Policy Number	Policy Name
6.10.3	Technology Acceptable Use Policy

Summary / Purpose

Access to technological resources is a privilege, and violation of established expectations for appropriate use of technology resources may result in termination. Responsible and appropriate usage must be applied to hardware, software, internet and network usage, and applicable licenses and copyrights. This policy establishes expectations of appropriate usage of these resources.

(6) Management

(6.10) Computer, Email and Cell Phone Usage

(6.10.3) Technology Acceptable Use Policy

All employees, students and volunteers of the organization may be granted access and usage of the organization's technology resources, including network and internet usage based on need and job/student status. All access to usage codes and/or devices is assigned to the individual and is not to be shared. Users are responsible for the security of their assigned devices. Users should log out/secure devices when not in use and report any unauthorized usage promptly. All care should be taken to honor intellectual properties including copyright and license restrictions. Respect should be given to other users. Spying, bullying and harassment will not be permitted in any fashion. General usage should be for the purposes of school business or classes only.

(6.10.3.1) Restrictions on usage:

Users may not do the following:

- Provide access to unauthorized users
- Utilize accounts and other privileges that they no longer are authorized to access
- Interfere with restrictions or security settings on any device or system on the organization's network
- Harass, bully, or violate the privacy of other users on the system.
- Destroy, copy or steal any information on the network without explicit permission from the creator or appropriate staff members.

- Introduce, propagate or create malware of any type including but not limited to Trojan Horses, viruses, spyware, worms, etc.
- Damage computer or network systems by any means.
- Use knowledge of network to gain unauthorized access or resources.
- Deprive other authorized users' access of full system and network resources or degrade system performance.
- Chain and mass emails should be avoided except for official business, and source addresses should never be altered.
- Stream media without authorization for specific activities.
- Comment or act on behalf of the organization unless you have permission to do so.
- Use the organization's resources for private business or commercial enterprise.
- Conduct political activities without express permission of the organization's leadership.

(6.10.3.2) Copyright and Licenses:

Due to legal restrictions and penalties on software licenses software may not be copied or installed without approval from the organization's IT personnel or leadership. Illegal usage of software may result in criminal penalties up to and including imprisonment. Software may not be copied from the organization's devices for personal access. If an employee is working remotely a device will be set up for use with properly licensed software necessary for use.

(6.10.3.3) Internet Usage

All internet usage on the organization's systems is monitored to ensure compliance. Internet access on the organization's campus requires a password to access. Passwords are not issued until users read and sign the Acceptable Use for Technology policy. All internet access must be in accordance with the organization's rules and policies, including this document.

(6.10.3.3.1) Acceptable Usage:

- Communications in the course of business or educational interactions and assigned responsibilities, including but not limited to: parents, students, coworkers, peers, business partners, etc.
- Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities
- Participating in educational or professional development activities
- Utilizing the Internet as an educational tool in the classroom.

(6.10.3.3.2) Inappropriate Use:

- Illegal or unlawful usage will not be permitted, including but not limited to: copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses).
- Any internet use inconsistent with the rules, policies and mission of the organization is prohibited.
- Excessive personal internet use is prohibited.

- Individuals shall not establish any <<school>> computers on a peer to peer network unless previously approved by management.
- Individuals may not view, copy, alter, or destroy data, software, documentation, or data communications on any school computer or network without authorized permission.
- Users should limit sharing, downloading or storing large files or videos in order to maintain network performance.
- Pornography, gambling, gaming and media piracy on <<school>> devices are strictly prohibited.

(6.10.3.3.3) Monitoring and Filtering

The organization's equipment or accounts may be monitored for inappropriate usage. If activity is discovered, or reported, in violation of school policy or applicable laws, records retrieved may be used to document the wrongful content in accordance with due process.

(6.10.3.3.4) Security

Users may not share passwords or other access data with another person. In the event an account has been compromised, or a password lost, the user must contact IT to request a reset password. Internet usage must be limited to approved purposes by approved users only.

(6.10.3.3.5) Failure to Comply

Allegations of misconduct will be adjudicated according to established procedures. Sanctions for inappropriate use of the Internet may include, but are not limited to, one or more of the following:

1. Temporary or permanent revocation of access to some or all computing and networking resources and facilities;
2. Disciplinary action according to applicable school policies; and/or
3. Legal action according to applicable laws.

(6.10.3.4) E-mail

(6.10.3.4.1) Account Activation/Termination

Staff will be assigned an email with individually established user names and passwords. Account and password information are the responsibility of the user. Email access will be revoked if/when the user ceases association with the organization, and user email files will be locked. The organization will not maintain or forward emails to former staff and other associates.

(6.10.3.4.2) Expectations of Use

The organization will disseminate official communications via email. Employees are expected to monitor email regularly and provide appropriate responses as necessary.

Emails sent from an account created by the organization shall reflect on the culture of the school. Please ensure courtesy in email usage. It is expected that all users will follow these policies and procedures as well as applicable laws in their use of the email system. E-mails sent through the school's system are subject to public records law and are subject to public document requests.

(6.10.3.4.3) Inappropriate Usage

Avoid sending large files (5 MB or above) via email, whenever possible use a shared drive system to transmit bulk files.

The following are prohibited on the organization's email system:

- Use of email for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).
- Altering, deleting or otherwise tampering with emails or files belonging to the organization or other users.
- Opening email attachments or links within messages from unknown or unsigned sources. Users should always make sure that links and attachments are legitimate to avoid viruses, etc.
- Sharing passwords or attempting to obtain another user's password.
- Commercial, mass mailing, chain letters, and political e-mails.

(6.10.3.4.4) Monitoring and Confidentiality

The organization's email accounts and the systems they are built on are school property. All emails, even deleted e-mails, are subject to monitoring and archival for records maintenance. Users should be mindful of communication within their emails due to public record laws and confidentiality restrictions. No confidential information should be shared outside of the secured organization's system via email as email is an insecure communication protocol.

(6.10.3.4.5) Reporting Misuse

Any and all misuse should be promptly reported to IT personnel and/or school leadership. If a concerning e-mail is received, do not interact with the e-mail and notify IT personnel immediately.

(6.10.3.4.6) Failure to Comply

Allegations of misconduct will be adjudicated according to established procedures. Sanctions for inappropriate use of email may include, but are not limited to, one or more of the following:

1. Temporary or permanent revocation of access to some or all computing and networking resources and facilities;
2. Disciplinary action according to applicable school policies; and/or
3. Legal action according to applicable laws.

(6.10.3.5) Server and Other Data Storage

In order to maximize storage capability only business or school related files should be saved on school servers. Personal files such as mp3's, pictures, and games should not be saved on shared server space. These files could also contain malware which endangers the whole school's infrastructure. Nonbusiness files may be deleted without notification.

(6.10.3.5.1) Storage Restrictions

Storage quotas may be implemented at any time. Employees will be notified when they near their storage quota. Requests for additional storage space must be presented to the IT department.

(6.10.3.6) Internet Safety Policy

Per Federal law, the organization's policy is to:

1. prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;
2. prevent unauthorized access and other unlawful online activity;
3. prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and
4. comply with the Children's Internet Protection Act [Public Law No. 106-554 and 47 USC 254(h)]

(6.10.3.6.1) Definitions

Key terms are as defined in the Children's Internet Protection Act (CIPA).

TECHNOLOGY PROTECTION MEASURE. The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:

1. **OBSCENE**, as that term is defined in section 1460 of title 18, United States Code;
2. **CHILD PORNOGRAPHY**, as that term is defined in section 2256 of title 18, United States Code; or
3. ***SEXUAL CONTACT***. The terms "sexual act" and "sexual contact" have the meanings given to such terms in section 2246 of title 18, United States Code.
4. ***HARMFUL TO MINORS***. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:
   (a) Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
   (b) Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
   (c) Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

(6.10.3.6.2) Access to Inappropriate Material

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes, for specific websites requested in advance. All requests to disable or minimize protection must be done in writing. It is the responsibility of the supervising staff to provide feedback to the IT Department whenever is necessary to blacklist websites that do not comply with CIPA.

(6.10.3.6.3) Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the organization's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) preventing unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) preventing unauthorized disclosure, use and dissemination of personal identification information regarding minors. Disabling or otherwise modifying any technology protection measure that has been implemented for this purpose, constitutes a violation of CIPA.

(6.10.3.6.4) Supervision and Monitoring

All staff members are responsible to supervise and monitor online unsafe of the online computer network and internet access in accordance with this policy and the Children's Internet Protection Act.

Date Adopted	Approval Signature
Click here to enter text.	