CHILD SAFETY ONLINE (CSO)

INTERNET AND SOCIAL MEDIA

Internet and Social Media sites are very **ADDICTIVE** and hugely **POPULAR** among youths. They have many risks of **PRIVACY** and other cyber securities where one has to be very **CAREFUL** about using and understanding their **PURPOSE**.

One has to understand that these sites are developed for **COMMERCIA**L purpose with the intention of **REVENUE** generation.

These factors may look cool but they are the basic **THREATS.**

ALWAYS understand what looks and feel real in internet may not be TRUE.

Internet is just a medium of **COMMUNICATION** it is part of our lifestyle but not our **LIFE.**

INTERNET CORE VALUES FOR CHILDREN

1. Internet is a means of **COMMUNICATION & LEARNING**
2. Internet should be used under **SUPERVISION** of adults only
3. **STOP** endorsing and acknowledging anyone or anything that you **DO NOT KNOW**
4. Be **FOCUSED** when you use the Internet
5. If there is any problem or issues **ALWAYS TALK** with your parents or guardian
6. Access or being sexually explicit, racist, violent, extremist or other harmful material, either through choice or in error is **ALWAYS WRONG**
7. **STOP USING** Spyware, Viruses and Malware for any purpose in your computer, smartphone, tablet or games console
8. Always **RESPECT** your parents **TOLERANCE**

Risks or Vulnerabilities of Children Online

- Curiosity and incline of children towards **violent, sexual and pornographic content**
- Understanding the validating process of **inaccurate or false information and extreme views**
- Dealing and facing issues of **harmful behaviors including self-harm, anorexia and suicide**
- Being more lively and public by **sharing personal information online**
- Actively or unintentionally getting **involved in bullying or hurtful behavior**

Current evolving issues and problems:

Issues and problems	Indicators
Online Gaming	➢ Addiction and long-term use causes physical abnormalities ➢ Cause increase in Aggression, restlessness and/or irritability ➢ Isolation and the child becomes dulls ➢ Migraines due to intense concentration or eye strain ➢ Carpal tunnel syndrome caused by the overuse of a controller or computer mouse
Mobile Applications	➢ Screen Addiction ➢ Impulsive behavior ➢ Eyes straining ➢ Limited thinking no creativity
Virus and Spyware	➢ Opening infected email attachments such as .exe files. ➢ Opening infected files from web-based digital file delivery companies (for example Hightail - formerly called YouSendIt, and Dropbox). ➢ Visiting corrupt websites. ➢ Via the internet, undetected by the user (worms are an example of this). ➢ Macros in application documents (word processing, spreadsheets etc).

	➢ USB connected devices (eg memory sticks, external hard drives, MP3 players). ➢ CDs/DVDs **Viruses and spyware can cause very serious consequences including:** ➢ Identity theft ➢ Fraud ➢ Deletion, theft and corruption of data ➢ A slow or unusable computer
Spam and Scam emails	➢ Free and easy Advertising, for example online pharmacies, pornography, dating, gambling ➢ Easy and quick links of exciting offers and getting rich quick and work from home schemes ➢ Scanning option of Hoax virus warnings. ➢ Appeals of Hoax charity and serving humanity ➢ Good luck emails of forwarding it to your contacts often to bring 'good luck' ➢ Use of Free webmail address or sent from a completely different address ➢ The email may not use your proper name, but a non-specific greeting such as "Dear customer." ➢ A sense of urgency; for example the threat that unless you act

	immediately your account may be closed. ➢ A prominent website link. These can be forged or seem very similar to the proper address, but even a single character’s difference means a different website ➢ A request for personal information such as username, password or bank details. ➢ You weren't expecting to get an email from the organization that appears to have sent it. ➢ The entire text of the email may be contained within an image rather than the usual text format. The image contains an embedded link to a bogus site ➢ Use email safely ➢ Do not open emails which you suspect as being scams. ➢ Do not forward emails which you suspect as being scams. ➢ Do not open attachments from unknown sources.
	There wide range of downloadable music, videos, software and documents. One has to Find out how your child can benefit from these legally and without risking becoming a victim of grooming, bullying, identity theft or viruses.

Downloading and file sharing	➢ viruses – downloading files or software can put computers at risk from potentially harmful programs ➢ theft – file sharing can allow other computers to view all the files on your computer, which means that your personal information might be stolen ➢ unsuitable images – if your child is using an illegal download site they could be exposed to pornographic, violent or age-inappropriate content ➢ exposure to potentially dangerous strangers – it's possible to chat on some file sharing sites, which could leave your child open to grooming, bullying and abuse
Hate content	Hate content are easy spread and can easy victimized children who have no understand of the issues and human rights values. Digital Literacy skills is something that always requires updates : ➢ The Other: The most basic element of hate is the idea of "the Other" – a group that is seen as being completely different from the author's group, sometimes even portrayed as inhuman. ➢ The Glorious Past: Another important element of hate is the idea that the group has fallen from its once-glorious past. This fall is shown as being the fault of the Other, and it is only by defeating

	and destroying the Other that this glorious past can be regained. ➢ Victimhood: Hate groups typically portray themselves, and the group they claim to represent, as victims of the Other.
Privacy and Identity Theft	Children may be at risk of having their online identity stolen and misused. It can be difficult to maintain a child's privacy as they may not understand what information is safe to share online, or what default privacy settings are on the sites and devices they're using. The internet offers access to a world of products and services, entertainment and information. At the same time, it creates opportunities for scammers, hackers, and identity thieves. Learn how to protect your computer, your information, and your online files.
Cyberstalking	Cyberstalking can be defined as using Internet, emails, social networking sites and other technology to stalk, harass or intimidate a victim which can cause mental distress, anguish and even trauma to the victim. Cyberstalking can be direct or indirect. Direct cyberstalking includes sending threatening or obscene emails, messages or voice mails. Indirect cyberstalking

	involves impersonating the victim, spreading rumors about them or using Internet to post hate/obscene messages about them. A cyber stalker might just follow a person from one social media account to another, persistently messaging them, commenting on or liking all their status. Why Parents need to be cautious about Cyberstalking
Cyberbullying	Cyberbullying is bullying that takes place over digital devices like cell phones, computers, and tablets. Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyberbullying crosses the line into unlawful or criminal behavior. The most common places where cyberbullying occurs are: ➢ Social Media, such as Facebook, Instagram, Snapchat, and Twitter

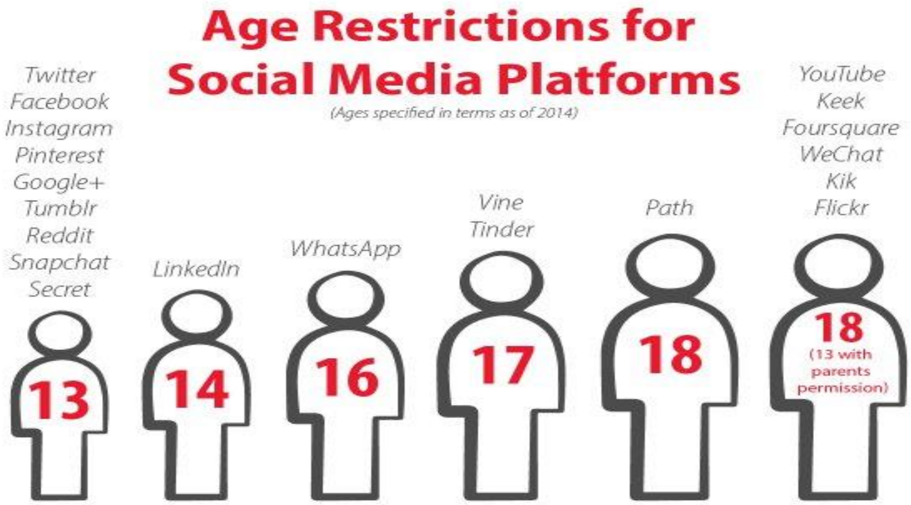
	➢ SMS (Short Message Service) also known as Text Message sent through devices ➢ Instant Message (via devices, email provider services, apps, and social media messaging features) ➢ Email
Texting and Sexting	Texting is currently one of the most instant forms of communication. While texting might be the perfect platform to say a quick "hi," there are some things to watch out for in a textual relationship with your partner. Sexting is sending sexually explicit text or photographs via mobile devices. Sometimes teens share the photographs voluntarily, but at other times teens may be coerced into taking or sending the photographs. Once the photos are sent, some kids use them to bully, harass, intimidate, or embarrass victims online or via mobile devices. Sexting between minors is a felony and can have serious legal consequences. You could be charged with a crime. If convicted you could be labeled as a sex offender for the rest of your life. Think before you "sext." Never send or post sexually provocative pictures. Once the picture is out there, it will never go away.

Online Abuse and Harassment

Online abuse is any type of abuse that happens on the web, whether through social networks, playing online games or using mobile phones. Children and young people may experience cyberbullying, grooming, sexual abuse, sexual exploitation or emotional abuse.

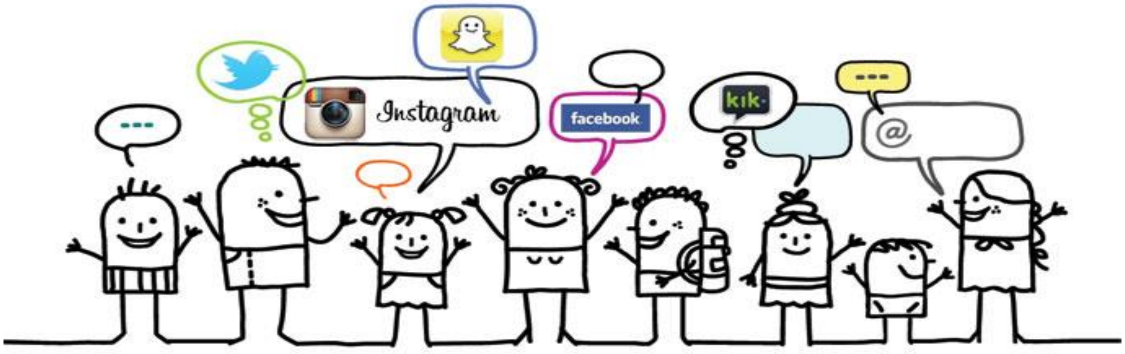
Parents tools and option available

- Educate and update yourself about the issues and problems about child online safety
- Parental Control software
- Firewall
- Antivirus
- Talking more about Safe internet browsing



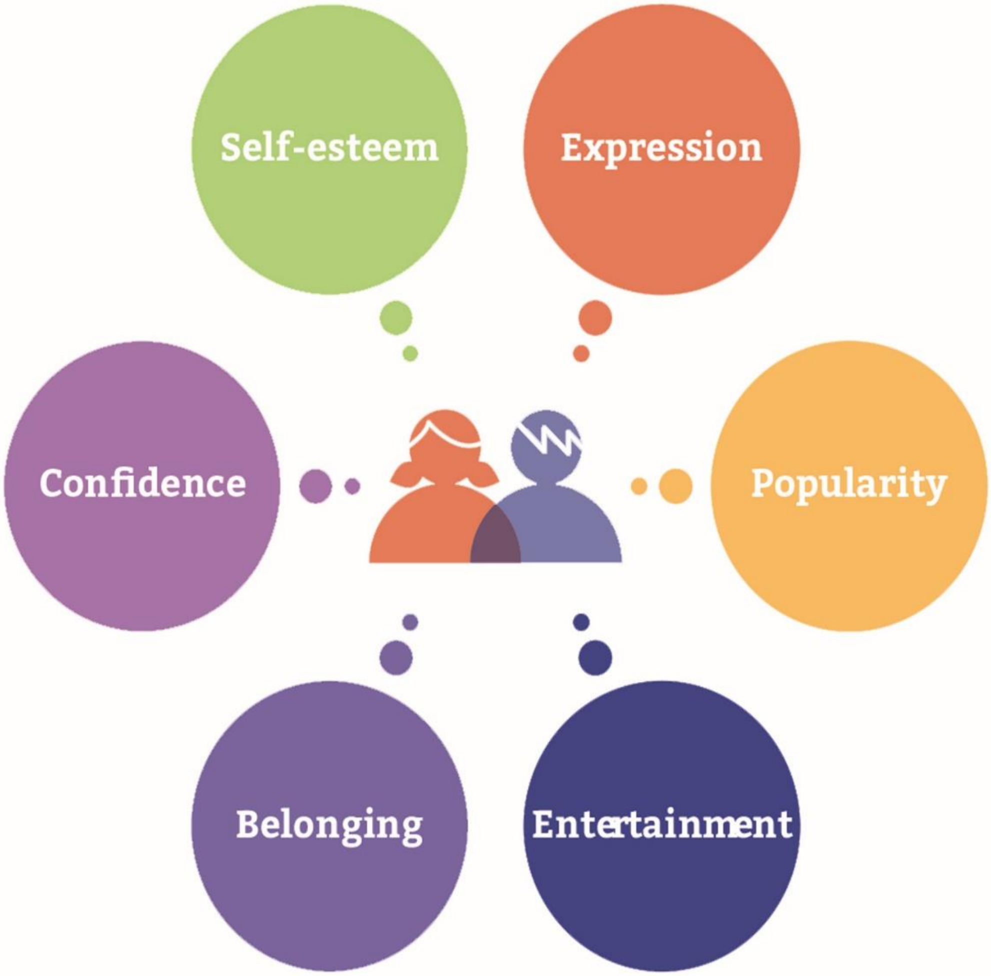
Primitive Measure

- Apart from installing internet security software and keeping it updated, we recommend a number of other ways in which to keep your computer protected against viruses and spyware. After all, prevention is better than cure.
- Email from an unknown, suspicious or untrustworthy source should not be open
- Before installing an antivirus always check and make sure there is no other antivirus installed
- Always scan the USB devices and be careful with USB connected devices (eg memory sticks, external hard drives, MP3 players) as they are common carriers of viruses and malwares
- Always check and be careful with CDs/DVDs
- Do not open any files from web-based digital file delivery companies (eg YouSendIt, Dropbox) that have been uploaded from an unknown, suspicious or untrustworthy source
- Switch on macro protection in Microsoft Office applications like Word and Excel.
- Always buy registered copies of software, do not use pirated software
- Downloading free software can be great threat so be careful while downloading



Mentality and Strategies

Age Group	Values	Strategy
0-5	**Integration of Internet values**	✓ Developing the Concepts and values of internet ✓ Bonding and sharing with children ✓ Creating better communication strategy ✓ Priority and preference use of internet
6-12	**Curiosity**	✓ Concept of safe browsing ✓ Concept of human rights ✓ Threats of cyber bullying ✓ Social media and intervention (Parental Software and watch a must)
12 and above	**Addiction and Carelessness**	✓ Listern to what they have to say ✓ Talk with them more about current issues of cybers securities and issues ✓ Spent more time ✓ Make rules of using internet and home discipline ✓ Family time ✓ Try to be a friend



Source: UKCISS

Things to remember 0-5 years

- Always make a point of giving your children access to internet for learning purpose only and set a limits for the amount of time they can spend on the computer
- Devices like mobile, tablet or laptop should not be easily access to children. Always keep your devices passwords/PINs protected for unauthorized use
- Set parental controls on computers and any other devices your child has access to enabling access to only appropriate content
- Always buy or download only apps, games, online TV and films which have age ratings, which you should check before allowing your child to play with or watch them
- Discipline should be maintain in technology rules as children learn from parents so first parents have to live by example
- While using internet in public place always check what your child is accessing or looking at, always keep a watch when you are in public wifi zone and how your child is reacting to the free service

Things to remember 6- 12 years

- Set the parental controls to the appropriate age, and enabling access to only appropriate content on computers and any other devices your child has access to
- Update your parental control software and switch it on at all times
- Build a discipline in terms of when where and how to use internet and other communication medium. Time setting can really help them for activities such as using the internet and games consoles
- Allow only age-appropriate content by checking out the age ratings on games, online TV, films and apps
- Keep the Internet discipline with all member in the family discuss with your older children what they should or shouldn't be showing their younger siblings on the internet, mobile devices, games consoles and other devices
- Don't be pressured by your child into letting them use certain technologies or view certain online content, if you don't think they are old enough or mature enough, no matter how much they pester you or what their friends' parents allow
- Give your child a lesson of privacy and how important it is to keep phones and other devices secure
- Discuss with your child what is safe and appropriate to post and share online. Written comments, photos and videos all form part of their 'digital footprint' and could be seen by anyone and available on the internet forever, even if it is subsequently deleted
- Talk with your child about the kind of content they see online. They might be looking for information about their changing bodies and exploring relationships. They also need to

understand the importance of not sending other people - whoever they are - pictures of themselves naked

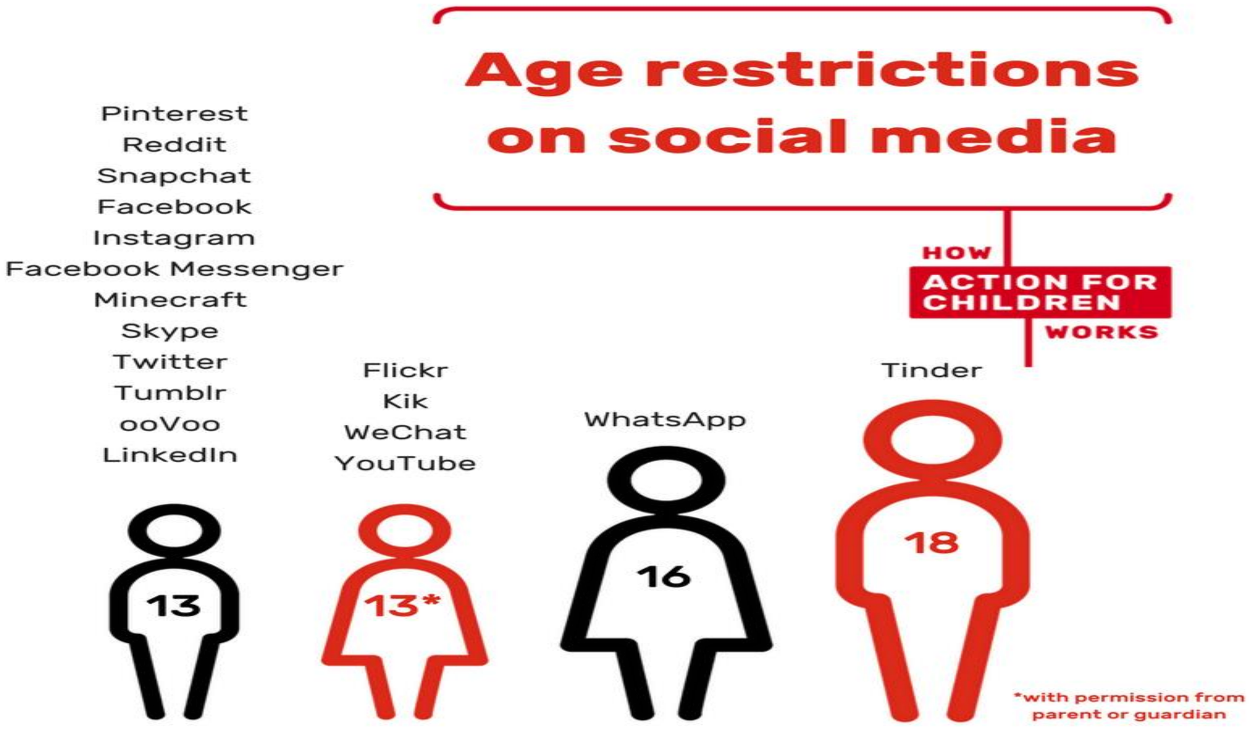
- Always ask them to respect the rules and regulation in terms of age restriction and limitation and remember that services like Facebook and YouTube have a minimum age limit of 13 for a reason
- Be sure to make them understand that being online doesn't give them anonymity or protection, and that they shouldn't do anything online that they wouldn't do face-to-face

Things to remember 13 and above

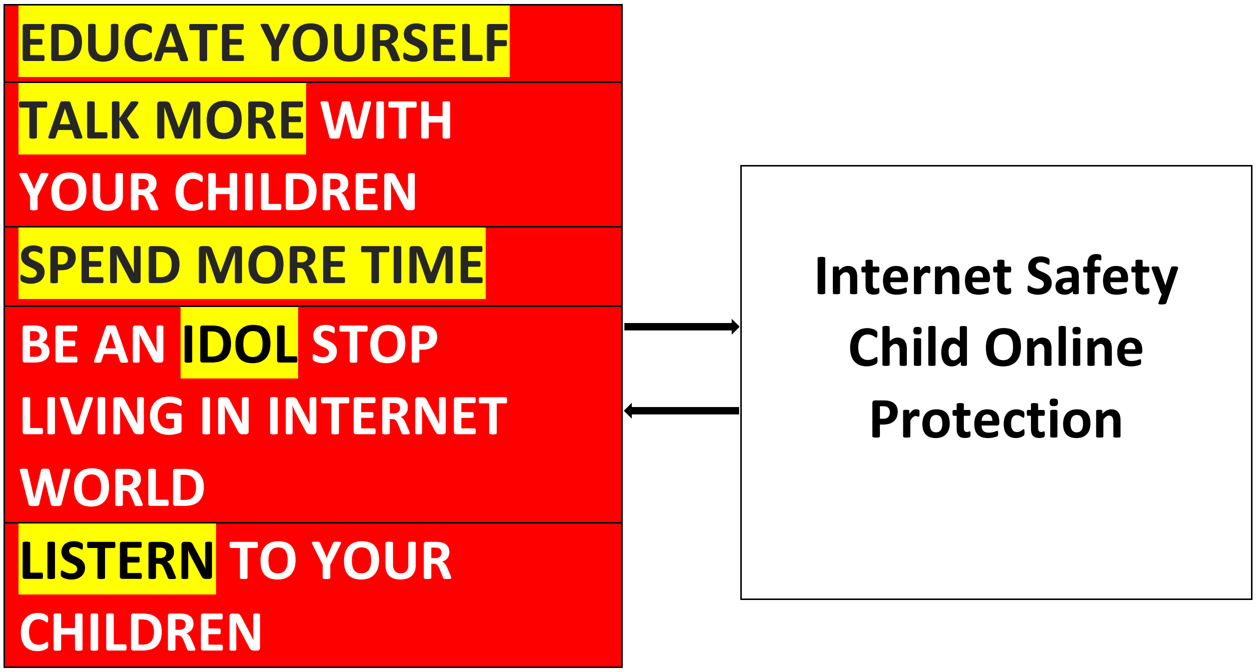
- Your child is in his or her teens It's never too late to reinforce boundaries though there might be a resistance that they may think they are adult enough, but they definitely still need your wisdom and guidance
- At this age Technology and internet may seem and sound easy but always make it your business to keep up to date and discuss what you know with your child
- This is the times where parents need to do some homework your child may be curious about health, wellbeing, body image and sexuality of themselves and others online. They may be discovering inaccurate or dangerous information on online at what is a vulnerable time in their lives so parents have to be very watchful and prompt
- Always Review the settings on parental controls with age of your child. They may ask you to trust them sufficiently to turn them

off completely, but think carefully before you do and agree in advance what is acceptable online behavior

- Have small talk session about bullying, and posting hurtful, misleading or untrue comments how they behave towards others. Make them aware of the dangers of behaviors like sexting and inappropriate use of webcams
- Don’t give them access to your payment card or other financial details.
- Be clear about copyrighted material and plagiarism so that you make a point about what is legal and what is illegal



THE MATRIX



EDUCATE YOURSELF

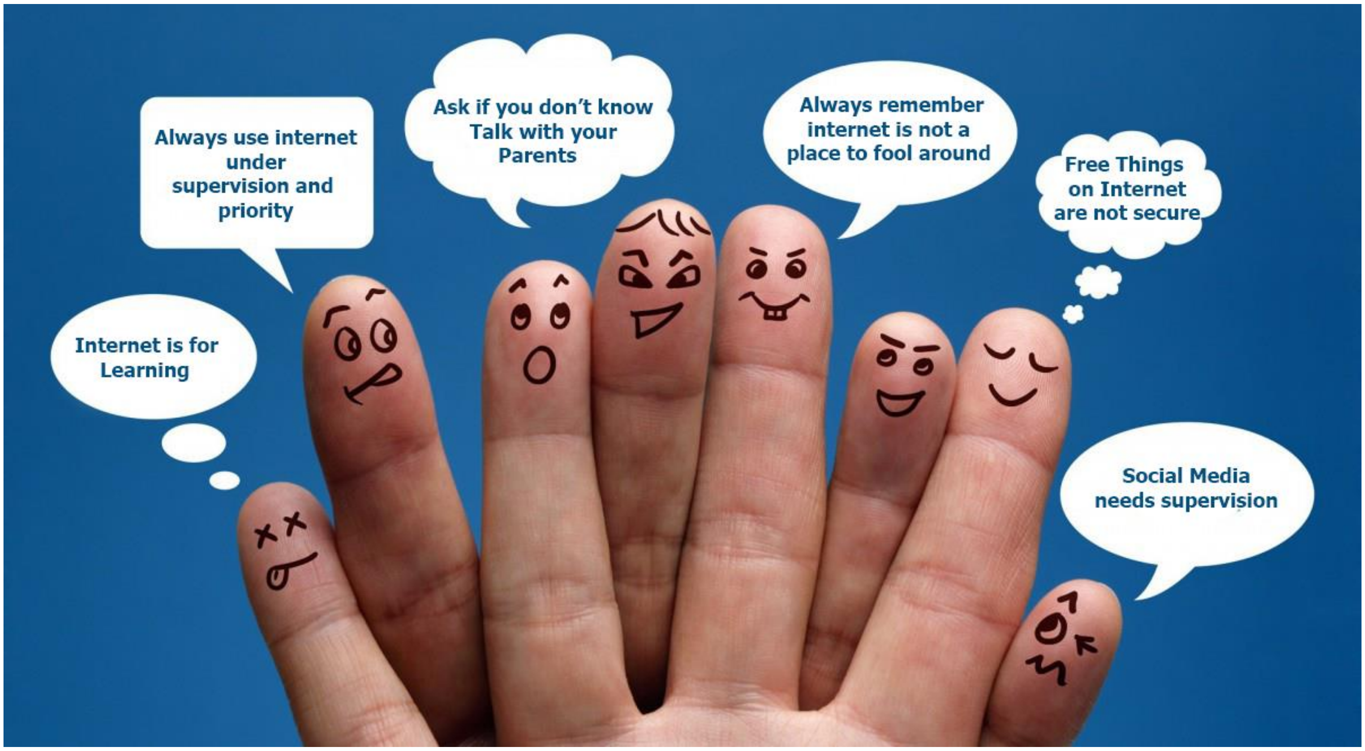
TALK MORE WITH YOUR CHILDREN

SPEND MORE TIME

BE AN IDOL STOP LIVING IN INTERNET WORLD

LISTERN TO YOUR CHILDREN

Internet Safety
Child Online
Protection


Internet is for Learning
Always use internet under supervision and priority
Ask if you don't know Talk with your Parents
Always remember internet is not a place to fool around
Free Things on Internet are not secure
Social Media needs supervision

Information about the Researcher

Shreedeep Rayamajhi

Link: https://en.wikipedia.org/wiki/Shreedeep_Rayamajhi

Email: shreedeep@rayZnews.com

Website: http://www.rayznews.com

Adv. Sajina Karki

Link: https://en.wikipedia.org/wiki/Sajina_Karki

Website: https://learninternetgovernance.blogspot.com/