



Hariri High School II

Acceptable Use Policy

2023- 2024

Responsible Office: Information Technology Services

Purpose

The aim of this policy is to ensure that Hariri High School II's IT facilities are used safely, lawfully, and equitably. The School seeks to encourage and facilitate the proper usage of resources in learning, teaching, and researching. This requires responsible and legal use of facilities and resources made available to any member of the Hariri High School II community who is using a computer and internet resources present at the school and its libraries.

Scope

This policy applies to all students, employees, and members of Hariri High School II community.

Policy

Access to the school's resources is a privilege that is granted by Hariri High School II and subject to certain rules, regulations, and restrictions. Such access carries with it legal and ethical responsibilities that should reflect a degree of honesty and discipline appropriate for our community of shared resources. Appropriate and ethical use demonstrates respect for intellectual property, ownership of data, system security mechanisms and individuals' right to privacy and to freedom from intimidation or harassment.

General Requirements

- Users are responsible for exercising good judgment regarding appropriate use of Hariri High School II resources in accordance with school regulations and policies.
- For security, compliance and maintenance purposes, authorized personnel may monitor and audit equipment, systems and network traffic. Devices that interfere with other devices or users on the school networks may be disconnected.

User Accounts

- Users are responsible for the security of data and systems under their control.
- Users should keep passwords secure and not share account or password information with anyone, including other students, personnel, family or friends.

Information Technology Resources

- Users must not use IT resources to gain unauthorized access to remote computers or to impair or damage the operations of school computers, networks and online services.
- Users must not interfere with school device management or security system software.
- Users should contact IT Security before purchasing hardware or software that connects to or runs on school computers or networks.
- Users must not use IT resources for personal financial gain. Occasional personal use of the school's IT resources for purposes other than commercial or financial gain is permitted when it does not consume a significant amount of IT resources, does not interfere with college business or with the performance of a user's job, and is otherwise in compliance with this policy.

Network Use

Users are responsible for the security and appropriate use of the school's network resources available. Using resources for the following is strictly prohibited:

- Causing security breach to the school's network resources, including but not limited to, accessing data, servers or accounts to which you are not authorized, circumventing user authentication on any device, or sniffing network traffic.
- Violating copyright law, including but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, software and learning resource materials.
- Use of the Internet or networks for defamation, sexual harassment, obscenity and cyberbullying.
- Intentionally introducing malicious code, such as viruses, Trojan horses, and spyware.
- Disabling or bypassing authorized security measures, such as local firewalls, virus checking software, web-site restrictions, etc.

Electronic Communications

The following is strictly prohibited:

- Inappropriate use of the communication equipment and services, including but not limited to, supporting illegal activities, and procuring or transmitting material that violates the school's policies against harassment or the safeguarding of confidential or protected information.
- Sending Spam via email, text messaging, instant messaging, voice mail or other forms of electronic communications.
- Forging, misrepresenting, obscuring, suppressing or replacing a user identity on any electronic communication to mislead the recipient about the sender.

Enforcement

The school considers any violation of this policy to be a serious offense. Violators may be subject to disciplinary action, up to and including suspension from school and termination of employment.