Guidelines for Children's Safety Online

Here are some guidelines that you can implement to ensure children's safety online on the distributed tablets, smartphones, laptops etc. These guidelines cover software solution and awareness guidelines for parents and students.

A) Software Solution

You can install the below-mentioned software on the devices of children to ensure online safety. Given below is a list of software (both free and subscription-based) that can be installed.

A.1 Here is a list of free software that you can use

1. Google Family Link(laptops/desktop/tablets/smartphones)

Google Family Link is a family parental controls service by Google that allows parents to adjust parameters for their children's devices. Google Family Link requires Google accounts in order to access the app remotely. It is a free parental control service that can be easily downloaded from the play store. Watch this video to understand how to set up a Google family link on your child's device.

Features-

- → Control over apps
- → Set screen time limits
- → Review and control your child's access to microphone, camera, location and contacts
- → Control search options (Google Safe Search is on by default) and limit the websites your child can visit in Google's Chrome browser with the option to 1) allow all sites, 2) try to block mature sites (default), or 3) only allow for certain sites on a list you approve
- → Manage purchases and downloads on Google Play store
- → Set limits on app use based on ratings from the Entertainment Software Rating Board

2. Microsoft Family Safety(laptops/desktop/ tablets/smartphones)

Microsoft Family Safety is a free set of features available on Windows 10 PC and Mobile that is bundled with the Windows 10 operating system. It is a free service offered by Microsoft that can be easily downloaded from the play store. Watch this videoto understand how to set up Microsoft Family Safety on your child's device.

Features-

- → Set screen time limits
- → Filter content to ensure access to age-appropriate content
- → Access to kids' weekly activity across all of their apps, games, and devices
- → Location awareness feature

→ Limits browsing to kid-friendly websites using Microsoft Edge on Xbox, Windows, and Android

3. Kidslox(laptops/desktop/tablets/smartphones)

Kidslox parental control app makes it simple to manage children's screen time and helps them develop a balanced attitude to technology. It gives you tools to block apps, block internet and filter web content. The basic version of Kidslox is free and can be downloaded from the Play store. Watch this video to understand how Kidslox works.

Features-

→ Set daily screen time limits. Block all 3rd party apps, individually or by category
→ Switch between unrestricted 'Parent mode', custom 'Child mode' and fully restricted 'Lockdown mode' at the touch of a button
→ Filter pornography and other adult content to give your child a safe browser experience
→ Stop your clever kids from changing the restrictions with a unique Kidslox PIN and childproofing tools

A.2 Here are some quick tips on enabling child safety settings on frequently used apps

- **Google Chrome**

Safe Search is a feature in Google Search and Google Images that acts as an automated filter of pornography and potentially offensive and inappropriate content. Watch this video to understand how to enable Google SafeSearch. Steps to enable Google safe on android and computer can be found here .

- **YouTube**

YouTube parental controls can be used by parents to make sure the child only watches appropriate videos. On a web browser, parents can enable YouTube Restricted Mode (Steps), which hides mature content. They can also download the YouTube Kids app and allow pre-approved content or block specific videos. Watch this video to understand how to turn on YouTube's parental control feature.

- **Instagram**

Instagram has a number of functions to help a child manage who can see their content and how they interact with others. They can also use the reporting function to flag content that breaks community guidelines and upsets them. This website lists the steps that can be taken on Instagram to filter, block, and report harmful content on Instagram. Watch this video to understand Instagram privacy & safety settings guide.

- **Facebook**

Watch this video to understand how to enable privacy settings on Facebook. The article lists the steps that can be taken to stay safe on Facebook.

A.3 These are a few subscription-based software that you can use

1. Qustodio(laptops/desktop/tablets/smartphones)

Useful in filtering content, applications, and monitoring the activity (Subscription-based software). Qustodio offers many plans starting from Rs. 172.5/month for 5 devices. It also has special plans designed for schools and offers a free trial for the same. Watch this video to see how to install Qustodio on your child's device.

Features-

→ Filter content and apps by blocking inappropriate apps, games and websites.
→ Monitoring Activity
→ Setting time limits to avoid scree addiction
→ Tracking calls and SMS
→ Locating family members
→ Reports, alerts and SOS

2. Kaspersky Safe Kids(laptops/desktop/tablets/smartphones)

Protect your kids online and offline with award-winning parental controls. Get flexible tools that help you safeguard their activities, monitor their behaviour and teach them self-control. Watch this video to see how to install Kaspersky Safe Kids.

Features-

→ Block access to inappropriate or harmful content
→ Set screen time limits per child, per device
→ Track your kids' location with GPS

3. Norton Family ((laptops/desktop/tablets/smartphones)

Norton Family provides insights that help parents foster a healthy life balance for their children and their devices, while providing tools to help them teach safe, smart, and healthy online habits. Watch this video to see how to install Norton Family.

Features-

- → Web, Time and Search supervision
- → Mobile app supervision
- → Location supervision
- → Reports of child’s online activity
- → Email alerts when child visits a blocked site

4. Seqrite Endpoint Security

Seqrite endpoint security is a simple and comprehensive platform which integrates innovative technologies like Anti Ransomware, Advance DNA Scan, Behavioural detection system to protect your network from today’s advanced threats. Watch this video to understand how Seqrite works.

Features

- → Advanced device control
- → Web Filtering (websites can be blocked to limit web access)
- → Ransomware Protection
- → Application control (to enforce control over the use of unauthorised applications)
- → Vulnerability scan

B) Awareness and Education on Child Safety

You can also educate children and parents on the risks of unsafe browsing and share tips to ensuring online safety in the following ways.

1. Create awareness about various forms of online abuse and ways to ensure online safety for children with beneficiary students. Guidelines for students are attached in Annexure 1. Please translate them into regional languages and share with the children who are using the devices.
2. Workshops can be organized for parents to teach them about various platforms offering online safety services. Guidelines for parents are attached in Annexure 2. Please translate them into regional languages and share with parents of children who are using the devices.
3. Events can be organized for students by collaborating with various organizations working on online safety. Here are a few organisations you can contact:
    a. Social Media Matters
    b. Data Security Council of India (DSCI) (Stay Cyber Safe Initiative)

Annexure 1: Guidelines for Students

Please share these guidelines through Whatsapp, email and other social media, or print them out and circulate these among your student community.

Dos:

1. Inform your parent or guardian if you find any message or information online that is threatening, obscene, or makes you uncomfortable in any way.
2. Respect the privacy of other internet users just like you expect your privacy to be respected.
3. Enable reading mode in your devices to make it optimised for reading.
4. Be very careful while downloading content from the internet. Ensure that you have a virus scan application installed on your device.
5. Install antivirus software on your devices (tablets, laptops, PCs) for security. Some free antivirus software are- AvastMcAfee (30 days free), AVG Antivirus,Bull Guard
6. Use the internet wisely as an aid to your studies.
7. Use kid-friendly search engines like- Kiddle, Kidtopiato search course-related material.
8. Inform your parents if a stranger sends you a message, calls, or tries to bully you. Block them immediately.
9. Keep strong passwords as they are important to keep your data secure. Enable two-step verification whenever possible.
10. Enable the Safe search option, while using Google, Yahoo, or any other search engine.
11. Be very cautious of fake news, cross-check a news piece before forwarding it to your classmates and teachers.

Don’ts:

1. Do not share identifying information like Name, Home Address, Contact Number in a public message. Send it privately to the concerned person.
2. Do not spend a lot of time in front of devices, as it can be harmful for your eyes.
3. Do not share your personal information like Name, Home Address, contact number,credit card information, etc with strangers.
4. Do not send a picture of yourself to anyone without informing your parents or guardian.
5. Do not arrange physical meetings/face-to-face meetings with your online friends without informing your parents, because people online may not be who they seem.
6. Do not talk to strangers on the internet or reply to their messages.
7. Do not open unnecessary links shared by strangers.
8. Do not click on pop-upads that you encounter on different websites. Clickbaitads can be dangerous.
9. Do not share your password with anyone orsave your passwords onanother person’s device.

10. Do not share a lot of personal information on social media platforms like Instagram, Facebook, WhatsApp, Snapchat, etc,
11. Do not share information on the internet that could hurt others.

Code of Conduct for Conference platforms (for online classes)

1. The students should keep their videos and audio off during the class.
2. Students should be on mute unless asked by the teacher to unmute. Use the raise hand option to ask questions or share your thoughts.
3. If the students have any doubts, the students should write their doubts in the chat box when asked or required by the teacher.
4. Do not write irrelevant text in the chat box. Do not engage in verbal abuse or bullying activity.
5. The students should not ask for the phone numbers of the teachers.

Annexure 2: Guidelines for Parents

Please share these guidelines through WhatAapp, email and other social media, or print them out and share these with parents.

Do's:

1. Encourage your child to come to you to discuss, if they come across something online that makes them feel uncomfortable
2. Teach your child the basics of internet safety like privacy settings, blocking strangers, and reporting offensive comments/content.
3. Ensure that the location sharing feature for the apps is turned off, to ensure the location of the child is not shared unintentionally.
4. Talk to your child about personal information sharing on social media platforms, and monitor their social media time usage.
5. Discuss with the child about risks associated with meeting strangers in person (offline).
6. Do engage with the child to find out what activitiesor websites interest them on the internet.
7. Enable safe search for the search engine used by the child. (Example- Google Safe Search)
8. Educate the child about various laws relating to online safety in the country. (App- https://www.childprotectionindia.com/about-app.php)
9. Set Parental Control for the devices used by the child, to filter out harmful content. (Example- Google Family Link)
10. Discuss with the kids' various forms of online abuse like stalking, hateful speech, hacking, online impersonation, etc.

Don'ts:

1. Do not be very critical about the child's exploration of the internet.
2. Do not scold your child if they get in some trouble online.