RAMANA VIDYALAYA

Parent Guide to Cyber Safety

CONTENTS

Introduction

Information and Communication Technology (ICT), brings great benefits to teaching and learning programmes. Ramana Vidyalaya places a high priority on equipping the school with internet facilities and ICT devices / equipment which will aid student learning outcomes.

A large percentage of parents these days use technology to keep their children busy. Kids receive their first internet-enabled device at an early age.

Technology is always changing and it's here to stay, but many are not aware of the potential risks of the cyber world. For a lot of children, the online world is more realistic than the real world. It then becomes crucial for our children's well-being that we are aware of what they see online, what is out there, both good and bad, and how it impacts their physical and emotional well-being.

Many of you might feel that you don't understand the new terms that kids use these days or that you don't have the technical skills to navigate the internet.

In this guide, we would like to outline areas that you should pay attention to as you and your children use the internet. Depending on the ages of your children, not all of it will apply to you. This can be treated as a set of guidelines to follow now, as well as to pay attention to, as children grow.

Smartphones and apps

Most children get their first smartphones at the age of 12–14 these days. A phone is an excellent safety tool; your child can use it to let you know he/she has reached the destination safely, call you for a ride, or in case of an emergency.

Smartphones, however, can also be misused, and in some situations, can make children vulnerable. Since smartphones are personal devices, we don't often know what our children do on them, or how they use them.

If you're considering giving your child a smartphone, it helps to have some clearly outlined guidelines in place beforehand. If your child already has a smartphone, it's not too late to review the rules. Demonstrate to the child that having a smartphone is a big responsibility.

Smartphone rules to implement:

- Always ask a parent before downloading a new app.

- Do not give your phone number to strangers or post it online.

- Tell a parent if you receive something on your phone that makes you feel uncomfortable.

- Do not answer a call or reply to a text message from an unknown number.

- Think about the messages and forwards you send. If you wouldn't say it in person, don't send it.

- Set limits on when and for what duration each day your child can use a smartphone.

- Insist that phones stay out of your child's bedroom and they aren't in use late at night.

Some ideas for parents:

- Have your child sign a "smartphone contract" (attached in this booklet), before you give him/her a smartphone. Print out a list of smartphone rules and stick it in a common place in your home.

- Set a personal example for your child. Don't bring your phone to the dinner table, don't text and drive, etc. If you would like to see a change in the behaviour of your child, ensure that you model the behaviour.

Video games and online games

Video games have long been a focus of fear and concern for many parents. With so many games featuring violent or sexual content, it is important to be careful about the kinds of games your children play. In addition, games that are entirely based online are open to abuse from other players.

Many games allow players from all over the world to chat with one another, potentially exposing kids to harassment and cyberbullying. Kids may also form relationships with other players and give away their personal information.

However, this doesn't mean that if a child really wants to play games, he/she should be discouraged. Games are also a great way for kids to develop a variety of skills. They help children develop problem-solving skills, learn how to commit to long-term goals, and how to work as part of a team. They can also be a great opportunity for family bonding.

If you truly want to use games as a way to improve a child's growth and learning, here's what you can do:

- Before buying a game from a store, check the "Age rating" given at the bottom of the box. The various ratings are: E (Everyone), T (Teen), M (Mature – 17+) and A (Adult). Always ensure that you do not buy games which have a M or an A rating.

- If your child has an online profile for a game, make sure the profile is set to private. Discourage them from using their full name or photo or sharing any other personal information for their profile.

- Teach your child to block players who send threatening or bullying messages.

Consider keeping all gaming devices / systems in a shared social space like the living room instead of the child's bedroom. This way you can see what your child is playing. You can also join! Playing games with your child can be a great bonding experience.

Social media

Social media consists of websites or apps that enable users to create and share content, and to participate in social networking. These sites and apps are constantly evolving and its important for parents/carers to stay updated about the platforms that are prevalent. Some of the most commonly used social media applications today are: Whatsapp, Twitter, Facebook, Instagram, Snapchat, YouTube, Tik Tok and Google+.

Social media can be particularly addictive for teens. It also opens the door to a variety of different issues, like cyberbullying, inappropriate sharing, and talking to strangers.

Access to social media is also central to teens' developing their identity. It's a way for children to connect with their friends. The key is to figure out some boundaries so that it remains a positive experience.

Safe rules for social media
- Discuss about the "pressure" to share: Kids constantly feel pressure to share details about their lives (they see others do it). Talk to them about the value of privacy to help relieve them of that pressure.

- Everything is permanent: Remind your kids that there is no such thing as deleting something on social media. Someone, somewhere, can retrace the information or photo that they post and use it against them someday. Knowing that whatever they post is permanent will encourage them to think twice about what they post.

- Educate them about online strangers: Predators use the internet to track and contact children. Teach your child to only accept friend requests from someone he or she knows.

How to enforce a safe environment

1. Don't let your children use social media until they reach the required age (13 – 14).

2. Keep the computer and other connected devices in a location where you can watch your child's activity.

3. Limit the amount of time your child spends on social media. Be very firm with enforcing this rule.

4. Insist that he/she blocks "location access" on all social media applications.

5. Monitor your child's online activity. Make sure the content he/she posts is harmless, and contains no identifiable information.

Viewing inappropriate content online
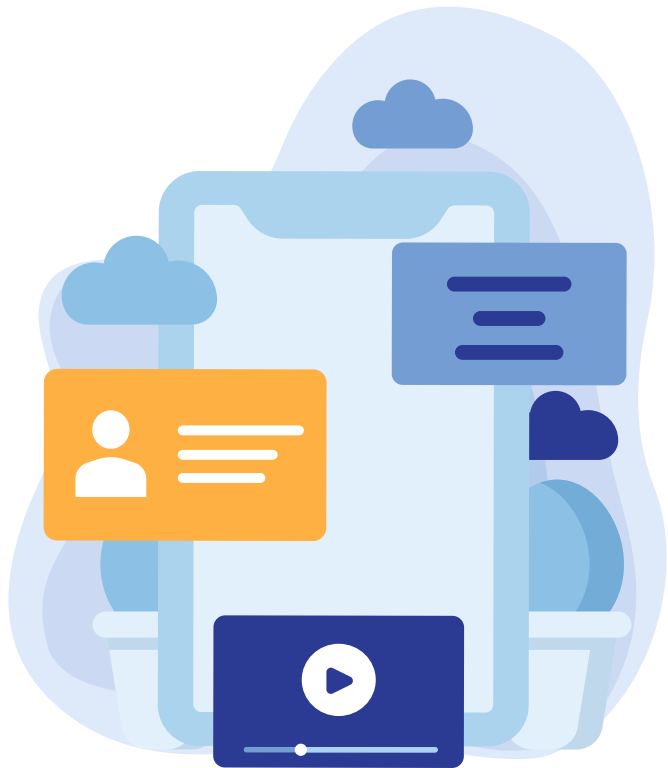
What is inappropriate content?

The internet is very open and public. It is also a place where kids can stumble upon content intended for adults; content which they may find upsetting, confusing or distressing. Movies and entertainment (TV shows, reality shows) are now readily and easily accessible due to the arrival of online streaming services such as Amazon Prime, Hotstar, Netflix, etc. These tend to portray a lot of violence, abuse and drugs. "Inappropriate content" can range from violent content, to sexual content like pornography.

How do children come across inappropriate content?

- They may have seen it by mistake.

- Someone might have sent it to them.

- They may have sought it out themselves, out of natural curiosity.

Why will children find it difficult to discuss inappropriate content?

- Many children don't go to their parents when they see something they perhaps shouldn't have seen, for fear that their parents will be angry with them, and take away their devices or internet access.

- If the content under discussion is sexual, your child will likely be embarrassed already as it is something new and out of the normal.

What to do if you know that your child has viewed inappropriate content?

- Respond calmly and be open to discussion.

- Let him/her know that you are ready to answer any questions without judgement.

- Be open and honest and answer any questions he/she may have.

Steps you can take to block inappropriate content:

- Set filters to block inappropriate content like pornography.

- Install an ad blocker to prevent viruses that might have inappropriate content.

- Please ensure you check the rating before allowing your children to watch a movie or TV show online.

Cyberbullying
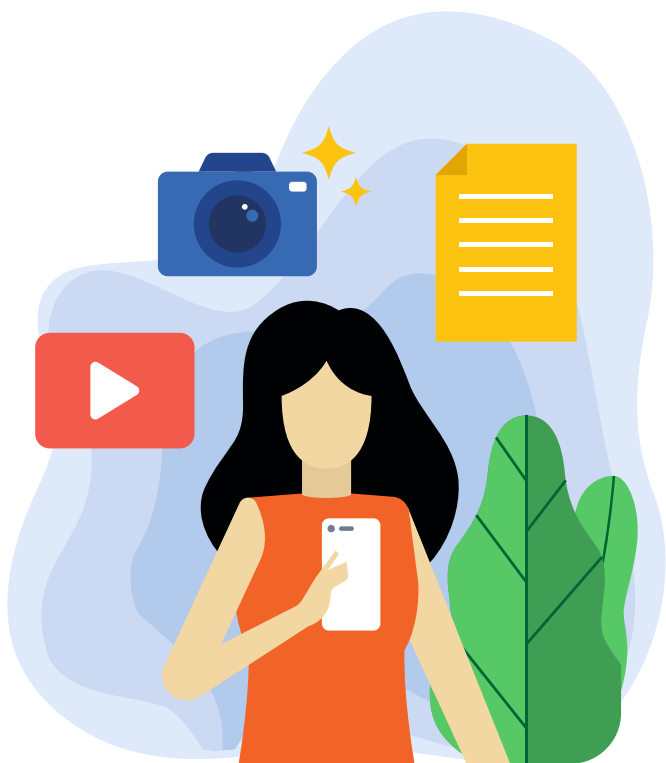
What is cyberbullying?

Cyberbullying is the use of online communication and devices to bully a person. It occurs across all of the platforms we have outlined above. Cyberbullying can occur by:

- Spreading rumours and sending threatening messages via social media, text, or email.

- Pretending to be another child and posting embarrassing material under his/her name.

- Forwarding private photos without consent.

- Posting online about another child with the intent to humiliate or degrade him/her.

Effects of cyberbullying

- Cyberbullying is particularly harmful because it is very public. A child's most private information can be splashed across the internet and is there permanently, unless reported and taken down.

- Cyberbullying can negatively affect the reputation of the victim and can have a deep impact on that child's future, including college admissions and employment.

- It is also extremely persistent. Digital platforms are constantly available and victims of cyberbullying struggle to find any relief.

Educate your child about cyberbullying

- Encourage your child to confide in you if his/her friends or peers are getting bullied.

- Educate your child about the repercussions of cyberbullying.

- Make it very clear that even "liking" or "sharing" harmful content is unacceptable.

Warning signs for cyber abuse

- A child who is bullied may shut down his/her social media account and open a new one.

- The child may begin to avoid social situations, even if he/she enjoyed being social in the past.

- Victims of cyberbullying often hide their screen or device when other people come into their vicinity and become cagey about what they do online.

- The child may become emotionally distressed or withdrawn.

E-mail and online transaction fraud

The internet can be used for payments & online transfers. Your children will eventually have their own bank accounts and it's essential that you educate them about online transfers.

Here are banking details that can be shared for transaction or verification purposes (after confirming that the receiver is authentic):

- Bank account name, number

- IFSC, name of the branch

- Credit/debit card number, card expiration details

Here are some banking details that should NEVER be shared with anyone over the phone, e-mail or in real life:

- Card Verification Value (CVV - the last three digits at the back of credit/debit card)

- ATM Personal Identification Number (PIN)

- One-Time Password (OTP)

- Account password/ transaction password

Even bank employees never ask for these confidential details. Anybody calling/ sending unknown links asking to upload these details is likely fraudulent. Encourage your children to exercise caution before sharing any banking details.

Parent-Child internet agreement

_____

Child's signature and date

_____

Parent's signature and date

General rules

- [ ] I will use the computer / smartphone only during the time that I have agreed upon with my parents.

- [ ] I will never give out or post personal information including my name, age, phone number, address, email, school name, extra curriculars, and where I practice or play.

- [ ] I will never give out my password or login information to anyone except my parents.

- [ ] I will never give out or post the personal information of my friends or family.

- [ ] I will never agree to meet anyone I have met on the internet in person, without informing my parents.

- [ ] If someone is making me feel uncomfortable or bullying me, I will tell my parents immediately.

- [ ] I will let my parents know before downloading any music, movies, games, or software.

- [ ] I will never steal or share copyrighted media.

- [ ] I will not install programs, software, or games without my parents' knowledge.

- [ ] I will not open email attachments or click on links in emails from unknown people.

- [ ] I will not click pop up ads and banners, but will close them by clicking on the browser window close button.

- [ ] I will not participate in contests or try to win free prizes on the internet without asking my parents first.

We highly encourage you to sign an internet agreement with your child. This is both healthy and does not intrude on your child's privacy in a negative manner. Once you've signed the internet contract with your child, we wish you and your child a happy and safe cyber experience!
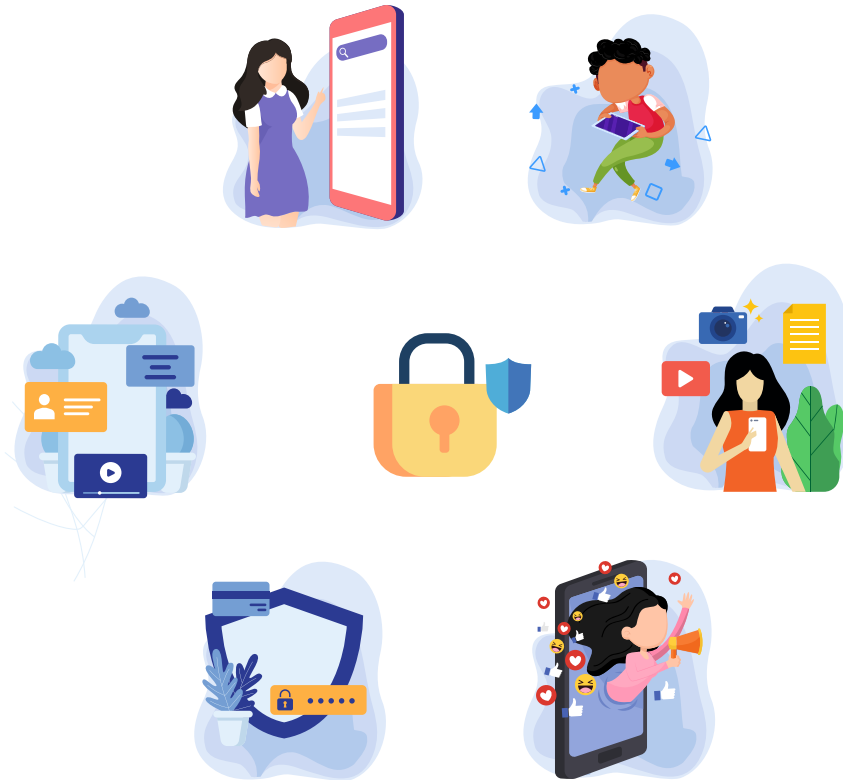
Cyber safety at Ramana Vidyalaya

- Ramana Vidyalaya conducts structured cyber safety sessions for students from Grades 9 to 12, and follows a computer science curriculum integrated with digital citizenship from Grade 8. To know more about this, you can visit www.commonsense.org.
- The Child Protection Policy followed by the staff (teaching and non-teaching) at the school includes a cyber code of conduct which outlines do's and don'ts of internet exposure and social media for the staff with respect to the online privacy and safety of students.

What to do if your child is bullied online?

Step 1 : Ramana Vidyalaya provides guidance in cases of cyberbullying. Don't hesitate to get in touch with us at principal@ramanaschool.com

Step 2 : Help us with whatever information and evidence you have regarding the abuse of the child.

Step 3 : Maintain privacy to ensure the complete safety of the child.

RAMANA VIDYALAYA

#371, MGR ROAD, SHOLINGANALLUR, CHENNAI – 600119

Ph. No. : +91-44-2450-1405, Email : info@ramanaschool.com