Ref No-DPSGFBD/CIRCULAR/III-XII / 072 /2022-23. **Date: May 11, 2022**

Dear Parent

PROMOTING CYBER SAFE BEHAVIOUR

We are very concerned with our observation that while children today have become active and creative users of technology, a large number of them are using technology with irresponsibility with:

- Underage accounts,
- unmonitored conversations
- Membership of unknown and unverified groups
- Unethical personal comments
- Thoughtless likes and sharing
- Pressurising peer to join groups
- Spending time beyond acceptable limits
- KEEPING INVOLVEMENT SECRET FROM PARENTS AND LYING WITHOUT REMORSE.

It is important to know: -

- There is a thin line dividing **positive cyber use and negative cyber lapse.**
- Even a single lapse can label the individual as a **Cyber offender** and consequences are SERIOUS
- Cyber lapses (or crimes) can alter the life of the offender (including a Juvenile offender) **in a blink and make the offender liable to strict police action which can lead to detention in Juvenile Home, high fine and lifelong tag of an offender**
- In case of proven cyber offence by a school going child, the school is duty-bound to co-operate with investigative authorities fully.
- As per school policy, students with proven cyber offence will not be allowed to continue their enrolment at DPS Greater Faridabad
- The **cyber offense committed at school or at home, while being enrolled as student of DPS Greater Faridabad will carry equal weight with school authorities.**

Parents are requested to:

- Ensure that Instagram and Facebook accounts of wards below legal permissible age **are deleted ON PRIORITY.**
- Sit down for an earnest and detailed conversation with ward to reinforce knowledge of cyber laws and need for ethics and accountability.
- Also watch their wards closely everyday to check social –emotional mental health. Is the child disturbed ? Not sleeping or eating well ? Not socialising with family? Wants to be alone ? In all such cases , there is need to strongly step in.

NOTE : Indiscipline in real classroom is managed , controlled and resolved by Teacher and the matter dissolves. But one mistake in Online /Virtual Classroom is forever as ** screenshots, Forwards, recordings live on as digital footprints .Hence, children need to be taught Digital Manners to follow at all times.

Students need to know that not all Internet information is valid or appropriate.

- Age inappropriate material or violent images can affect students negatively.
- Internet information may promote negative attitudes, such as hate or intolerance, and dangerous or illegal activities, such as self-injuring behaviour, gambling, and illegal drug use etc.

- Web searching bust be carefully done under parent supervision. Students need to know what to do and who to ask for help when they encounter a person or site on the Internet.
- Reporting illegal Internet communications and activities immediately to the guardian or teacher is necessary.

Internet messages and the people who send them are not always what or who they seem.

- People in chat rooms, instant message "buddies," or those who visit a blog may not be who they appear to be.
- Students should learn to recognize when someone is potentially dangerous.
- Students need to realize when an Internet encounter may be questionable and how to protect themselves when this occurs.
- E-mail can cause malicious code infection problems for a computer or network. Students should not open Email or attachments from unknown sources.
- Students need to know which information is safe to share with others online, which should never be shared and why sharing it could put them at risk.
- Students should never reveal any information about where they live or attend school.
- Students need to be aware of their electronic messages, even those with known friends, can leave electronic footprints that can be misused by others.

Predators and cyberbullies anonymously use the Internet to manipulate students.

- Bullies use Internet tools, such as instant messaging and the Web, to harass or spread false rumours. Students need to know how to seek proper help in these potentially dangerous situations.
- Students need to know that posting personal information and pictures can allow predators to contact and begin grooming them for illegal meetings and actions. Personal photos can be easily misused or altered when posted on social platform.
- Gaming sites can attract cyberbullies. Some games may contain pornographic and/or violent images. Students need to talk with parents about what is acceptable. Teachers will also guide students about it.
- Students need to know how to detect whether a specific file download is legal and/or free of malicious code.

COMMON CYBER CRIMES WITH PENALTIES – MUST KNOW FOR ALL DIPSITES & PARENTS

1) Creating fake email/ social networking accounts: Creating social networking account such as Facebook, Twitter, Instagram, linked in etc. using the name of the victim and using their identify to send unsolicited content to generate hatred or defame or name them is an offence. Also posting objectionable content using the signature and photograph of victim is a crime. It often confuses the public and generates negative publicity.
Provisions applicable: Section 465,Section 420 ,Article 370 if there is the extensive distribution of fake news in the social messaging site like WhatsApp, section 66D.
3-7 years of imprisonment / fine upto 1 lac-5 lac or both)

2) Web defacement / posting derogatory pictures on web or social networking accounts:
The homepage of a website is replaced with a defamatory page. Government sites generally face the wrath of hackers on symbolic days. Pictures and/or words are scribbled across the defaced website. It's kind of a vandalism in which a website is marked by hackers who are trying to make their mark and it's a common type of cyber-attack.
Provisions applicable: Sections 43 and 66 of IT Act and Sections 66F, 67 and 70 of IT Act also apply in some cases.
The punishment of the offence under this section is imprisonment up to three years, or with fine up to Rs.2 lakhs or with both.

3) Online hate community: Online hate community is created inciting a religious group to act or pass objectionable remarks against a country, national figures etc.]
Pls. note-Even derogatory comments on individuals /peers /people in known circle is a cyber offence involving high penalties.
Provisions applicable: Section 66A of IT Act and 153A & 153B of the Indian Penal Code.
(3-7 years of imprisonment / fine of 5 to 10 lac or both)

4) Email account hacking: If victim's email account is hacked and obscene emails are sent to different people via victim's address book.
Provisions applicable: Sections 43, 66, 66C, 67, 67A and 67B of IT Act.
The maximum punishment for the above offences is imprisonment of up to **3 (three) years or a fine or Rs. 5,00,000 (Rupees five lac) or both.**

5) Introducing viruses, worms, backdoors, rootkits, trojans, bugs: All of the above are some sort of malicious programs which are used to destroy or gain access to some electronic information.
Provisions applicable: Sections 43, 66of IT Act and Section 426 of Indian Penal Code
Punishable with **imprisonment up to three years and with fine.**

6) Cyber terrorism: Many terrorists are using virtual (G-Drive, FTP sites) and physical storage media (USB's, hard drives) for hiding information and records of their illicit business.
Provisions applicable: Conventional terrorism laws may apply along with Section 69 of IT Act.
Whoever commits or conspires to commit cyber terrorism shall be punishable with **imprisonment which may extend to imprisonment for life.**

7) Cyber pornography: Child sexual abuse material (legally known as child pornography) refers to any content that depicts sexually explicit activities involving a child.
Provisions applicable: Sections 67, 67A and 67B of the IT Act.
The punishment for a first offence of publishing, creating, exchanging, downloading or browsing any electronic depiction of children in obscene or indecent or sexually explicit manner is**imprisonment for 5years and a fine of Rs 10 lakh.**

8) Phishing and email scams: Phishing involves fraudulently acquiring sensitive information through masquerading as a trusted entity. (E.g. Passwords, credit card information)

Provisions Applicable: Section 66, 66A and 66D of IT Act and Section 420 of IPC
This is a punishable offence under Section 43 of the Information Technology Act, 2000 **with penalty upto Rs. 1 Crore.**

9)Theft of confidential information: Many business organizations store their confidential information in computer systems. This information is targeted by rivals, criminals and disgruntled employees.

Provisions applicable: Sections 43, 66, 66B of IT Act and Section 426 of Indian Penal Code.
If non-disclosure clause may be prima facie viewed as negative in nature, then it may lead to **termination or dissolution of employment and services and more.**

10)Cybersquatting:**Cybersquatting is the practice of registering names, especially well-known company or brand names, as internet domains, in the hope of reselling them at a profit. It is the bad-faith registration and use of a domain name that would be considered confusingly similar to an existing trademark.**

11)Source code theft: A source code generally is the most coveted and important “crown jewel” asset of a company. Hacking and stealing it is an offence.

Provisions applicable: Sections 43, 66, 66B of IT Act and Section 63 of Copyright Act.

12) Tax evasion and money laundering: Money launderers and people doing illegal business activities hide their information in virtual as well as physical activities.

Provisions applicable: Income Tax Act and Prevention of Money Laundering Act. IT Act may apply case-wise.

13)Online share trading fraud: It has become mandatory for investors to have their demat accounts linked with their online banking accounts which are generally accessed unauthorized, thereby leading to share trading frauds.

Provisions applicable: Sections 43, 66, 66C, 66D of IT Act and Section 420 of IPC.

If anyone knowingly or intentionally conceals, destroys, alters or causes another to do as such shall have to suffer **imprisonment of up to 3 years or fine up to 2 lakh rupees.**

IMPORTANT

If any parent or student of our school comes across any information on any cyber offense, it is hoped that information will be shared with school in the best interest of all.

We thank you for reading this important circular at length.

We strongly trust our young Dipsites to uphold their personal safety and image of school at all times through ethical use of the internet.

Let’s enjoy being positive citizens and using technology to create a better world for all of us.

Regards

Principal