المدرسة الهندية العامة العليا الخاصة
Indian Public High School Private

POLICY NAME:	**IT (COMPUTER AND NETWORK USE) POLICY**				
APPROVAL AUTHORITY:	**PRINCIPAL**	**ADOPTED:**	**03.05.2021**	**REVIEWED:**	**03.10.2022**
RESPONSIBLE EXECUTIVE:	**E-SAFETY OFFICER**	**REVISED:**	**15.4.2025**	**NEXT REVIEW ON:**	**15.4.2026**
RESPONSIBLE OFFICE:	**IT DEPARTMENT**	**AVAILABLE:**	**IN THE LIBRARY, WEBSITE, NLP**		

Scope:
IPHS has developed the Computer and Network Use Policy to guide individuals wrt acceptable use of computers, information systems, and networks owned, leased or used by IPHS. All such systems and networks are considered IPHS property for purposes of this policy. This policy is also intended to describe best practices to ensure availability, integrity, reliability, privacy, and confidentially of the School's computers, information systems, data, and networks. IPHS makes computing and network resources available to faculty, staff, students to support the educational .

This policy supplements other IPHS policies and procedures, including, but not limited to, Social Medial Policy and Acceptable Use Policy, and Connecting Devices to the IPHS Network Policy, should be read together with those policies.

The School reserves the right to amend this policy at its discretion with or without notice. In case of amendments to the policy, IPHS will make efforts to inform users of changes. The most current policy can be found on the IPHS Website:

User Responsibilities:

IPHS's computing and network resources and services are limited and should be used wisely and carefully with consideration for the needs of others. By using the school's computers, information systems, and networks, "you" – user of school computing resources, assume personal responsibility for acceptable use in conformity with this policy, other applicable IPHS policies, and with applicable Local laws and regulations.

All communications and information transmitted by or through, received by or from, or stored in these systems are IPHS records and property of IPHS. You have no right of personal privacy in any matter stored in, created, received, or sent over IPHS computers, storage devices, email and internet. This includes and is not limited to: NASCORP (databases) Student Information System – in-house software applications, all externally hosted software applications and the following site: https://www.iphsrak.com/ and any other www.IPHS web domain name.

Be aware that even deleted or erased computer, e-mail and voicemail messages may remain stored in IPHS computer servers or telephone systems. By placing information on IPHS's computer systems or servers, or using any IPHS equipment, you have consented to IPHS right to capture, edit, delete, copy, republish and distribute such information.

The IPHS Bullying Policies and IPHS policy with respect to Confidential Information apply to all forms of communication including written e-mail .

IPHS provides access to Internet services such as web-browsing. Use of the school's internet services are only for educational use. This restriction includes any Internet service which is accessed on or from IPHS's premises using IPHS's computer equipment or via IPHS -paid access methods and/or used in a manner that identifies you with IPHS. This also includes remote access such as NASCORP and the IPHS portal.

The following is a non-exclusive list of prohibited use of IPHS technology resources. In a constantly changing world of information technology, it is impossible to enumerate all non-acceptable uses of IPHS computers, information systems, and networks. IPHS reserves the right to prohibit any use of its computing facilities by any person(s) if and when such use appears to be inconsistent with this policy, other computer Use policies, the mission of the school, or any applicable local law.

Prohibited uses:

All users may not…

1. Attempt to use technology resources without proper authorization;
2. Attempt to obtain privileges or access for which you are not authorized;
3. Attempt to learn another user's password(s) or personal information;
4. Attempt to alter or obscure your identity or your computer's identity, including but not limited to IP Address and email address, while communicating on any network, system or application;
5. Attempt to access, modify and/or delete another user's files, configuration or application without the expressed agreement of the owner or by an IPHS Administrator;
6. Share confidential computer, system, application, or network password with any other person;
7. Attempt to interfere with or disrupt computer or network accounts, services or equipment of others including, but not limited to, consumption of excessive IT resources, (e.g. local area network or Internet bandwidth) through the propagation of worms, Trojans, or viruses;
8. Attempt to "crash" any school computing facilities, including any so-called "denial of service attack";
9. Attempt to monitor, intercept, analyze or modify network traffic or transactions;
10. Attempt to alter or reconfigure any IPHS IT resources, (e.g. network infrastructure, servers, wireless);
11. Attempt to use unauthorized devices when connecting to the IPHS network ;
12. Attempt to remove, duplicate or export confidential / sensitive IPHS data in any digital format, outside of IPHS systems and network, without prior written consent by an IPHS administrator. This includes any/all data stored: on-premise and/or externally hosted third party provider.
    - Examples of confidential / sensitive information include, and are not limited to: Emirates ID numbers; financial account information; Health records; employee records; and accounting records.
13. Attempt to use computing or network resources for profit or commercial gain outside of official IPHS business;
14. Download and/or share copyrighted material for which you do not have the proper authorization;
15. Attempt to copy software or any intellectual property in a manner that appears to violate copyright law, or otherwise infringing on any intellectual property rights of others;

16. Compose, transmit, or access data containing content that could be considered discriminatory, offensive, pornographic, obscene, threatening, harassing, intimidating, or disruptive to any other person. Examples of unacceptable content may include, but are not limited to, sexual comments or images, racial slurs, gender-specific comments, or any other comments or images that could reasonably offend someone on the basis of race, color, religion, creed, sex, gender, gender identification, sexual orientation, ethnicity, national origin, ancestry, age, disability (including HIV-AIDS or COVID status), marital status, military status, citizenship status, predisposing genetic characteristics, or any other characteristic protected by law.

17. Consume any food or drink in IPHS Computer lab.