Cyber Security Policy

Aim

The aim of the Cyber Security Usage Policy is to ensure that all staff and students are aware of the cyber-attacks on electronic Computing/Mobile device via internet and to use it sensibly and safely for the purpose of information sharing and improved learning experience.
Cybersecurity aims at protecting systems, networks, and programs from digital attacks.

School Responsibilities

The school recognizes the need to maintain the confidentiality, integrity, and availability of all sensitive information, including student records and other confidential data. In line with Digital Dubai's efforts to promote a secure and safe digital environment, the school has established the following cyber safety routine.

1-Two-factor Authentication: The school requires all employees and authorized individuals who access the school's systems remotely to use two-factor authentication. This will help to prevent unauthorized access to the school's systems and protect sensitive information.

2-Penetration Testing and Ethical Hacking: The school will conduct penetration testing (pen testing) or ethical hacking exercises at least twice a year to assess the security of its systems. The results of these exercises will be shared with Digital Dubai to help identify and address any potential security risks. This will help to ensure that the school's systems are protected from cyber threats and that sensitive information is kept secure.

All Staff and students should be able to recognise if, any abnormal behaviour on their electronic device provided by the school or their BYOD device connected at school network are fully aware of the best internet practice to be able to deal with it effectively as well as are fully aware in surfing internet safely.

It is vital for students to understand how to stay safe online, the need to be aware of any dangers that might come their way, and for staff to create this awareness among them through different lessons and activities.

Legal Implication

In accordance with this policy, Pristine Private School will comply with the following:

- A law governing the publication and sharing of *Dubai data (Law No. 26 of 2015)* aims to protect and safeguard all individuals, including children.
- In accordance with Dubai Data Law (*Law No. 26 of 2015 on the Organization and Publication of Dubai Data)*
- According to *Federal Law No. 3 of 2016 Concerning Child Rights*, the following is required: "Telecommunications companies and internet service providers shall notify the

competent authorities or concerned entities of any child pornography materials distributed by social media sites and on the Internet. They must provide any necessary information and data on the people, entities, or sites that distribute such material or intend to mislead children."

- *UAE Federal Law 5 of 2012 on Combatting Cyber Crime* aims at criminalizing persons who get unlawful access to a computer network, electronic information system, or website and those who indulge in destructing, deleting, omitting, copying, altering or publishing any data or information.
- Furthermore, in March 2018, the Ministry of Interior and the National Programme forhappiness and Wellbeing launched the 'Child Digital Safety' initiative, aimed at raising awareness about online threats and challenges among children and school students, and promoting safe and constructive use of the internet.
- The new Decree by *Federal Law No. 34 of 2021 ("Cybercrimes Law")* has repealed the previous pertinent legislation, which was Decree of Federal Law No. 5 of 2012 against cybercrimes.

This policy must be read alongside Social media Policy, Acceptable Internet Usage Policy and BYOD Policy

BYOD (Bring Your Own Device Policy)

This allows students who already own devices to use them at school for educational purposes with the permission of the classroom teacher. BYOD increases the amount of technology available in the classroom, giving the students more hands-on access to technology devices for learning safely. By allowing students to bring their personal devices into school and integrating learning technologies in the classroom, our students will develop research, innovation, and digital literacy skills necessary to be competitive in the modern global workforce.

Social Media Policy

Pristine Private School recognizes the rights of students, faculty staff, and employees who want to participate in online social networking. Social Media Policy guidelines are designed to create an atmosphere of good will, honesty, and individual accountability. Staff and students should always keep in mind that information produced, shared, and retrieved by them is a reflection on the school community and is subject to the school's policies. When accessing, creating, or contributing to any blogs, wikis, podcasts, or other social media for classroom, these guidelines are to be kept in mind.

Students, staff , Parents, Guests are expected to set and maintain high ethical standards in their use of social networking. Since social media reaches audiences far beyond the community, staff and students must use social sites responsibly and be accountable for their actions.

Acceptable Internet Usage policy

The aim of the Acceptable Internet usage policy is to ensure that all students and Staff are aware of the risks and hazards of internet usage and use it sensibly and safely for the purpose of information sharing and improved learning. All students and Staff should be free of any fear of cyber bullying by anyone known or unknown, should be able to recognise cyber bullying and be fully equipped to be able to deal with it effectively as well as are fully competent in surfing internet safely. All users competently use the web tools to develop critical thinking and problem-solving skills enabling them to become effective global citizens.

IT Provision cannot be used for

- Browsing websites and conducting online searches that could be construed in any manner as extremist, intolerant of other people's faiths and beliefs, or that pose a threat to UAE legislation and the Digital Dubai Regulation.
- Transmitting, retrieving, or storing any harassing or discriminating messages, as well as any communications that are offensive to a particular person or group.
- Obtaining content that would be offensive based on someone's race, colour, religion, political beliefs, ethnic origin, sexual orientation, gender, age, ability, nationality, or marital status;
- Participating in ANY type of cyberbullying; looking for pornographic or offensive content;
- Obtaining content for the purpose of harassing someone else;
- Creating communications that are threatening or defamatory.
- Downloading illegally downloaded content or anything that violates the legal rights of another individual

Scope of the policy:

- Updating accounts password regularly to prevent unauthorised access.
- Safe Internet and social media usage to prevent Cyber Attacks.
- Don’t share account password with anyone to prevent hacking.
- Don’t share the Digital Network privileged Wi-Fi password with others to prevent unauthorised access of the privileged network.
- Safe email attachment sent or received by to prevent Phishing attack.
- Keep complex password and maintain logs of password history to prevent Brute Force attack.

Monitoring IT Use

PPS grants its students and employees the privilege of using the company's computer systems and personal devices, such as laptops, tablets, smartphones, and smartwatches, to create and communicate electronic information through its networks. However, it should be noted that all

such activities, including email and internet usage, are subject to PPS's monitoring guidelines to ensure responsible and ethical use.

Cyber Security Violation Consequences

The school places a strong emphasis on cyber security and is dedicated to educating its users about its policies for safe and responsible usage of technological and informational resources. Internet access is provided to staff and students for various purposes, including general use, email, and academic research. While there is an enormous amount of online content, the school recognises that users may unintentionally run into offensive material, which should be reported to the IT administrator.

The school addresses intentional actions that violate its policies in a proactive manner to maintain a safe and secure online environment. In order to make sure its technological and informational resources are used responsibly and ethically.

Disciplinary measures, such as suspension or reporting to Digital Dubai may be taken, if students or staff are found to have accessed or shared content that is inappropriate or unrelated to academic purposes.

Policy Details: Cyber Security Policy	
Version Date	**November 2022**
Review Date	**August 2024**