CYBER SAFETY POLICY

المدرسة الهندية الجديدة
أم القيوين

THE NEW
INDIAN SCHOOL
Umm Al Quwain

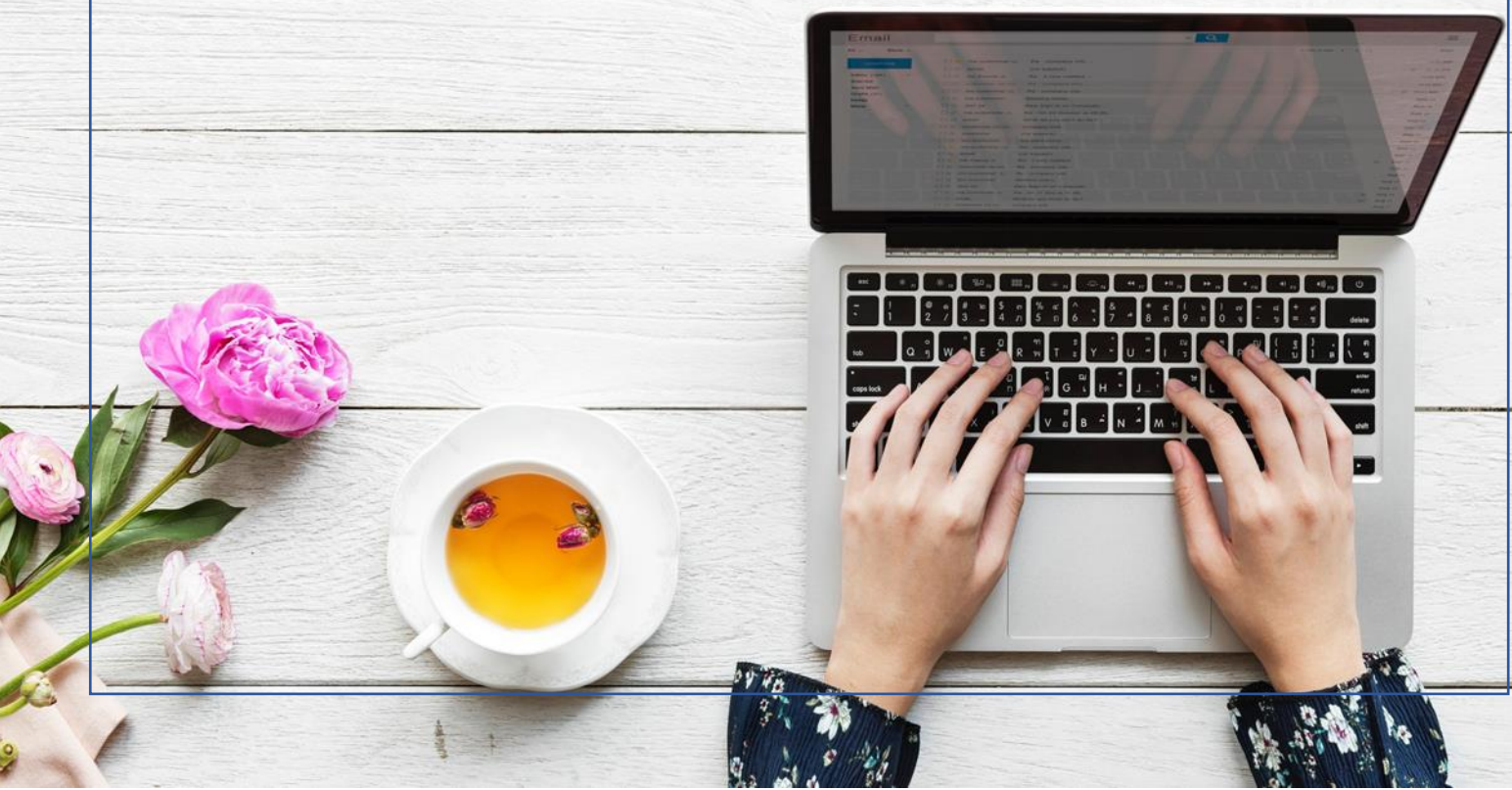

TABLE OF CONTENTS

INTRODUCTION

The Internet is without a doubt one of the best resources available to us. Unfortunately it's also extremely dangerous if you aren't aware of who and what lurks behind the scenes. Everyone should know how to be safe when surfing the web, but internet safety tips and tricks are spread out all over the web without a go-to resource. Since the majority of internet scam and virus victims are students and young people, that community must be conscious and vigilant while browsing the internet world.

"Cyber Bullying is the use of the Internet and related technologies to harm other people in a deliberate, repeated, and hostile manner." - **Wikipedia**

RATIONALE

The New Indian School UAQ embraces the presence and use of Information and Communication Technologies (ICT) as an integral part of the learning environment. The Internet allows for access to information 24 hours a day, 7 days a week. For school online capabilities not only create entrée to a vast amount of resources but also facilitate distance learning and collaboration between classes and students in different locations. Along with the benefits the Internet brings, however, come costs such as new threats to students. The Cyber Safety policy seeks to ensure the safe and responsible use of ICT within the NIS community.

AIMS:

- To promote the appropriate use of ICT by all members of the school community that ensures the safety and wellbeing of all students, staff and parents, emphasizing a zero tolerance to cyber bullying and other forms of online threats.
- To ensure students, staff and parents are aware of their roles and shared responsibilities in relation to cyber safety and appropriate online behavior's.
- To develop the skills, knowledge, attitudes and behavior's required of students, staff and parents to participate and function responsibly, safely and appropriately in cyberspace.

DEFINITION:

Cyber safety:

The way in which users behave responsibly online to keep themselves and their friends safe. It incorporates the safe and desirable use of the Internet and ICT equipment and devices, an awareness of our digital footprint, and how to behave appropriately and respectfully.

ONLINE THREATS TO STUDENTS

As well as the threats that all users face when going online, such as computer viruses and email scams, students are at risk from the following:

Cyber bullying: Cyber bullying is bullying that takes place over digital devices such as cell phones, computers, and tablets. Cyber bullying can occur through SMS, text, and mobile applications (apps) or online in social media, forums, or gaming where people can view, participate in, or share content. Cyber bullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or

private information about someone else, causing embarrassment or humiliation. Some cyber bullying crosses the line into unlawful or criminal behavior.

Inappropriate Content: Adolescents and children can unintentionally come into contact with inappropriate content, such as sexually explicit material. Unsolicited obscene materials can also be received electronically.

Sexting: Sexting is the sharing and receiving of sexually explicit messages and nude or partially nude images via text messages or apps. Sexting, while commonly occurring off school grounds, also occurs on school property, with content being sent and viewed on cell phones. Of note is that possession of sexually explicit photos received by sexting can be considered a type of possession of child pornography from a legal perspective.

Sextortion/Ransomware: Students may also become victim to sextortion, possibly via ransomware, if they engage in sexting. Sextortion occurs when someone threatens to distribute private and sensitive material if not provided with images of a sexual nature, sexual favors, or

money. Ransomware is a particular form of computer malware in which perpetrators encrypt users' files, and then demand the payment of a ransom for users to regain access to their data. Ransomware can also include an element of extortion, in which the perpetrator threatens to publish data or (possibly sexually explicit) images if the victim does not do what the perpetrator wants, such as provide nude photos.

Oversharing: Personal information that is sometimes shared by students includes their name, age, address, phone number, and Social Security number.

Online Predation: Online predators put victims through "the grooming process," a series of steps by which they build the victim's trust by sympathizing with him or her or feigning common interests, after which they proceed to set up a face-to-face meeting with the victim and then move forward with manipulation and seduction.

IMPLEMENTATION:

The New Indian School promotes partnership between all members of the school community in adhering to this policy. Our approach to cyber safety aligns with our school values and is supported by our ICT Acceptable Use Policy, Digital Media Policy, Virtual Learning Policy and Well-Being Policy.

Also the school will be strictly following the guidelines of Child Digital Safety policies under the Cyber Safety and Digital Security Law of The United Arab Emirates.

Reference: ***https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security***

PREVENTION:

The school is responsible for sourcing and implementing relevant and developmentally appropriate programs and strategies that promote positive online behaviors and cyber safe practices.

- A range of classroom-based, interactive, online student learning, staff professional learning, and parent education opportunities will be utilized such as Cyber safety experts, promoting cyber safe websites, support materials and publishing relevant information via school newsletter and Circulars.
- All staff, students and parents are responsible for acting in accordance with the school's annual ICT User Agreements, and to work in partnership to ensure the safe and productive use of ICT.

- The school has the authority to monitor, access and review all school-based ICT usage by students, staff and parents. This includes

emails sent and received on the school's computers and/or network facilities.

INTERVENTION

Students, staff or parents can report any breaches of the ICT User Agreements or incidents of cyber bullying activity to a staff member or Principal at any time either by WhatsApp or by mail to feedback@nisuaq.com

- Any alleged incidences or allegations of behavior that are in breach of the NIS ICT User would be thoroughly investigated by the school.
- Significant breaches made by, or involving, students will result in the school notifying the parents of those students.
- Where a breach is deemed to be extremely serious, relevant government authorities may be contacted by the school administration.
- The school's response to alleged breaches will be followed up with due diligence and consideration for all parties involved or affected by any breach.
- The progress and well being of any student involved in breaches will be monitored and evaluated in line with our Cyber Safety and Well-Being Policy.
- Where cyber bullying has been identified, counseling and support may be offered, as determined by the school.
- Consequences of inappropriate use will follow the steps outlined in the Cyber Safety and Well-Being Policy.

CONCLUSION & EVALUATION

Due to the rapid evolution of ICT, regular evaluation and updating of this policy will occur as and when required by the school leadership. ICT team will constantly monitor the tidings in vogue and will foresee the futuristic developments regularly and constantly and make amends in the said policy as and when required.

THANKS