Advisory to Parents and Teachers on Children's Safe Online Gaming

Don'ts:

- Do not allow in-game purchases without parental consent. To avoid in app purchases, OTP based payment methods may be adopted as per RBI's guidelines.
- Avoid credit/debit cards registration on apps for subscriptions. Place an upper limit on expenditure per transaction.
- Do not let children buy directly from the laptop or mobile they use for gaming.
- Advise children not to download software and games from unknown websites.
- Tell them to be beware of clicking links, images and pop-ups in the websites as they may contain a virus and harm the computer, and may contain age-inappropriate content.
- Advise them not to give personal information over the Internet while downloading games.
- They should never share personal information with people in games and on gaming profile.
- Advise them not to communicate with strangers, including adults, through web cam, private messaging or online chat, as it increases the risk of contact from online abusers, or bullying from other players.
- Advise them against engaging in game for long hours without taking a break considering health aspects and addiction.

Do's:

- While playing online games, if something wrong happened, stop immediately and take a screenshot (using the "print screen" button on the keyboard) and report it.
- Help your child to protect their privacy online, get them to use a screen name (avatar) that does not reveal their real name.
- Use antivirus/spyware programs and configure web browsers securely using firewall.
- Activate parental controls and safety features on the device or in the app or browser as it helps restrict access to certain content and limit spending on in-game purchases.
- Notify if a stranger tries to start a conversation about something inappropriate or requests personal information.
- Check the age rating of any games your child is playing.
- In case of a bullying, encourage not to respond and keep a record of the harassing messages and report the behaviour to the game site administrator/block, mute or 'unfriend' that person from their players list, or turn off the in-game chat function.
- Play alongside your child to get a better sense of how they are handling their personal information and who they are communicating with.
- Help your child understand that some features in online games are used to encourage more play and spending. Talk to them about gambling, what it is and its consequences both online and in the physical world.
- Always ensure that your child accesses internet from a computer placed in the family space.
- Keep your eyes open for:
  - Unusually secretive behaviour, mostly related to their online activity
  - A sudden increase in the time they spend online, especially social media
  - They seem to change screens on their device when approached
  - They become withdrawn or angry, after using the internet or sending text messages
  - Their device suddenly has many new phone numbers and email contacts.
- Install internet gateway at home which has features like monitoring, logging and controlling the types of content that the children can access.
- Teachers need to keep an eye on falling grades and social behaviour of the students.
- If teachers observe something that may seem suspicious or alarming, they should inform the school authorities immediately.
- Teachers should ensure that children are sensitized about the pros and cons of the internet from time to time.
- Teachers should train students for secure configuration of web browsers & web applications.

TO REPORT ANY UNTOWARD INCIDENT, USE THE FOLLOWING LINKS:

National Helpline- https://cybercrime.gov.in/Webform/Helpline.aspx
Statewise Nodal Officers- https://cybercrime.gov.in/Webform/Crime_NodalGrivanceList.aspx

****