# Leaders Private School, Sharjah

## INFORMATION TECHNOLOGY POLICY

*This policy should be read in conjunction with the E-Safety Policy, Acceptable Use Policy for Students and Acceptable Use Policy for Staff, Behaviour Policy, Behaviour Management Policy-MOE, Behaviour Policy for Distance Learning-MOE,* National Child Protection Policy in Educational Institutions in United Arab Emirates, *the Child Protection Policy, Anti-bullying Policy and the Cyber Bullying Policy.*

**Document Details**

| | |
|---|---|
| Information Sharing Category | Public |
| Version | 2.0 |
| Reviewed on | September 2022 |
| Next Review Date | September 2023 |

## 1. Overview

This establishes guidelines and codes of conduct appropriate to the use of computer resources at Leaders Private School.

Computing and networking resources are provided for students, faculty and staff for a wide variety of purposes. These resources are limited, and how each individual uses them may impact the work of other members of the community. It is important that everyone using these resources be aware of what constitutes proper use and behavior. To advance these goals, the School has adopted policies on computer usage.

## 2. Objective / Purpose

This document has two purposes: to prohibit certain unacceptable uses of the Schools' computers and network facilities, and to educate users about their individual responsibilities.

## 3. Scope

This policy covers all computers owned or administered by any part of school or connected to the school's communication facilities, including departmental computers and personally owned computers, and also the school's computer network facilities accessed by anyone from anywhere.

## 4. Policy

a) No one shall assist in, encourage, or conceal from authorities any unauthorized use, or attempt at unauthorized use, of any of the School's computers or network facilities.

b) No one shall knowingly endanger the security of any School computer or network facility, nor willfully interfere with others' authorized computer usage.

c) No one shall use the School's communication facilities to attempt unauthorized use, nor to interfere with others' legitimate use, of any computer or network facility anywhere.

d) No one shall connect any computer to any of the School's networks unless it meets technical and security standards set by the School administration.

e) No one shall hide/ conceive computer hardware belonging to school.

f) All users shall share computing resources in accordance with policies set for the computers involved, giving priority to more important work and cooperating fully with the other users of the same equipment.

g) No one without specific authorization shall use any School computer or network facility for non-School business.

h) No one shall give any password for any School computer or network facility to any unauthorized person, nor obtain any other person's password by any unauthorized means whatsoever. No one except the system administrator in charge of a computer is authorized to issue passwords for that computer.

i) No one shall misrepresent his or her identity or relationship to the School when obtaining or using School computer or network privileges.

j) No one shall capture, reproduce or transmit the photograph(s) of a person without his/ her consent.

k) No one without specific authorization shall read, alter, or delete any other person's computer files or electronic mail. This rule applies regardless of whether the operating system of the computer permits these acts.

l) Hacking: Any users who are caught hacking or attempting to hack the school's computing resources, or any other computer system by way of the school's network will lose their computing privileges and possibly face disciplinary and criminal action. Hacking includes, but is not limited to, activities such as gaining unauthorized access to data, files, or directories; unauthorized examination, alteration, creation, or deletion of data, files, or directories; executing password cracking programs; unauthorized use of another user's account; unauthorized use of protocol analyzers or "sniffers"; spamming; sending e-mail bombs; and infecting computer systems with a virus or similar program.

m) Destruction of Property**:** Any users who willfully or through anger damage or destroy state property will lose their computing privileges, and face disciplinary action.

n) No one shall copy, install, or use any software or data files in violation of applicable copyrights or license agreements, including but not limited to downloading and/or distribution of music, movies, or any other electronic media.

o) No one shall create, install, or knowingly distribute a computer virus, "Trojan horse," or other surreptitiously destructive program on any School computer or network facility, regardless of whether any demonstrable harm results.

p) No one without proper authorization shall modify or reconfigure any School computer or network facility.

q) No one shall store confidential information in computers or transmit confidential information over School networks without protecting the information appropriately.

r) Users shall take full responsibility for data that they store in School computers and transmit through the network facility.

s) Users of School computers shall comply with the regulations and policies of mailing lists, social media sites, and other public forums through which they disseminate messages.

t) System administrators shall perform their duties fairly, in cooperation with the user community, the appropriate School administration, School policies, and funding sources. System administrators shall respect the privacy of users as far as possible and shall refer all disciplinary matters and legal matters to appropriate authorities.

u) Email and other electronic messaging technologies are intended for communication between individuals and clearly identified groups of interested individuals, not for mass broadcasting. No one without prior authorization shall use School facilities to distribute spam messages--the same or substantially the same e-mail message to more than one person without prior evidence that they wish to receive it.

v) The School reserves the right to discard incoming mass mailings and spam without notifying the sender or intended recipient.

w) For its own protection, the School reserves the right to block communications from sites or systems that are involved in extensive spamming or other disruptive practices, even though this may leave School computer users unable to communicate with those sites or systems.

## 5. Enforcement and Implementation

### a) Roles and Responsibilities

Each School department/unit is responsible for implementing, reviewing and monitoring internal policies, practices, etc. to assure compliance with the Policies on the Use of Computers.

The School's IT Department is responsible for enforcing this policy, and is authorized to create technical and security standards for School computing and network facilities and protection standards for information stored or transmitted by School computing and network facilities.

### b) Protection

- Internet usage is blocked based on users in firewall.
- Only the school staffs can access the internet.
- All unwanted websites are blocked.

- Antivirus softwares are installed in all the school computers.
- Access to LPS's office premises, Computer Labs and on-site IT assets are restricted to authorized personnel.
- USB ports are blocked on all systems in the computer labs.
- Wi-Fi connections are protected with secure password.
- Regular checks and scans will be carried out to ensure security hardware and software is properly functioning.

**c) Consequences and Sanctions**

Violations of these policies may incur the same types of disciplinary measures and consequences as violations of other School policies (*Behaviour Management Policy, Behaviour Policy for Distance Learning, the Child Protection Policy, Anti-bullying Policy and the Cyber Bullying Policy)*, including progressive discipline up to and including termination of employment, or, in the cases where students are involved, reporting of a Student Code of Conduct violation. In some cases, violations of this policy may also be violations of Government laws, and consequences may include criminal prosecution.

Systems and accounts that are found to be in violation of this policy may be removed from the network, disabled, etc. as appropriate until the systems or accounts can comply with this policy.

## 6. Definitions

**School computers and network facilities** - all computers owned or administered by any part of Leaders Private School or connected to the School's communication facilities, including departmental computers, and also all of the School's computer network facilities accessed by anyone from anywhere.

**Authorization** - permission granted by the appropriate part of the School's management structure, depending on the particular computers and/or network facilities involved and the way they are administered.