Internet Safety Policy

1**. Overview**
Institutional information and information resources shall be used in an approved, ethical, and lawful manner to avoid loss or damage to Institutional operations, image, or financial interest and to comply with official policies and procedures. Students shall contact the Director of Information Technology prior to engaging in any activities not explicitly covered by these policies.

For the purpose of this policy institution refers to Innovation Montessori Ocoee (IMO) Charter School operating under charter from the Orange County School District, Orange County Florida.

2. Scope
The Institution owns all institutional information resources; use of such resources constitutes consent for the institution to monitor, inspect, audit, collect, and remove any information without permission or further notice. Students shall be instructed in what use is acceptable and what is prohibited. Information Technology will send regular security awareness bulletins to students to address any concerns. IMO regards any violation of this policy as a serious offense. Violators of this policy are subject to IMO discipline action as prescribed by IMO standards of discipline.

3. Designation of responsibilities

3.1 Institutional Executive Director:
- Shall be responsible for ensuring appropriate and auditable security controls are in place.

3.2 Institutional Principals, Assistant Principals and Deans shall be responsible for:
- Informing personnel of institutional policies on acceptable use of information resources.
- Communicating with parents and guardians when violations occur related to student use of technology.
- Coordinating with the Orange County School District when appropriate regarding infractions of the technology policies.

3.3 Teachers and educational staff shall be responsible for:
- Informing current and new students of IMO policies on acceptable use of information resources.
- Ensuring that students comply with IMO policies and procedures.

3.4 Department of Information Technology shall be responsible for:
- Monitoring systems for integrity
- Maintaining and ensuring data backups of critical electronic information as designated by the Director of Information Technology.
- Developing and maintaining the institutions information resource security policies
- Addressing violations of IMO and district policies on information resources

- Interpreting institutional policies on information resources

3.5 Students shall be responsible for:

- Abiding by official IMO policies on acceptable use of information resources.
- Promptly reporting suspicion or occurrence of any unauthorized activities to the Director of Information Technology or one of their designees
- Any use made of their accounts, logon ID's, passwords, PINs, and tokens.

4. Hardware and Software

IMO provides laptop computers based on the Microsoft Windows Operating System for student education use both in classroom and with permission at home. Because students work on institution owned computers, they must comply with institution policies and procedures regardless of the device's physical location. Personal devices are not authorized for use for academic work on school campuses. Resources may be made available to facilitate additional learning at home as needed and personal devices can be used at home in accordance with the remainder of these policies.

4.1 Software

To prevent the introduction of malicious code and protect the integrity of institutional information resources, all software shall be obtained from official institutional sources. Users shall not be permitted to install and/or modify information resources in a manner that diminishes security standards set forth by the institution.

4.2 Complying with copyright and licensing.

All software used on Institutional information resources shall be procured in accordance with official IMO and district policies and procedures, and shall be licensed, and registered in the name of the institution. All students shall abide by software copyright laws and shall not obtain, install, replicate, or use software except as permitted by the software licensing agreements and institution policy.

4.3 Use of Personally Owned Software

To protect the integrity of the institutional information resources, students are not authorized to use personally owned software on institutionally owned equipment. This includes purchased and licensed applications; shareware; freeware; downloads from the Internet, Intranet, FTP sites, local area networks (LAN's) or wide area networks (WANs); and other personally owned or controlled software unless otherwise authorized in writing by the Director of Information Technology or her/his designee in advance of such use. Documented approval shall be secured prior to use and/or installation of personally owned software on institutionally owned equipment.

4.4 Hardware Repair

All hardware repairs on all institution devices will be completed by the Department of Information Technology in accordance with department procedures and processes. No staff other than IT staff are authorized to repair, modify, configure, or replace any hardware component without first obtaining the permission of the Director of Information Technology or the Executive Director of the institution.

Students are expected to maintain the hardware entrusted to them in good working order. While accidents certainly happen, it is expected that students take care in preventing damage to the hardware entrusted to them. Any damage to the device found to be non-accidental in nature is subject to require payment to replace or repair. This includes any charger or cable that may be included with the device. Replacement chargers will be made available to purchase in the event a replacement may be needed.

Hardware is to remain on campus for campus use unless specific arrangements are made with the Department of Information Technology well in advance. To prevent loss, theft, damage, etc. devices should not leave the State of Florida without prior approval.

4.5 Use of Freeware, online games, chat rooms, resources etc.
To prevent the introduction of malicious code and protect the integrity of institutional information resources, online gaming websites shall not be accessed via any institution owned device or network within or outside of operating hours.

Social Media, chat rooms as well as online messaging services besides what is prescribed in the subsequent sections of policy are not to be accessed on institutional devices or networks for any reason without prior authorization by the Department of Information Technology. This includes but is not limited to TikTok, Discord, Facebook, Instagram, Snapchat, and Twitter (X).

5. Electronic Mail and Messaging
Access to the Institution's electronic mail (email) system is provided to all students for dissemination of information and conducting institutional business. Since email may be monitored, all students using Institutional resources for the transmission or receipt of email shall have no expectation of privacy.

5.1 Acceptable use of Electronic Mail and Messaging
The institution provides email to facilitate the conduct of official business. Use of electronic mail and/or electronic messaging resources shall not be done in a manner that interferes with the institutions ability to perform its mission and shall meet the conditions outlined in official institutional directives, missions and/or goals.

5.2 Prohibited Use
Prohibited activities when using the Institutions electronic mail shall include, but not be limited too, sending, or arranging to receive the following:

- Information that violates institutional policies, regulations, local, state, or federal laws.
- Unsolicited commercial announcements or advertising material, unless approved by the institution in advance.
- Any material that may defame or libel the institution, the recipient, the sender, or any other person.
- Email hoaxes, malicious code, or spam (defined as unwanted and unsolicited emails or materials in such large volumes that they tend to disrupt the proper functioning of institutional information resources and or individuals' ability to use those resources).
- Information technology services for unlawful purposes including fraudulent, threatening, defamatory, harassing, or obscene communications.
- Any use deemed threatening, defamatory, harassing, or obscene by the Director of Information Technology, her/his designee, with approval from the Executive Director of the Institution.

6. Internet Safety
Access to the Internet is available to students using the assigned student network. Since Internet activities will be monitored using network monitoring tools, firewalls, classroom management software etc; all students accessing the Internet shall have no expectation of privacy. While other campus wide networks may exist, students are to only connect their device to the approved Student network using the manner prescribed by Information Technology. Any student device detected on any other password protected network will be immediately removed and subject to disciplinary action.

6.1 Acceptable Use
The institution provides Internet access to facilitate the conduct of Institutional business. Use of the Internet shall not be done in a manner that interferes with the work of students, personnel, or the Institutions ability to perform its mission, and shall meet the conditions outlines in official institutional directives or goals.

6.2 Prohibited Use
Prohibited activities when using the Internet include, but are not limited to, the following:

- Posting, sexually explicit material, hate-based material, hacker-related material, or other material that may be deemed detrimental to the integrity, image, and mission of the institution.
- Posting or sending restricted information outside of the Institution without proper or formal authorization.
- Posting commercial announcements or advertising material.
- Promoting or maintaining a personal or private business.
- Using non-work or non-academic related applications or software that occupies excess workstation of network processing time.
- Use of online browser-based games.
- Any use deemed threatening, defamatory, harassing, or obscene by the Director of Information Technology, her/his designee, with approval from the Executive Director of the Institution.
- Any use deemed as not furthering and supporting the educational mission of the Institution by the Executive Director or her or his designee.

6.3 Cellular devices and mobile hotspots
Wireless mobile phones and associated cellular hot spot features are not to be used to conduct academic business or to circumvent network protections.

6.4 Use of Online Content or Social Media
Prior to allowing students to use online content or social media, staff must confirm that the content is not blocked by the student internet filter. If content is blocked, staff must contact the Director of Information Technology prior to student use by completing a helpdesk ticket. The staff member must provide the site name, documentation on how the requested site relates to the curriculum, and the timeframe for unblocking the site. Requests should be made well in advance to allow time for processing and reconfiguration of the network security filters.

In accordance with the Children's Internet Protection Act (CIPA), all Innovation Montessori web access is filtered; however, this does not preclude the possibility that inappropriate sites are not blocked. Do not use Innovation Montessori's Internet to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature). A special exception may be made if the purpose of access is to conduct research with instructor and district approval. Students shall immediately notify a teacher if inappropriate information is mistakenly accessed. This will protect students against a claim of intentional violation of this policy. Parents or guardians should instruct their students if there is additional material that they think it would be inappropriate to access. The district fully expects that the student will follow his or her parents' instructions in this matter.

7. Authorized Monitoring

All institutional owned information systems including but not limited to hardware, networks, software applications, services such as email and messaging, are subject to monitoring and restriction by the Department of Information Technology in consultation with Administration. There is no expectation of privacy for students using these resources. The Department of Information Technology may place monitoring software on student devices, as deemed appropriate and prudent by the Director of Information Technology in consultation with the Executive Director of the Institution and Administration. Additionally, students are prohibited from removing, interfering with, disabling, or otherwise preventing the said monitoring of devices.

8. Generally Prohibited Uses of Information Resources

Generally prohibited activities when using Institutional Information Resources shall include, but are not limited to, the following:

- Stealing or copying of electronic files without permission including the use of peer to peer P2P or other files haring websites.
- Violating copyright laws.
- Browsing the private files or accounts of others.
- Performing unofficial activities that may degrade the performance of systems, such as playing of electronic games including browser-based games and applications.
- Attempting to access any network, resource, computer, or institutional resources, even if the attempt were unsuccessful, that would or could result in damage or disruption to the resources.
- Preforming activities intended to circumvent security or access controls of any organization, including the possession or use of hardware or software tools intended to defeat software copy protection, discover passwords, identify security vulnerabilities, decrypt encrypted files, or compromise information security by any other means.
- Writing, copying, executing, or attempting to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of or access to any institution computer, network, or information.
- Using another user's login credentials passwords, PIN's or any other unique identifier with or without the user's knowledge or consent.
- Conducting fraudulent or illegal activities.
- Disclosing restricted Institutional information.
- Engaging in conduct inconsistent with the institution's stated goals and mission.
- Unauthorized entry into a file or attempted entry of a file or program, to use, read, or change the contents, or for any other purpose regardless of intent.
- Use of any technology to intimidate, harass, bully, or otherwise interfere with any staff, student, or teacher's ability to perform their official duties.

9. User ID's and Passwords

Innovation Montessori Ocoee requires that each student who accesses multiuser information systems have a unique user-ID and a private password. Each authorized individual is personally responsible for the protection and security of his or her user-ID and password and should be aware of the applicable federal and state laws regarding access to authorized systems. Authorized users should not share their private passwords with other individuals or allow other individuals to perform activities on computers under another login.

10. Security Compromise Tools

Innovation Montessori Ocoee staff or students must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information

systems security. Examples of such tools include those which defeat software copy-protection, discover secret passwords, identify security vulnerabilities, exfiltrate data, or decrypt encrypted files. Similarly, users are prohibited from using "sniffers" or any other hardware or software which monitors the traffic on a network or the activity on a computer.

The Information Technology Department will employ tactics, software, and hardware measures to prevent hacking and other IT Security Compromises As such users should not engage in any penetration testing, network exploration or exploitation unless directed by the Director of Information Technology.

11. Items not explicitly covered by policy

Students shall contact the Director of Information Technology prior to engaging in any activities not explicitly covered by these policies.

The institution reserves the right to disconnect or remove institutionally owned or privately-owned equipment or restrict use thereof at any time as required to maintain the functionality, security, or integrity of network, computing, and telecommunications resources. This policy is not intended to abridge academic freedom or the constitutional guarantees of freedom of speech or freedom of expression but rather to allow us to continue to provide a secure computing environment for our students and staff.

12. Social Media

No social media sites may be accessed on School Devices or on the school's network without prior written permission of the Director of Information Technology.

The FLDOE and IMO prohibits the use of TikTok, and any successor platforms, on all district- or school-owned devices, or on any device (including privately owned) connected to district- or school-provided internet; and (b) Prohibits the use of TikTok, or any successor platforms, to be used to communicate or promote any school district, school, school-sponsored club, extracurricular organization, or athletic team.