



DR. PILLAI GLOBAL ACADEMY
local actions...global options
New Panvel

INFORMATION TECHNOLOGY POLICY



Revised: March 2022

TABLE OF CONTENTS

Scope	3
Preamble	3
User Policy and safety rules	3
Mandatory Guidelines to IBDP students	5
Student must not	7
Appendix	
Parental consent slip	8
Bibliography	9

Dr. Pillai Global Academy, New Panvel, provides a secure digital environment through the rules laid by its IT policy which are strongly adhered by its faculty members and students to meet its standards and avoid academic dishonesty at every level. The IT Department consists of trained faculty members to cater to the needs of approved international curricula across the school rendering need-based facilities to enhance teaching and learning process within the school campus.

The policy is manifested through its specific terms and conditions imbuing the school's mission in delivering world class education to its students.

SCOPE

This policy relates to all computer use and access to workstations, laptops and other electronic devices at Dr. Pillai Global Academy, New Panvel.

PREAMBLE

Access to the internet is provided for the purposes for educational teaching-learning and research. The purpose of this policy is to provide rules for appropriate use of all types of Information technology and the internet.

Students and parents are expected to read carefully the following agreement. The user is responsible for his/her actions and activities involving the school computers, networks and Internet services and for his/her computer files, passwords and accounts.

USER POLICY AND SAFETY RULES

While teachers play the role of facilitators in explaining concepts through digitalized platforms, students are allowed hands-on training to learn and explore on various applications within their disciplines. Students at higher grades explore the opportunity to research on their subjects as part of their curriculum to fulfil the requirements as laid out by their respective Boards. However, parents and students should carefully understand the rules to avoid illegal practices for maintaining the school's sanctity and ethical considerations to maintain a healthy teaching-learning environment, the breach of which can lead to legal action by the school authorities.

In this regard, unacceptable practices as listed below are strictly prohibited by the students if norms laid by the policy are violated to breach the academic integrity in education.

- **Illegal Activities** – Using School Department computers, networks and Internet services for any illegal activity or activity that violates other school Department policies, procedures and/or school rules.
- **Violating Copyrights** – Copying or downloading copyrighted materials without the owner's permission.
 - **Plagiarism** – Representing one's own work as any materials obtained on the Internet (such as term papers, articles, etc.) when not cited or referenced appropriately and abiding by the norms given by the Boards and as laid out extensively in the Academic integrity policy of the school.
- **Copying or Installing Software** – Copying, downloading or installing software through school's internet without the expressed authorization of the computer system administrator.
- **Non-School Related Uses** – Using networks and Internet services for non-school related purposes such as private financial gain, commercial, advertising or solicitation purposes, or for any other personal use.
- **Misuse of Passwords and Unauthorized Access** – Sharing passwords, using other users' passwords and/or accessing other users' accounts.
- **Malicious Use or Vandalism** – Any malicious use, disruption or harm to School Department computers, networks and Internet services, including but not limited to hacking activities, breaching of security features, and creating, uploading or spreading computer viruses.
- **Unauthorized Access to Chat Rooms, Instant Messaging or Newsgroups** – Accessing chat rooms, instant messaging or newsgroups without specific authorization from the supervising teacher.
- **Negatively Impacting Network Capacity** – Engaging in activities that cause unreasonable demand on network capacity or disruption of system operation including but not limited to downloading large files without permission from the computer system administrator.
- **Social Networking** – Use of social networking sites is strictly prohibited in school.

- **National Cyber Law** – Computing, network and Internet resources must not be used to knowingly violate the laws and regulations of the country or any other nation, or the laws and regulations of any state, city, province, or local jurisdiction in any material way.
- **Ownership** – Students have no right of ownership or expectation of personal privacy to their Internet usage, including personal computers or laptops while on the DPGA campus. It is possible to monitor network and Internet usage under such situation and DPGA reserves the right to inspect any and all network traffic and files at any time. DPGA reserves the right, without notice, to limit or restrict any computer, network or Internet usage.
- **Privacy Policy** – No one may use DPGA facilities to monitor use of computing or network resources by any other individual, or perform any probing, scanning, sniffing, or vulnerability testing, except as otherwise provided by DPGA policies or law.
- **Virus** – No one may use DPGA computer, network, or Internet facilities to deliberately propagate any virus, worm, Trojan horse, trap-door, or back-door program code or knowingly disable or overload any computer system, network, or to circumvent any system intended to protect the privacy or security of another user.
- **Violating Filtration** – No one may install, remove, or otherwise modify any software for the purpose of bypassing, avoiding, or defeating any filtering, monitoring, or other security measures DPGA may have in place, except as otherwise provided by DPGA policies.

MANDATORY GUIDELINES TO IBDP STUDENTS

- Laptop/ipad is to be used for only academic purpose under supervision of subject teachers at designated locations.
- The laptops should not have any objectionable data at any point of time. Videos other than related to academics, songs and movies, etc. are not to be stored in any format.

- The school has full authority to check any student's laptop/ipad/smart phone at any point of time in his/her presence/absence if suspected of any malicious activities.
- The school does not take any responsibility for the authenticity of software installed on laptops.
- The laptops should be used during specified time as decided by teachers-in charge only.
- The school's WIFI connection will be allowed only to IBDP students to complete their assignments which are a part of their curriculum to be fulfilled. However, under such conditions, the net must only be used for academic/research purpose. Downloading of any other material is strictly prohibited.
- Students are strictly prohibited to carry their personal dongles to school. They should use school's WIFI only to have internet access for their academic purposes.
- Any student found accessing any restricted site which is not meant for him/her will be penalized and the same may lead to school authority confiscating his/her laptop.
- The students are solely responsible for his/her laptop.
- The school authority has full rights to make any change in the laptops for academic purpose.
- Any chat applet, messenger and social networking sites are strictly not allowed.
- IBDP students can check their school e-mail ids only during the school hours for getting need-based feedback from subject teachers and other details including circulars from school's end.
- Headphones, Earphones, Gaming device and any similar kind of devices are not allowed in the academic block unless otherwise permitted with a specific purpose.
- Students need to deposit their hard disks or pen drives with Grade Tutors and use only when required under supervision.

- The school authority has full rights to check any portable storage device of the students.
- The laptop should also not have personal photos and videos in it which might be objectionable. Students willing to keep photos and videos must get them approved by the IT department.
- DPGA, New Panvel reserves the rights to confiscate the laptop/ipad/smart phone/smart watch in case the above points are violated.

STUDENT MUST NOT

- Change the IP or any other configuration related to use of DPGA computers.
- Knowingly infringe copyright.
- Download programs or games.

Infractions of these policies constitute misuse of DPGA, New Panvel's assets and therefore are considered violations of DPGA Code of Conduct and may result in disciplinary actions by school authorities, sanctioned under relevant provisions of DPGA, New Panvel Rules and Regulations.

APPENDIX

PARENTAL CONSENT SLIP

I hereby give my consent for having read the rules and regulations thoroughly as cited under DPGA, New Panvel's Information and Technology Policy.

I agree that school authority can take strict action on my ward _____ if found guilty of violating any of the rules as stated in the policy.

Parents' Name : _____

Parents' Signature : _____

Date : _____

BIBLIOGRAPHY

Ministry of Electronics & Information Technology, Information Technology Act,
<https://www.meity.gov.in/content/information-technology-act>.

Sreenidhi International School, IT policy,
<http://www.sis.edu.in/Pages/IT%20Policy.aspx>