MANAVA BHARATI
INDIA INTERNATIONAL SCHOOL
Panchsheel Park (SOUTH), New Delhi-110017

Circular For Parents

Effective communication is key to positive partnerships, and it is especially crucial for the relationship between us - **MBIIS and parents.** The students and their future are our combined responsibility.

Further, with the advent of technology (especially in the aftermath of the COVID pandemic) we are all having to rely far more on electronic means of communication.

At MBIIS, we rely on three primary modes of communication with the parents - the school's online portal, Google Classrooms, and official emails.
It is our endeavor to use only these channels for communication.

We are also extremely cognizant of the rules and guidelines mandated for Cyber Communication (as outlined in the Information Technology Act, 2000).

In the recent days, we have been apprised of some alarming cases of misuse, at the behest of a few students.

1. It has been brought to our attention that certain emails seemingly sent by the school were sent via fake IDs. Investigations yielded that some students had created fake IDs to masquerade as official **MBIIS IDs.**

2. In other cases, fake IDs were used by students, to send emails to teachers/school staff, that too, relied on spoofing.
   Email spoofing involves forging the sender's email address or modifying the email headers to make it appear as if the email originated from an official source.

Such acts are serious offenses as per the Information Technology Act, and also a breach of trust.
Through this circular, we want to apprise you of the protocols we wish to follow when we communicate with you/the students.

Strengthen communication to/with the School

Parents are requested to always check the following points before accepting and opening the emails from MBIIS:

1. The school communicates via the following email IDs:
   a. connect@mbiis.in - The school's official email ID for attendance, circulars, assignments etc.
   b. office@mbiis.in - The school's administrative office, as well as communication from the Principal.
   c. The class or subject teachers' official IDs. Each teacher at MBIIS has an individual email for all school/student related communication. No teacher is allowed to communicate with/or respond to emails from personal IDs.

As a general thumb rule, please always check the email IDs - all mails sent from/to MBIIS should end with "@mbiis.in".

Other Do's and Don'ts.

- Students can attend Online Classes or submit assignments only via their individual official School email ID. No other e-mail ID will be granted access to Online Classes.
- Students are not allowed to share their ID with other students or even their parents.
- The official School ID should not be used for personal use.
- Parents are not allowed to correspond with the school using their wards' school email IDs.
- Each parent, registered guardian and each student is provided an independent user ID to log into the school portal. It is not expected that such IDs will be shared or used interchangeably.
- **Please correspond with the school only through your email IDs as registered with the school. If you need to change/update your email ID, please write to us at connect@mbiis.in.**
- The school views all the above extremely seriously. Any misuse/indiscipline/misrepresentation/masquerading by the student using his official or any other ID, will be considered as a significant offence and the school reserves the right to invoke disciplinary action which may amount to suspension or termination, at the sole discretion of the school.

Guidelines for Students:

Students need to be made aware of their responsibilities as Cyber Citizens too. They need to be aware that the guidelines mandated for Cyber Communication (as outlined in the Information Technology Act, 2000) apply to them (and by extension, you, since they are "minors").
Understanding cybercrime is crucial for students as they navigate the digital world. As Cyber Citizens, here are some important points student need to know:

➔ **Online Safety:** Students should be aware of online safety practices, including using strong and unique passwords, being cautious while sharing personal information online, and understanding the privacy settings of social media platforms. Passwords and online personas (like Instagram or Snapchat profiles) should never be shared with others. Much like banking information is private, so are online IDs and profiles.

➔ **Social Media Awareness**: Students should be mindful of the information they share on social media platforms. Oversharing personal details can make them vulnerable to identity theft or cyberstalking. They should also be cautious of friend requests or messages from unknown individuals.

➔ **Sharing Photos/Videos**: Anything posted online lives forever. It is near-impossible to erase online history, especially when shared in public domains or even via social media. Discretion needs to be applied when sharing any form of personal information/content, with a view to the future.

➔ **Forwards and Misinformation:** Forwarding videos, photos, memes, news and other such content can lead to unintended consequences. WhatsApp, Snapchat and Instagram shares especially in groups can come under scrutiny of Authorities and lead to investigations and other reviews. Please refrain from partaking in such forwarding/sharing practices. Refrain from becoming Group Admins on any such platforms.

➔ **Cyberbullying:** Cyberbullying is a form of online harassment that can have serious emotional and psychological effects. Students should understand what constitutes cyberbullying, how to report incidents, and seek help from parents, teachers, or trusted adults if they experience or witness cyberbullying.

➔ **Phishing and Scams**: Students should be aware of phishing emails, messages, or websites that attempt to deceive them into revealing personal information or downloading malware. They should be cautious when clicking on links, and if something seems suspicious, they should verify the source before taking any action.

➔ **Responsible Cyber Citizenship:** Students should understand the importance of responsible digital behavior. This includes respecting the privacy and intellectual property of others, being mindful of their online interactions, and avoiding engaging in harmful or illegal activities online.

➔ **Reporting Cybercrime:** If students come across any form of cybercrime or suspicious activity online, they should report it to a trusted adult, such as a parent, teacher, or school counselor. They can also report incidents to the school's administration or local law enforcement, depending on the severity of the situation.

By understanding the risks associated with cybercrime and adopting safe online practices, students can protect themselves, their personal information, and contribute to a safer digital environment for everyone.

Principal