

# Cyber Well-being

This book helps young people understand how to stay safe, responsible, and confident in the digital world. It covers online privacy, social media use, cyberbullying, and digital balance, while encouraging healthy habits and critical thinking. The focus is on building resilience and making smart choices online. It also highlights the importance of protecting digital identity and respecting others in virtual spaces. By the end, learners gain practical skills to navigate technology with awareness and responsibility.

- [Introduction & Overview](#)
- [Session 1: Getting Started with Cyber Well-being.](#)
- [Session 2: Keeping Your Accounts Safe](#)
- [Session 3: What We Leave Behind Online \(Digital Footprints\)](#)
- [Session 4: When Online Feels Unsafe \(Cyberbullying and Response\)](#)

# Introduction & Overview

## Welcome to the Cyber Well-being Module!

We all spend a lot of time online these days. Whether you are using a smartphone, tablet, or computer, the internet is a fantastic place to chat with friends, watch videos, play games, and learn new things.

However, just like in the physical world, the online world comes with its own set of risks. Every message you send, link you click, and photo you post leaves a permanent mark, and not everyone you meet online has good intentions.

This module is designed to help you navigate the digital world safely and confidently. We will not use complicated tech jargon here. Instead, through simple everyday stories and practical activities, you will learn how to protect your personal privacy, secure your accounts, spot fake messages, and handle uncomfortable online situations without fear.

Our goal is not to stop you from enjoying the internet, but to make sure you stay in control of your digital life. By the end of these four sessions, you will know exactly how to protect yourself, your reputation, and your future opportunities whenever you go online.

**One line to remember throughout this module:** *Stop. Think. Check. Ask.*

## Table of Contents: Cyber Well-being

| Session   | Title                                            | Focus                                                                                                                                  |
|-----------|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Session 1 | Getting Started with Cyber Well-being            | Understanding online safety, smartphone use in daily life, protecting personal information, and knowing who to contact for help.       |
| Session 2 | Keeping Your Accounts Safe                       | Creating strong passwords, keeping OTPs and login details private, using privacy settings, and spotting suspicious or urgent messages. |
| Session 3 | What We Leave Behind Online (Digital Footprints) | Understanding digital footprints, the risks of oversharing, location tags, and thinking before posting.                                |

|                  |                                                          |                                                                                                                                                |
|------------------|----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Session 4</b> | When Online Feels Unsafe<br>(Cyberbullying and Response) | Recognizing cyberbullying and scams, saving proof like screenshots, using the S.T.A.R.R. Action Plan, and reporting problems to trusted adults |
|------------------|----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|

# Session 1: Getting Started with Cyber Well-being.

We spend a lot of time online, on smartphones, tablets, or computers. Sometimes it is for fun, sometimes for learning, and sometimes just to pass the time. But every message, click, and post is not always safe. This session helps us understand cyber well-being and basic online safety.

## Session Objectives

By the end of this session, you will be able to:

- Explain cyber well-being in simple terms.
- Understand how smartphones are used in daily life and how they connect us online.
- Identify personal information and decide what can be shared with friends, family, or strangers, and what should stay private.
- Recognize safe and unsafe online actions.
- Determine appropriate actions when something online feels strange.
- Identify who to contact when help is needed.

## What is cyber well-being?

Cyber well-being means using the internet in a safe and healthy way. It means protecting your privacy, thinking before you click or reply, being respectful online, and asking for help when something feels wrong.

## The world of smartphones

Smartphones are part of daily life ; people use them to talk to family, learn new things, play games, watch videos, and stay in touch with friends. Along with these benefits, smartphones also connect users to people they do not know, so it is important to be thoughtful about what is done and shared on them.

- Smartphones help us learn, connect with family and friends, enjoy entertainment, and access information quickly.
- Smartphones can also expose us to strangers online, unwanted messages, and apps or links that are not always safe.

# Who can I share information with?

Not all information should be shared in the same way with everyone. It is important to think about who is receiving the information before sharing anything online.

| Who You're Talking To | What Is Usually Okay to Share        | What to Avoid Sharing                                                    |
|-----------------------|--------------------------------------|--------------------------------------------------------------------------|
| Family                | Daily updates, feelings, and plans   | Passwords and OTPs should still be protected carefully                   |
| Friends               | Hobbies, interests, and general chat | Home address, exact location, and private photos                         |
| Strangers online      | Nothing personal                     | Name, address, phone number, school details, photos, passwords, and OTPs |

# What should stay private and why?

Not everything belongs online. Sharing certain details can put your safety, security, and future opportunities at risk. Review this guide to understand why keeping these items private is essential for your well-being.

| Personal Information                     | Why it needs to be private                                                                             |
|------------------------------------------|--------------------------------------------------------------------------------------------------------|
| <b>Home Address &amp; Exact Location</b> | Sharing this can allow strangers to track your physical whereabouts, compromising your safety.         |
| <b>Phone Number</b>                      | Publicly posting your number can lead to unwanted calls, spam, and potential harassment.               |
| <b>Date of Birth</b>                     | This is a key piece of information used for identity theft and account takeovers.                      |
| <b>Passwords, PINs &amp; OTPs</b>        | These are the "keys" to your digital life; sharing them gives others total control over your accounts. |
| <b>School/Institution Details</b>        | Revealing where you live or study can help malicious actors target you or your community.              |
| <b>Private Photos</b>                    | Once shared, control over who sees or uses them can be lost.                                           |

**Privacy Rule of Thumb:** If you wouldn't tell a total stranger this information in the street, you shouldn't post it online where everyone can see it.

## Safe online habits

| Habit                           | Action                                                                                                                     |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>Protect Your Accounts</b>    | Use strong, unique passwords for all your online accounts.                                                                 |
| <b>Keep Credentials Private</b> | Never share passwords, PINs, or One-Time Passwords (OTPs) with anyone.                                                     |
| <b>Verify Before Clicking</b>   | Avoid opening unknown or suspicious links, regardless of how urgent they may appear.                                       |
| <b>Seek Guidance</b>            | Ask a trusted adult or staff member before downloading any new apps or games.                                              |
| <b>Secure Your Sessions</b>     | Always log out of your accounts after using public or shared devices.                                                      |
| <b>Speak Up</b>                 | Immediately inform a trusted adult if you receive a message or see content that makes you feel scared, confused, or upset. |

# Story: Rohit and the fake prize

Rohit is 16 and lives in a child care institution. He receives a WhatsApp message from an unknown number saying, “You have won a free gaming voucher. Click the link and send your mobile number and OTP to claim it”. Rohit feels excited for a moment, then pauses and realizes that a stranger should not be asking for an OTP. He shows the message to a staff member instead of clicking, and the staff member tells him it is unsafe and asks him to block the number.

## Activity 1: True or False

1. You should share your home address online.  
☐ True ☐ False
  2. Strong passwords use letters, numbers, and symbols.  
☐ True ☐ False
  3. If a stranger asks for your personal information online, it is safe to give it.  
☐ True ☐ False
  4. Cyberbullying means being mean to someone using the internet.  
☐ True ☐ False
  5. If something online makes you uncomfortable, you should tell a trusted adult.  
☐ True ☐ False
- 

## Activity 2: Safe or unsafe

1. Clicking on an unknown link.  
☐ Safe ☐ Unsafe
2. Asking permission before downloading an app.  
☐ Safe ☐ Unsafe
3. Sharing an OTP with a friend.  
☐ Safe ☐ Unsafe

4. Logging out after using a public computer.  
☐ Safe ☐ Unsafe
  5. Sending a rude message in a group chat.  
☐ Safe ☐ Unsafe
  6. Telling a trusted adult about a strange message.  
☐ Safe ☐ Unsafe
- 

## Activity 3: Keep it private

Sort these items into the right category by deciding what is safe to share online and what should stay private.

| Item              | Category (Safe to Share / Do Not Share) |
|-------------------|-----------------------------------------|
| Favourite colour  |                                         |
| Hobby             |                                         |
| Favourite song    |                                         |
| Favourite food    |                                         |
| Favourite subject |                                         |
| Home address      |                                         |
| Phone number      |                                         |
| Date of birth     |                                         |
| Password          |                                         |
| OTP               |                                         |

---

## Activity 4: Who Am I Talking To?



For each item below, decide who it is okay to share it with: **Family, Close Friends, or No One Online.**

7. My school name: \_\_\_\_\_
8. My daily routine or timing: \_\_\_\_\_
9. My phone number: \_\_\_\_\_
10. My favourite hobby: \_\_\_\_\_
11. My home address: \_\_\_\_\_

## Activity 4: Match the situation with the response

| Situation                                   | Response                     |
|---------------------------------------------|------------------------------|
| Unknown message asking for personal details | Tell a trusted adult         |
| Suspicious link                             | Do not click it              |
| Rude online comment                         | Block and report             |
| Request for password or OTP                 | Do not share                 |
| Confusing message from a stranger           | Ask for help before replying |

## Activity 5: Fill in the blanks

1. Never share your \_\_\_\_\_ with strangers online.
2. Always ask \_\_\_\_\_ before downloading apps or games.
3. If you see something scary online, tell \_\_\_\_\_.
4. A strong password should be hard to \_\_\_\_\_.
5. OTP stands for \_\_\_\_\_.

# Activity 6: What would you do?

1. What should you do if someone is mean to you online?

---

2. Why is it important to log out from public computers?

---

3. Name one way to make your password strong.

---

4. Who is one trusted adult you can speak to if something online feels wrong?

---

## Quick Recap

| Topic                       | Action                                                                                                                    |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Personal Privacy</b>     | Smartphones help with learning, connection, and entertainment, but they also connect users to strangers and risks online. |
| <b>Credentials Security</b> | Do not share personal information with strangers, and think carefully about who you are sharing with.                     |
| <b>Link Safety</b>          | Think before clicking unknown links.                                                                                      |
| <b>Reporting</b>            | Talk to a trusted adult if something online feels wrong.                                                                  |

One line to remember

**Stop. Think. Check. Ask.**

# Session 2: Keeping Your Accounts Safe

Many things we do online depend on accounts and logins. If someone gets into your account, they can see your messages, use your name, or misuse your information. This session is about passwords, OTPs, privacy settings, and fake messages.

## Session Objective

By the end of this session, you will be able to:

- Understand what makes a strong password.
- Keep OTPs and login details private.
- Use basic privacy settings.
- Spot suspicious messages, links, and login requests.
- Know what to do when something feels fake or urgent.

## Account safety habits

| Habit                    | Action/Description                                                    |
|--------------------------|-----------------------------------------------------------------------|
| Use Strong Passwords     | Create unique, complex passwords using letters, numbers, and symbols. |
| Keep Credentials Private | Never share OTPs, PINs, or login details with anyone.                 |
| Maintain Privacy         | Regularly review and use privacy settings on all your apps.           |
| Secure Sessions          | Always log out of accounts when using public or shared devices.       |

| Habit                 | Action/Description                                                    |
|-----------------------|-----------------------------------------------------------------------|
| Keep Software Updated | Ensure apps and operating systems are updated to the latest versions. |

# What is a strong password?

A strong password is not your name, birthday, or phone number. It is not "1234" or "password". It uses a mix of letters, numbers, and symbols, and is different from the password you use for other accounts.

# What should stay private online?

| Private Information | Reason for Privacy                                       |
|---------------------|----------------------------------------------------------|
| Passwords           | Must remain confidential to prevent unauthorized access. |
| OTPs                | Must remain confidential to prevent unauthorized access. |
| PINs                | Must remain confidential to prevent unauthorized access. |
| Security Answers    | Must remain confidential to prevent unauthorized access. |
| Recovery Codes      | Must remain confidential to prevent unauthorized access. |
| Net Banking Details | Must remain confidential to prevent unauthorized access. |
| ATM PINs            | Must remain confidential to prevent unauthorized access. |

# Messages that should make you pause

| Suspicious Message | Why It's a Warning Sign |
|--------------------|-------------------------|
|--------------------|-------------------------|

|                                                         |                                                  |
|---------------------------------------------------------|--------------------------------------------------|
| "Your account will be blocked if you do not click now." | Creates false urgency to panic you.              |
| "You have won a prize. Click to claim."                 | Too good to be true; often leads to scams.       |
| "Send your OTP to verify."                              | Legitimate services will never ask for your OTP. |
| "Install this app urgently."                            | Often a trick to install malicious software.     |

# Story: Sneha and the urgent message

Sneha is 17. She receives a message that looks like it is from a popular app. It says her account will be suspended unless she clicks a link and confirms her OTP. Sneha feels nervous. The message looks urgent. She notices a small spelling mistake and a strange link. She decides not to click and shows it to a staff member. The staff member tells her it is fake and asks her to delete and block.

## Activity 1: True or False

1. It is okay to share your OTP with a friend.  
☐ True ☐ False
2. A strong password should be easy to guess.  
☐ True ☐ False
3. You should use the same simple password everywhere.  
☐ True ☐ False
4. Privacy settings can help control who sees your posts.  
☐ True ☐ False
5. A message asking for your OTP should be checked carefully.  
☐ True ☐ False

# Activity 2: Safe or unsafe

6. Using a password like your name and birth year.  
☐ Safe ☐ Unsafe
  7. Turning on privacy settings in an app.  
☐ Safe ☐ Unsafe
  8. Sharing your login with a friend.  
☐ Safe ☐ Unsafe
  9. Clicking on a message that says "claim now".  
☐ Safe ☐ Unsafe
  10. Logging out after using a shared device.  
☐ Safe ☐ Unsafe
  11. Keeping your software updated.  
☐ Safe ☐ Unsafe
- 

# Activity 3: Spot the fake message

1. "Click this link to get a free prize."  
☐ Safe ☐ Suspicious
  2. "Please send your OTP to verify your account."  
☐ Safe ☐ Suspicious
  3. "Your friend tagged you in a photo."  
☐ Safe ☐ Suspicious
  4. "Install this app now or your account will be blocked."  
☐ Safe ☐ Suspicious
  5. "Check the sender and ask before replying."  
☐ Safe ☐ Suspicious
-

# Activity 4: Build a better password

| Weak Password<br>(Avoid) | Better Password<br>(Example) |
|--------------------------|------------------------------|
| 1234                     | Riya@4821                    |
| password                 | Sun#2026                     |
| anjali                   | M@ngo57!                     |
| 111111                   | Blue@19Star                  |

My own password pattern could be: \_\_\_\_\_

One thing I should avoid in my password is: \_\_\_\_\_

---

# Activity 5: Fill in the blanks

1. Never share your \_\_\_\_\_ with anyone.
  2. A strong password should be hard to \_\_\_\_\_.
  3. OTP means one-time \_\_\_\_\_.
  4. Privacy settings help control who can see your \_\_\_\_\_.
  5. If a message feels urgent and strange, first \_\_\_\_\_ before acting.
- 

# Activity 6: What would you do?

1. What would you do if someone asked for your OTP? \_\_\_\_\_
  2. What would you do if a link looks suspicious? \_\_\_\_\_
  3. Why is it useful to keep your account private? \_\_\_\_\_
  4. Who can you ask if you are not sure about a message? \_\_\_\_\_
- 
- 

# Quick Recap

| Topic              | Key Takeaway                                                   |
|--------------------|----------------------------------------------------------------|
| Password Safety    | Passwords should be strong and private.                        |
| OTP Security       | OTPs should never be shared.                                   |
| Account Protection | Use privacy settings and keep software updated.                |
| Threat Awareness   | Fake messages often create urgency.                            |
| Seeking Support    | If something feels wrong, stop and check with a trusted adult. |

# One line to remember

**Private means private. Passwords, OTPs, and login details stay with me.**



# Session 3: What We Leave Behind Online (Digital Footprints)

Every post, like, comment, share, and search leaves a small trail online. This is called a digital footprint. This session helps you understand what you leave behind and how oversharing can affect safety and reputation.

## Session Objective

By the end of this session, you will be able to:

- Understand what a digital footprint is.
- Identify actions that leave a trail online.
- Think before posting or sharing.
- Understand how oversharing can affect safety and reputation.
- Use simple privacy choices to protect yourself.

## What is a digital footprint?

A digital footprint is the permanent trail of information you leave behind every time you use the internet, like a set of tracks you leave in the sand. It includes everything you do online, such as:

- **Posts:** Sharing a photo or status update.
- **Comments:** Writing text under someone else's post.
- **Likes:** Reacting with a heart or thumbs-up.
- **Shares:** Forwarding or reposting content.

- **Searches:** Looking up topics or questions.
- **Tags:** Adding names or locations to a post or photo.
- **Messages:** Sending private or group chat history.

**Remember:** once you share something online, it can be easily copied or saved. Your digital footprint becomes a permanent record that can impact your life in several ways:

- **Privacy and Safety:** Your online history can reveal sensitive details about where you are and what you do.
  - **Reputation:** What you post shapes how others perceive your character and values.
  - **Relationships:** Your digital behavior influences how friends and family trust you.
  - **Future Opportunities:** Many schools and employers look at your online presence when considering you for admissions or jobs.
- 

# What can make your digital footprint risky?

Certain online habits can expose you to unnecessary risks. Being mindful of these actions helps you maintain a safer online presence:

- **Sharing your real-time location:** Tagging where you are can allow others to track your physical movements.
- **Posting personal photos publicly:** Publicly sharing photos can compromise your privacy and allow others to use your images without permission.
- **Using weak privacy settings:** Open profiles allow strangers to see information intended only for friends and family.
- **Sharing school or institution details:** Mentioning exactly where you study or live helps malicious actors identify your daily routine or location.
- **Interacting with strangers:** Replying to unknown people can lead to unwanted contact, scams, or cyberbullying.

# Story: Nisha and the location tag

Nisha is 16 and likes posting selfies. She uploads a photo in front of her institution gate and adds a location tag. Many people like the post. A friend later points out that the photo shows where she lives. Nisha realises she has shared more than she wanted. She removes the location tag, changes privacy settings, and starts thinking more before posting.

## Activity 1: True or False

1. Everything I post online disappears after one day.  
☐ True ☐ False
  2. A digital footprint is the trail we leave online.  
☐ True ☐ False
  3. A location tag can show where I am.  
☐ True ☐ False
  4. Only adults have a digital footprint.  
☐ True ☐ False
  5. I should think before posting a photo or comment.  
☐ True ☐ False
- 

## Activity 2: Safe or unsafe

6. Posting your school location openly.  
☐ Safe ☐ Unsafe
7. Setting your account to private.  
☐ Safe ☐ Unsafe
8. Sharing a meme with no personal details.  
☐ Safe ☐ Unsafe
9. Tagging your live location in a public post.  
☐ Safe ☐ Unsafe

10. Checking who can view your story.

☐ Safe ☐ Unsafe

11. Commenting rudely under someone's photo.

☐ Safe ☐ Unsafe

---

## Activity 3: Match the action with the result

| Action                 | Footprint Left Behind |
|------------------------|-----------------------|
| Posting a photo online | Visible post          |
| Searching for a topic  | Search trail          |
| Liking a video         | Activity trail        |
| Tagging your location  | Location trail        |
| Writing a comment      | Comment trail         |

---

## Activity 4: Think Before You Post

Reflect on the following questions to help you make safer online choices:

**1. Safety Check:** If a photo reveals your home, school, or institution, what risks might it create?

Why is it safer to keep that location private?

---

---

**2. Impact Awareness:** How could a message or comment you share today affect you or someone else in the future?

---

---

**3. Pre-Posting Habits:** What specific steps (like checking privacy settings or removing location tags) do you take to protect your privacy before you hit 'post'?

---

---

**4. Seeking Support:** Who are the trusted adults or friends you can turn to for advice when you're unsure if a post is safe to share?

---

---

## Activity 5: Make it safer

1. "I am at my institution gate right now." Safer version: \_\_\_\_\_
  2. "My class starts at 9 am every day." Safer version: \_\_\_\_\_
  3. "Here is my photo with location on." Safer version: \_\_\_\_\_
  4. "Add me, anyone can see this account." Safer version: \_\_\_\_\_
- 

## Activity 6: Fill in the blanks

1. A digital \_\_\_\_\_ is the trail we leave online.
  2. A location tag can show where we \_\_\_\_\_.
  3. . Before posting, it is good to think, "Will this \_\_\_\_\_ online?"
  4. Privacy settings help protect our \_\_\_\_\_.
  5. Once something is shared online, it can be \_\_\_\_\_ or copied.
- 

## Activity 7: What would you do?

1. What would you do if you posted something by mistake?

2. What would you do if someone asks for your location online?

3. What would you do if you are not sure whether a photo is safe to post?

4. How can a private account help you?

## Quick Recap

| Topic                          | Key Point                                                         |
|--------------------------------|-------------------------------------------------------------------|
| <b>Online Actions</b>          | Every online action leaves a permanent trail.                     |
| <b>Safety &amp; Reputation</b> | Oversharing can impact your safety and how others see you.        |
| <b>Privacy Settings</b>        | Settings help, but they are not perfect protection.               |
| <b>Thoughtful Posting</b>      | Think before you post, because the internet remembers everything. |

## One line to remember

**If I would not want it remembered later, I should think twice before posting it.**

# Session 4: When Online Feels Unsafe (Cyberbullying and Response)

Even with good habits, unsafe situations can still happen online. This session is about cyberbullying, rude or threatening messages, fake links and scams, saving proof, blocking and reporting, and talking to trusted adults.

## Session Objective

By the end of this session, you will be able to:

- Recognise unsafe online behaviour.
- Understand what cyberbullying and scams look like.
- Know how to save proof such as screenshots.
- Know when to tell a trusted adult.
- Know basic reporting options.

## What can go wrong online?

| Risk           | Description                                             |
|----------------|---------------------------------------------------------|
| Cyberbullying  | Mean comments, threats, and repeated insults.           |
| Fake Messages  | Prize claims, fake verification, and urgent warnings.   |
| Privacy Misuse | Someone sharing your photo or personal details wrongly. |
| Account Misuse | Someone trying to get your password or OTP.             |

| Risk                       | Description                                                        |
|----------------------------|--------------------------------------------------------------------|
| <b>Stress from Overuse</b> | Feeling upset, tired, or confused after being online for too long. |

# What should you do first?

## S.T.A.R.R. Action Plan for Online Safety

- **Stop:** Do not reply in anger or fear. Take a moment to pause.
- **Take Screenshots:** Save evidence of the conversation or incident immediately.
- **Avoid:** Block the person to stop further contact.
- **Reach Out:** Tell a trusted adult, staff member, or counselor who can help.
- **Report:** Use the platform's official tools to flag the harmful behavior.

# Story: Imran and the game chat

Imran is 17 and plays online games. A stranger in the game chat asks him for a photo and offers free coins. When Imran does not respond, the stranger becomes rude and sends threatening messages. Imran does not argue. He takes screenshots, blocks the user, and tells a staff member. The staff member helps him report the account and reminds him that speaking up was the right step.

---

# Activity 1: True or False

1. Cyberbullying only happens on social media.  
☐ True ☐ False
2. If something online feels wrong, it is better to stay silent.  
☐ True ☐ False
3. Screenshots can be useful proof.  
☐ True ☐ False



4. A trusted adult can help you report online trouble.

☐ True ☐ False

5. It is okay to share your OTP to stop someone from being angry.

☐ True ☐ False

## Activity 2: Safe response or not?

1. Replying angrily to a rude message.

☐ Safe Response ☐ Not a Safe Response

2. Taking a screenshot of a threatening chat.

☐ Safe Response ☐ Not a Safe Response

3. Sharing your password to avoid conflict.

☐ Safe Response ☐ Not a Safe Response

4. Blocking a stranger who keeps messaging you.

☐ Safe Response ☐ Not a Safe Response

5. Telling a staff member or trusted adult.

☐ Safe Response ☐ Not a Safe Response

6. Deleting all evidence before telling anyone.

☐ Safe Response ☐ Not a Safe Response

---

## Activity 3: Practice Your Online Safety Responses

Match each situation with the correct response from the options below.

| Situation | Response |
|-----------|----------|
|-----------|----------|

|                                  |       |
|----------------------------------|-------|
| Rude repeated messages           | _____ |
| Suspicious link                  | _____ |
| Someone asks for password or OTP | _____ |
| Fake prize message               | _____ |
| Harassing chat                   | _____ |

# Response Options:

- Block and tell a trusted adult
- Do not click and report
- Do not share
- Delete and warn others
- Save screenshots and report

# Activity 4: Fill in the blanks

1. If something online feels wrong, first \_\_\_\_\_.
2. Take a \_\_\_\_\_ if you need proof.
3. Do not share your \_\_\_\_\_ or OTP.
4. Tell a \_\_\_\_\_ adult.
5. Report the problem on the platform or through the right \_\_\_\_\_.

# Healthy online habits

| Healthy Online Habits                                  | Online Habits to Avoid                                     |
|--------------------------------------------------------|------------------------------------------------------------|
| ● Taking breaks from screen time                       | ● Staying online very late every day                       |
| ● Talking to someone if a message upsets you           | ● Checking messages again and again when you feel stressed |
| ● Keeping some offline time for sleep, study, and rest |                                                            |

# Quick recap

| Core Concept       | Recommended Practice                                          |
|--------------------|---------------------------------------------------------------|
| Unsafe Situations  | Do not ignore them; take immediate action.                    |
| Gathering Evidence | Save proof (like screenshots) before deleting chats or posts. |
| Taking Action      | Block the user, report the issue, and inform a trusted adult. |
| Data Privacy       | Never share passwords, OTPs, or personal details.             |
| Digital Well-being | Practice healthy screen habits to protect your well-being.    |

## One line to remember

**Do not stay silent. Stop, save, block, and speak up.**