



TAGORE INTERNATIONAL SCHOOL

PASCHIMI MARG, VASANT VIHAR, NEW DELHI-110057

Standard operating Procedure for CYBER SAFETY (Nursery - XII)

Our school has an obligation to provide a safe, secure, and caring environment. We maintain a zero-tolerance policy towards misuse of technology for any kind of cybercrime or for bullying of students and staff.

"Bullying in any form is strictly prohibited inside or outside the school premises, and no such act will go unnoticed or unpunished."

This Cyber Safety Policy of Tagore International School Vasant Vihar explains the desired student code of conduct. This policy is to engage all students, teaching and non-teaching staff, and parents in an effort against all forms of cybercrime as a part of the moral and administrative fabric of the school.

DEFINITIONS:

- **Cybersecurity**, or information technology security, is the technique of protecting computers, networks, programs, and data from unauthorized access or attacks that are aimed at exploitation of any kind.
- **Cyber safety** refers to safe and desirable practices in online environments and in the use of electronic and ICT equipment devices.
- **ICT equipment and devices** include, but are not limited to, interactive boards, computers, laptops, tablets, storage devices, cameras, all types of mobile phones, video and audio players and receivers, social networking sites, and any other technologies as they come into use.
- **Cyberbullying** involves the unwanted use of electronic equipment devices to harass and cause discomfort to other members of the school community.
- **Netiquetes** describes the rules of conduct for respectful and appropriate communication on the internet.

IMPLEMENTATION:

Being involved in online spaces requires students to behave responsibly—for themselves and others. This includes:

- appropriate use of language
- upholding democratic values
- respect for diversity and equality
- respect for privacy and dignity of others
- no violation of human rights

- not visiting any in-appropriate sites
- respect for people's property (e.g. copyright)
- not accessing and misusing other people's data without their consent
- following the protocols laid down for online classes
- not sharing of class google groups with people outside the class

Behaving Safely Online Means:

- protecting your own privacy and personal information
- selecting appropriate spaces to work and contribute
- protecting the privacy of others (this can be sharing personal information or images)
- being proactive in informing a parent/guardian or teacher about what is 'not quite right'
- following the netiquettes

These principles of safety and responsibility apply to internet and social media use at home and at school.

THE SCHOOL WILL

- make students aware of the benefits and risks of using ICT.
- integrate cyber safety education into the curriculum with other school safety issues.
- promote staff awareness of their professional responsibilities for students' well-being in the area of cyber safety
- provide workshops for the students, parents, and teachers to be safe in cyberspace.
- use student's photograph on school's website as well as social media platforms for sharing information related to school activities

THE STUDENT WILL:

- sign an agreement to abide by the school's cyber safety policy that aims to prevent bullying and harassment.
- ensure that all material being accessed on the internet is appropriate.
- seek clarification about accessing websites or other sources of information where they may be unsure of content.
- ensure that their communication with other students, staff members, and community members does not result in personal harassment, vilification or attack. This includes, but is not limited to, written words and the posting of images.
- not take snapshots of participants or use any clips of meeting recordings for creating any form of digital or print media to circulate on social media or otherwise during online sessions. This includes, but is not limited to, creating memes, videos, etc. of teachers and students.
- **ensure that they do not log in using a fake identity.**
- report any communications that are inappropriate to parents/guardians or a teacher when ICT equipment devices are used beyond school time.
- follow all the guidelines and protocols that ensure their safety in cyberspace
- be responsible for ICT equipment and devices being used in school

- not use mobile phones, tablets, smart watches or any such electronic device in school premises

THE PARENT WILL:

- explain the “Cyber Policy Undertaking Form” to their ward(s).
- support the school in encouraging responsible use of ICT equipment and devices by their ward.
- keep control of all the online activities of their ward.
- go through the list of offences and penalties under Indian I.T. Act 2000.

Some of the offences and penalties against the under-mentioned sections of the Indian I.T. Act 2000 include:

Section	Offence	Punishment
65	Tampering with Computer Source Code	Imprisonment up to 3 years or fine up to Rs 2 lakhs
66	Computer-related offences	Imprisonment up to 3 years or fine up to Rs 5 lakhs
66-B	Dishonestly receiving stolen computer resource or communication device	Imprisonment up to 3 years and/or fine up to Rs. 1 lakh
66-C	Identity Theft	Imprisonment of either description up to 3 years and/or fine up to Rs. 1 lakh
66-D	Cheating by Personating by using computer resource	Imprisonment of either description up to 3 years and /or fine up to Rs. 1 lakh
66-E	Violation of Privacy	Imprisonment up to 3 years and /or fine up to Rs. 2 lakh
67	Publishing or transmitting obscene material in electronic form	On first Conviction, imprisonment up to 3 years and/or fine up to Rs. 5 lakh. On Subsequent Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh
68	Failure to comply with the directions given by Controller	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh
72	Breach of Confidentiality and privacy	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh.

SCHOOL-BASED ACTIONS AND CONSEQUENCES

If a student is found to be involved in any misconduct, it will be considered an informed decision / choice made by the student to engage in such activity. It will not be considered a mistake. Following action will be taken in such situations:

- Oral/written warning.
- Suspension from attending classes/school for a specified period.
- Withholding or cancelling the result.
- Expulsion/rustication from school in extreme cases.

This policy will be reviewed annually.

Warm regards



(Jyotika Jakhar)
PRINCIPAL