NIBRAS INTERNATIONAL SCHOOL

an American Education

NIS E- Safety Policy for Families & Students

Academic Year 2023-2024

- ✔ **Purpose**

Nibras International School E-Safety policy enables our school to create a safe e-learning environment that:

- protects children from harm,
- safeguards staff in their contact with pupils and their own use of the internet ,
- ensures the school fulfills its duty of care to pupils
- provides clear expectations for all acceptable use of the internet.
- to create awareness among the stakeholders on 'the various initiatives of U A E in relation to child protection by incorporating the **Federal Law No: 3 of 2016** (**Wadeema's Law**)- Federal Law No. 3 of 2016 concerning child rights, which states that all children must be provided with appropriate living standards, access to health services, education, equal opportunities in essential services facilities without any kind of discrimination,
- to create awareness among the stakeholders on 'the various initiatives of U A E in relation to child protection by incorporating the **Federal Law No: 5 of 2012** on combatting cybercrimes – the article of this law highlights a number of computer and online related activities and how they would be dealt with under the law. It addresses subjects such as IT security, invasion of privacy, malicious and illegal activities including hacking, fraud, improper system use, defamation, threats to state security, terrorism, insult to religions, and many more. etc.

- ✔ **What is E-safety**

E-safety is often defined as the safe and responsible use of technology. This includes the use of the internet and also other means of communication using electronic media (E.g.text messages, gaming devices, email etc). In practice, e-safety is as much about behavior, as it is electronic security.

- ✔ **Acceptable use of Policy**

We in Nibras International School, Dubai are pleased to be able to offer our students, staff and guests' access to computer technology, including access to the internet and google account. We are dedicated to access and support of appropriate technology which unlocks our potential and connects us locally and globally. We envision a learning environment where technology is a part of us, not apart from us. We believe that the tremendous value of technology and the information technology network as an educational resource far outweighs the potential risks. We will leverage existing and emerging technology as a means to learn and thrive in the 21st Century and prepare our students for success toward their goals in the competitive global, electronic age. We feel that access to the tools and resources of a world-wide network and understanding when and how these tools are appropriately and effectively used are imperative in each student's education. The school's information technology resources, including email and Internet access, are provided for educational purposes. If you have any doubt about whether a contemplated activity is acceptable, consult with your immediate teacher, supervisor, Principal to help decide if the use is appropriate. Adherence to the following policy is necessary for continued access to the school's technological resources

- ✔ **Users must respect and protect the privacy of others by:**

1. Using only assigned accounts.

2. Only viewing, using, or copying passwords, data, or networks to which they are authorized.

3. Refraining from using VPNs and distributing private information about others or themselves.

✔ **Users must respect and protect the integrity, availability, and security of all electronic resources by:**

1. Observing all school Internet filters and posted network security practices.

2. Reporting security risks or violations to a teacher or IT Manager.

3. Not destroying or damaging data, networks, or other resources that do not belong to them, without clear permission from the owner.

4. Conserving, protecting, and sharing these resources with other users.

5. Notifying a staff member or IT administrator about network malfunctions.

✔ **Users must respect and practice the principles of community by:**

1. Communicating only in ways that are kind and respectful.

2. Reporting threatening or discomforting materials over internet to a teacher or IT administrator.

3. Not intentionally accessing, transmitting, copying, or creating material that violates the school's code of conduct or honor code (such as messages/content that are pornographic, threatening, rude, discriminatory, or meant to harass).

4. Not intentionally accessing, transmitting, copying, or creating material that is illegal (such as obscenity, stolen materials, or illegal copies of copyrighted works).

5. Not using the resources to further other acts that are criminal or violate the school's code of conduct or honor code.

6. Avoiding spam, chain letters, or other mass unsolicited mailings.

7. Refraining from buying, selling, advertising, or otherwise conducting business, unless approved as a school project.

✔ **Consequences for Violation**

Violations of these rules may result in disciplinary action, including the loss of a user's privileges to use the school's information technology resources. Further discipline may be imposed in accordance with the school's code of conduct and honor code up to and including suspension or expulsion depending on the degree and severity of the violation.

✔ **Supervision and Monitoring**

The use of school owned information technology resources is secure, but not private. School and network administrators and their authorized employees monitor the use of information technology resources to ensure that users are secure and in conformity with this policy. Administrators reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement. The school reserves the right to determine which uses constitute acceptable use and to limit access to such uses. The school also reserves the right to limit the time of access and use.

✔ **Bring Your Own Device (BYOD)**

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

• The school has a set of clear expectations and responsibilities for all users

• All network systems are secure and access for users is differentiated

• Where possible these devices will be covered by the school's / academy's normal filtering systems, while being used on the premises

• All users will use their username and password and keep this safe

• Regular audits and monitoring of usage will take place to ensure compliance

• Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy

Student Device Specification's

→ **Chromebook**

CPU: AMD A4-9120C processor Dual-core 1.60 GHz

Graphics: AMD Radeon R4 Graphics

RAM: 4 GB, DDR4 SDRAM

Screen: 11.6-inch (29.5cm); HD (1366 x 768); 16:9; IPS

Storage: 64GB Flash Memory

Ports: 2 x USB-A; 2 x USB-C;

Connectivity: Wireless IEEE 802.11ac; Bluetooth 4.1

Camera: HD webcam

→ **Laptop**

OS - Windows 10 , 64-bit operating system, x64-based processor

Processor - 10th Gen Intel(R) Core(TM) i5 @ 2.40GHz 2.42 GHz

RAM 8.00 GB

Hard Disk - 128 GB SSD

→ **Ipads (Elementary Only)**

OS	iOS 12.1.3, up to iPadOS 15.6, planned upgrade to iPadOS 16
Chipset	Apple A12 Bionic (7 nm)
CPU	Hexa-core (2x2.5 GHz Vortex + 4x1.6 GHz Tempest)
GPU	Apple GPU (4-core graphics)
WLAN	Wi-Fi 802.11 a/b/g/n/ac, dual-band, hotspot
Bluetooth	5.0, A2DP, EDR
Internal	64GB 3GB RAM, 256GB 3GB RAM

✔ **PASSWORD POLICY**

The school will be responsible for ensuring that the school network is as safe and secure as possible and that procedures within this policy are implemented. A safe and secure password system is essential and will apply to all school technical systems, including networks, devices, email and virtual learning environment. Creating a good password computer is crucial for the safety of the children. It is, therefore, good to set some policies in place while creating passwords for the computers and all online login systems. Some of the possible policies may include:

✔ **Length**

We recommend a minimum of six (preferably eight) characters in a password for students. The reason for this is because the time one takes to crack a password increases exponentially with its length.

✔ **Complexity**

Passwords should contain at least one alpha, one numeric and one non alphanumeric character (a symbol).

✔ **Repetition**

Change the password on regular intervals and make sure that it is not the same as the previously used passwords. It is recommended that a user does not keep using two passwords over and over again by alternating between them.

✔ **Privacy** Do not share passwords with anyone, passwords are to be treated as sensitive and confidential. Do not use the "Remember Password" feature of applications (e.g. Google, Outlook, or browsers such as Firefox or Chrome etc.).

✔ **User compliance**

I understand and will abide by this Acceptable Use Policy. I further understand that should I commit any violation of this policy, my access privileges may be revoked, disciplinary action and/or appropriate legal action may be taken.

NIBRAS INTERNATIONAL SCHOOL
an American Education

❖ ICT Acceptable Use Policy for NIS Students:

Agreement / E-Safety Rules

- Our family will provide our child with a working and fully charged laptop, chromebook, or macbook every day with the specifications stated by the NIS IT Department. This will ensure our child's ability to access school online resources for class as well as participate in external tests such as MAP, PIRLS, etc.
- Our family realizes it is not the school's responsibility to supply an electronic device. A temporary replacement may be provided if there is one available and only to complete a class assessment. Laptops will not be given to students who do not have their devices charged or who do not have a working device longer than 7 days.
- I will only use my laptop for school purposes and not for personal use during the school day.
- I will not share my username or password with anyone. I am responsible for any action that takes place on my personal device or from my account and will accept the consequences.
- I will only use the internet for school-related purposes. I will not download any programs or applications unless directed to by a teacher. This includes VPN, games, social media, and chat groups (i.e. Snapchat, Discord, etc)
- If I download any of the above at home, I acknowledge that I am not allowed to open or use these programs during school hours.
- I acknowledge I am not allowed to use or accept permission from anyone allowing me to gain access to unapproved wifi networks. I shall ONLY use the designated wifi for NIS students. Any violation will be considered hacking into a secured network and may have legal consequences.
- Our family understands that it is illegal in the UAE to take pictures or videos of anyone without permission. In addition, we are aware that NIS policy prohibits students from taking pictures or videos on campus without written consent from NIS administration.
- I will not write, text, or email any offensive, racist, sexist, bullying, sexual, or otherwise inappropriate messages to any NIS student, teacher, or employee. I understand that "joking" is not an excuse and will accept consequences if I partake in this behavior.
- I will not use any of my electronic devices to disparage, embarrass, intimidate, or offend NIS students, staff, employees, or NIS families whether I am on campus or not. I will also not use the NIS name in a derogatory manner in chat groups, social media, or online forums.
- There is no use of cell phones for any reason throughout the school day.
- Our family understands that not following the above rules can present a security risk for the school and potential safeguarding issue for its students. There will be school consequences as well as potential legal consequences for violating the NIS E-Safety Policy.
- I will not use NIS school email for unauthorized logins such as login to social media, online shopping, chat groups, movies, etc.

***Note, your child's device will no longer be permitted for use at NIS if this form is not submitted by October 2, 2023. Please review with your child and return prior to this date. Thank you for supporting NIS.**