Privacy & Protection Guidelines for Internet Access by Children

Idea Cellular believes in the concept of free internet and is committed to providing access to the world of internet, to our customers. We believe that information and communication technology has created unprecedented opportunities for citizens, particularly children and the youth, by enabling them to communicate, connect, share, learn, access information and express.

While the company is a strong proponent of easy access to the world of information on the internet, we are equally cognizant of the challenges posed by the availability of objectionable content and privacy risks which can pose a threat to child safety.

We strongly recommend caution and parental guidance for children/teenagers when they access information from the internet. We also strongly recommend parents and guardians to spend time and to participate in and monitor their online activity. Here are a few tips to ensure secure access to the internet, especially for children.

- Undertake all safety measures for secure use of internet and deploy parental control tools on computers and mobile devices; privacy features on social networking sites; and activate safety options on Google, Facebook and other search engines and social networking platforms.

- Encourage discussion on digital issues with your children; demonstrate to them the importance and need for technology and information and its benefits; explain and encourage responsible online behavior among them and make them aware about issues such as bullying and pornography and anything else that may be harmful for them.

- Monitor your children's interest areas while surfing on the internet and set guidelines on what can be viewed/accessed/downloaded.

- Keep websites and applications password protected, if you don't wish those to be accessed by children.

- Let your children not befriend strangers.

- Educate your children to not reveal personal information like name, address, date of birth, passport number, Aadhaar number, credit card details, telephone numbers, school details, family members' names and contacts, location details etc. on social networking sites.

- Make your children aware about 'block' and 'unfriend' tools on social networking sites, for them to avoid contact with any stranger, and ensure that they immediately bring any such occurrence to your notice.

- Caution children from sharing their personal photographs and videos in open platforms which can be viewed publicly.

- Sensitize children about age appropriate content on the internet.

- Educate your children to report child online exploitation and abuse on "Child Helpline – 1098" notified by the Government of India.

General Caution:

Every customer accessing the internet should be aware of the legal implications of misuse of the service. The following activities on internet are treated as cyber-crimes:

- **Cyber stalking –** where someone is repeatedly and persistently followed and pursued online by email or other electronic means or communication.
- **Cyber bullying –** where someone emotionally harasses, embarrasses, defames, or intimidates of social exclusion, taunts, insults or uses threatening behaviour by using internet, email or other electronic means or communication.
- **Unwanted exposure to sexually explicit material etc –** where someone sends pictures, videos, sound clips, cartoons or animations depicting sexual content by e-mail or any another electronic means
- **Child pornography –** where someone captures/displays/sends images or videos of child/children (below 18 years) in an obscene or indecent (i.e. sexually explicit) manner or where someone represents by whatever means of a child engaged in real or simulated explicit sexual parts of a child, the dominant characteristics of which is depiction for a sexual purpose.
- **Pornography –** where someone captures/displays/sends images or videos of the private body parts of any person without his/her consent.
- **Hacking –** where someone accesses or uses the computer/laptop/mobile or email or social sites' accounts of another person without authorization/consent of that person (such as Gmail, Facebook, Twitter and other such social networking sites). This includes destroying or deleting or altering any information residing on such devices/websites.
- **Identity theft –** where someone uses the password or any other unique identification feature of another person without authorization/consent of that person.
- **Cyber terrorism –** where someone attempts to gain access to a computer/laptop/mobile without authorization/consent or causes denial of access to that person who is authorized to access that computer/laptop/mobile.
- **Offensive communication –** where someone sends any grossly offensive information of another person which is known to be false for the purpose of annoying, inconveniencing, insulting, deceiving, or taking vengeance.
- **Sexting –** where someone does self - production and posting of intimate pictures, sexually explicit conversations, posting/sharing of intimate pictures