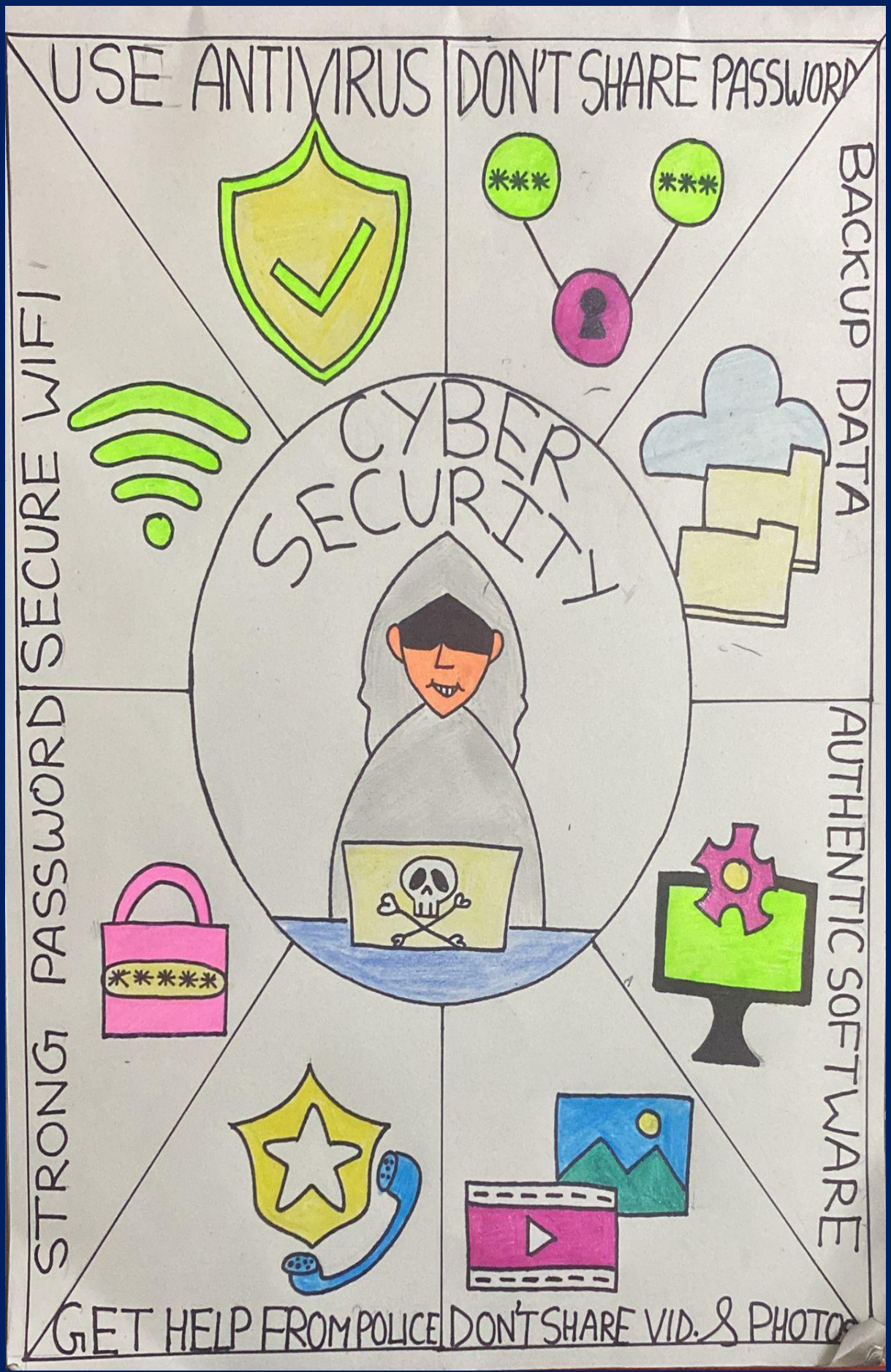
THINK BEFORE YOU CLICK
STAY CYBER SAFE!

One careless click can lead
to scams. Stay sharp online!

AARYAN SEHGAL IX-A

❖ Gaming & Entertainment

- Do use age-appropriate games and content. Don’t engage yourself in online gambling or betting.
- Do restrict chat and voice features when necessary. Don’t share personal photos, videos, or voice data with gamers.
- Do avoid in-game purchases without parental approval. Don’t make impulsive purchases, always consult your parents.
- Do set time limits for gaming and streaming activities. Don’t spend too much time on them.
- Do maintain healthy posture and eye care while using screens. Don’t neglect your sleep or studies, and pay attention to your physical health.
- Do take regular breaks from all the digital devices that you have. Don’t avoid academics and physical activities over screen time.


USE ANTIVIRUS
DON'T SHARE PASSWORD
BACKUP DATA
AUTHENTIC SOFTWARE
DON'T SHARE VID. & PHOTOS
GET HELP FROM POLICE
STRONG PASSWORD
SECURE WIFI
CYBER SECURITY

❖ Seeking Help & Reporting Issues

- Do report any cybercrime incidents on the cybersecurity helpline number - 1930.
- Do communicate openly with parents or guardians about online activities. Don’t hesitate to seek help.
- Do inform teachers or counsellors about serious online issues. Don’t hide online threats or uncomfortable experiences.
- Do seek guidance before meeting any online acquaintance. Don’t meet online contacts without parental or adult supervision.
- Do report illegal, harmful or explicit content immediately. Don’t share self-harm or dangerous content.
- Do ask for help if you feel threatened or manipulated online. Don’t respond to blackmail or extortion attempts.
- Do participate in cyber safety awareness programmes. Don’t assume all online platforms are secure.
- Do trust your instincts if something feels unsafe online. Don’t ignore your intuition.

REMEMBER

Responsible digital behaviour is a shared responsibility.

By following these do’s and don’ts, we can create a safer and more respectful online environment for ourselves and for others around us.