MIDLAND INNOVATION+ TECHNOLOGY CHARTER SCHOOL

7 SOUTH 12TH STREET / MIDLAND / PENNSYLVANIA / 15059
724-510-0944 / INFO@MITCHARTERSCHOOL.ORG

MITCHARTERSCHOOL.ORG

ACCEPTABLE USE AND INTERNET SAFETY POLICY

CODE: ACCUSE001, STATUS ACTIVE, ADOPTED (JUNE 15, 2022)

Purpose
The Board of Trustees of the Midland Innovation + Technology Charter School (MITCS) provides computer network and Technology Resources to enhance educational opportunities for MITCS students, employees, and the MITCS community. This policy details acceptable use of Technology Resources provided by MITCS. These services and equipment are provided by MITCS as a privilege to the user and appropriate and ethical use of any MITCS Technology Resources, tools and equipment is required.

It is every Technology Resource User's (as defined below) duty to use Technology Resources responsibly, professionally, ethically and lawfully. Access to these resources may be designated a privilege, not a right. This policy applies to aspects of both adult and minor acceptable use of Technology Resources.

This Policy is intended to fulfill requirements of state and federal laws to the extent applicable, including the Federal Children's Internet Protection Act (CIPA), 47 U.S.C. 254(h) and (l) and the Neighborhood Children's Internet Protection Act (N-CIPA), the 2008 Broadband Improvement Act and any applicable implementing regulations. As such, this policy addresses the following:

- Access by minors to inappropriate matter on the Internet and World Wide Web;
- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
- Unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
- Unauthorized disclosure, use, and dissemination of personal information regarding minors; and
- Measures designed to restrict minors' access to materials harmful to minors.
- In using or accessing MITCS's Technology Resources, Users must comply with the following provisions.

Definitions
For the purposes of this policy and related procedures and forms, the following terms are defined as follows:

Technology Resources: Technologies, devices and resources used to access, store or communicate information. This definition includes, but is not limited to: computers, information systems, networks, laptops, iPads, modems, printers, scanners, fax machines and transmissions, telephonic equipment, audio-visual equipment, digital cameras, wireless reading devices, i.e. Kindles and Nooks, Internet, electronic mail, electronic communications devices and services, multi-media resources, hardware and software, including Moodle software.

User: Any person who has signed this Policy and is permitted by MITCS to utilize any portion of MITCS's Technology Resources including, but not limited to, students, parents, employees, Board of Trustee members, contractors, consultants, vendors and agents of MITCS
.
User Identification (ID): Any identifier that would allow a user access to MITCS's Technology Resources or to any program including, but not limited to, e-mail and Internet access.

Password: A unique word, phrase or combination of alphanumeric and non-alphanumeric characters used to authenticate a User ID as belonging to a specific User.

Child Pornography: Under federal law, any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

- the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
- Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
- Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
- Under Pennsylvania law, any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of eighteen (18) years engaging in a prohibited sexual act or in the simulation of such act.

Harmful to Minors: under federal law, is any picture, image, graphic image file or other visual depiction that:

- Taken as a whole, with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
- 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 lewd exhibition of the genitals; and
- Taken as a whole lacks serious literary, artistic, political or scientific value as to minors.

Harmful to Minors: under state law, is any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:

- Predominately appeals to the prurient, shameful, or morbid interest of minors;
- Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; and
- Taken as a whole lacks serious literary, artistic, political, educational or scientific value for minors.

Minor: For purposes of compliance with CIPA, an individual who has not yet attained the age of seventeen. For other purposes, minor shall mean any person under the age of eighteen (18).

Obscene: Under federal and Pennsylvania law, any material or performance if:

- the average person, applying contemporary community standards, would find that the subject matter, taken as a whole, appeals to the prurient interest;
- the subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene; and
- the subject matter, taken as a whole, lacks serious literary, artistic, political, educational or scientific value.

Technology Protection Measure: A specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.

Vandalism: Any malicious attempt to harm or destroy Technology Resources, data of another user, Internet or other networks. This includes, but is not limited to, the uploading or creation of computer viruses.

Authorized Users
MITCS's Technology Resources may be used by any authorized User. Use of MITCS's Technology Resources is a privilege, not a right. If a potential user has a history of discipline problems involving Technology Resources, the Chief Executive Officer ("CEO") or their designee may make the decision not to give the potential user access to certain MITCS Technology Resources.

User Privacy
Computer accounts and Technology Resources are given to Users to assist them in the performance of MITCS -related functions. A User does not have a legal expectation of privacy in the User's electronic communications or other activities involving MITCS's Technology Resources, including e-mail, in anything they create, store, send, share, access, view or receive on or through the Internet.

By using MITCS's network and Technology Resources, all Users are expressly waiving any right to privacy and consenting to having their electronic communications and all other use accessed, reviewed and monitored by MITCS. A user ID with email access will only be provided to authorized Users on condition that the User consents to interception of or access to all communications accessed, sent, received or stored using MITCS technology and signs this Policy. Electronic communications, downloaded material and all data stored on MITCS's Technology Resources, including files deleted from a User's account, may be intercepted, accessed or searched by MITCS administrators or designees at any time in the regular course of business to protect Users and MITCS's equipment. Any such search, access or interception will be reasonable in inception and scope and shall comply with all applicable laws.

Please refer to MITCS's policy relating to Remote Access and Monitoring of Technology Resources for a comprehensive review of the provisions governing MITCS's use of software to access, monitor and track school-issued Technology Resources.

Technology Administration
The Board of Trustees directs the CEO or his/her designee to assign trained personnel to maintain MITCS's technology in a manner that will protect MITCS from liability and will protect confidential student and employee information retained on or accessible through MITCS's Technology Resources.

Administrators may suspend access to and/or availability of MITCS's Technology Resources to diagnose and investigate network problems or potential violations of the law or MITCS policies and procedures. All MITCS Technology Resources are considered MITCS property.

MITCS may maintain or improve Technology Resources at any time. MITCS or authorized MITCS agents may remove, change or exchange hardware, equipment or other technology between buildings, classrooms or Users at any time without prior notice.

Content Filtering and Monitoring
The availability of access to electronic information does not imply endorsement by MITCS of the content, nor does MITCS guarantee the accuracy of the information received. MITCS shall not be responsible for any information that may be lost, damaged, or unavailable when using the network or for any information that is retrieved via the Internet.

MITCS shall not be responsible for any unauthorized charges or fees resulting from access to the Internet or other network resources.

The Board of Trustees declares that computer and network usage is a privilege, not a right. MITCS's computer and network resources are the property of MITCS. Users shall have no expectation of privacy in anything they create, store, send, delete, receive or display on or over MITCS's internet, computers or network resources, including personal files or any use of MITCS's Internet, computers or network resources. MITCS reserves the right to monitor, track, and log network access and use; monitor fileserver space utilization by MITCS users; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access/privileges and/or administer appropriate disciplinary action. MITCS shall cooperate to the extent legally required with the Internet Service Provider (ISP), local, state, and federal officials in any investigation concerning or related to the misuse of MITCS's Internet, computers and network resources.

The Board of Trustees requires all users to fully comply with this policy and to immediately report any violations or suspicious activities to the CEO or designee.

MITCS reserves the right to restrict access to any Internet sites or functions it deems inappropriate through established Board policy, or the use of software and/or online server blocking. Specifically, MITCS operates and enforces a technology protection measure(s) that blocks or filters access to inappropriate matter by minors on its computers used and accessible to adults and students. The technology protection measure shall be enforced during the use of computers with Internet access.

Upon request by students or staff, the CEO or designee may authorize the temporary disabling of Internet blocking/filtering software to enable access for bona fide research or for another lawful purpose. Written permission from the parent/guardian is required prior to disabling Internet blocking/filtering software for a student's use. If a request for temporary disabling of Internet blocking/filtering software is denied, the requesting student or staff member may appeal the denial to the CEO or designee.

Viruses
Viruses can cause substantial damage to Technology Resources. Users are responsible for taking reasonable precautions to ensure they do not introduce viruses to MITCS's Technology Resources.

All material received on flash drive, external hard drives, or other magnetic or optical medium, and all materials downloaded from the Internet or from Technology Resources or networks that do not belong to MITCS must be scanned for viruses and other destructive programs before being transferred to MITCS's Technology Resources. Any User receiving an e-mail from a questionable source must contact the Principal before opening the e-mail or any attachment included in the e-mail.

To ensure security and avoid the spread of viruses, Users accessing the Internet through a Technology Resource attached to MITCS's network must do so through an approved Internet firewall or technology protection measure.

Encryption Software
Users shall not install or use encryption software on any MITCS Technology Resource without first obtaining written permission from the Principal. Users shall not use passwords or encryption keys that are unknown to the Principal and School Administration. The federal government has imposed restrictions on export of programs or files containing encryption technology. Software containing encryption technology shall not be placed on the Internet or transmitted in any way outside the United States.

Web Content Developed by Students
As part of class/course assignments, students may be developing and/or publishing content to the internet via web pages, electronic and digital images, blogs, wikis, podcasts, vodcasts, and webcasts, or may be participating in videoconferences:

- Personal information such as phone numbers, addresses, e-mail addresses or other specific personal information shall not be published or shared to a public page or videoconference.
- All web content must comply with this Policy.
- All web content and videoconferencing must be under the direction and
- supervision of the teacher/administrator and is to be used for educational purposes only.
- All web content is subject to copyright law and fair use guidelines.
- All web content shall only be posted to MITCS approved web pages, blogs, wikis, podcasts, webcasts, vodcasts and videoconferences.

Prohibitions
Students, staff and all Users are expected to act in a responsible, ethical and legal manner in accordance with MITCS policies and federal and state laws. Specifically, the following uses of MITCS's Technology Resources are prohibited:

- To facilitate illegal activity, including unauthorized access and hacking.
- To engage in commercial, for-profit, or any business purposes, except where such activities are otherwise permitted or otherwise authorized.
- Non-work or non-school related work.
- Product advertisement or political lobbying.
- Production or distribution of hate mail, unlawfully discriminatory remarks, and offensive or inflammatory communication.
- Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
- To access or transmit material that is harmful to minors and/or Users, indecent, obscene, pornographic, child pornographic, terroristic, or advocates the destruction of property.
- Use of inappropriate language or profanity.
- To transmit material likely to be offensive or objectionable to recipients.
- To intentionally obtain or modify files, data and passwords belonging to other Users, or integral to system and network operations.
- Impersonation of another user, anonymity, and pseudonyms.
- Loading or use of unauthorized games, programs, files, or other electronic media.
- To disrupt the work of other Users.
- Destruction, modification, or abuse of Technology Resources and peripheral hardware or software.
- Relocation of MITCS hardware without prior administrative consent.
- Quoting personal communications in a public forum without the original author's prior consent.
- To access or use any form of electronic mail on MITCS Technology Resources unless authorized by the CEO or his/her designee.

- Using the network to participate in online or real-time conversations unless authorized by the teacher/administrator for the purpose of communicating with other classes, students, teachers, experts or professionals for educational purposes.
- Using a disk, removable storage device or CD/DVD brought into MITCS from an outside source that has not been properly scanned for viruses or authorized for use by a teacher/administrator in accordance with MITCS established procedures.
- To discriminate against, advocate violence against, harass, intimidate, bully or cyberbully others.
- To send unsolicited ("spamming") or forwarded e-mails and chain letters to persons.
- Using "spoofing" or other means to disguise user identities in sending e-mail or other electronic communication via bulletin boards, newsgroups, social networking sites, instant messages, e-mail systems, chat groups, chat rooms, or through other Technology Resources.
- To send, transmit or otherwise disseminate proprietary data, trade secrets, or other confidential information of MITCS.
- Post or allow the posting of personal information about themselves or other people on the technology resource unless authorized by the Principal. Personal information includes address, telephone number (including home, work and cell phone numbers), school address, work address, pictures or video bites, clips, etc.
- To refer to or attempt to refer to MITCS or its employees, agents, trustees, parents or students in any electronic communication, posting, blog, website, e-mail or social networking site, without written authorization of the Principal.
- To access or transmit gambling, pools for money, or any other betting or games of chance.
- Using Technology Resources to solicit information with the intent of using such information to cause personal harm or bodily injury to another or others.
- Using Technology Resources to post, share or attempt to post information that could endanger an individual, cause personal damage or a danger of service disruption.
- Indirectly or directly making connections that create "backdoors" to MITCS, other organizations, community groups, etc. that allow unauthorized access to the Technology Resources of MITCS.

Student Education

MITCS will educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

Security

MITCS intends to strictly protect its Technology Resources against numerous outside and internal risks and vulnerabilities. Users are important and critical players in protecting these assets and in lessening the risks that can harm Technology Resources. Therefore, Users are required to comply fully with this Policy and to immediately report any violations or suspicious activities to the Principal.

System security is protected in part by the use of passwords. All passwords must be at least eight characters and include alphanumeric and special characters. Users will be required to change their passwords every thirty (30) days. MITCS will maintain a password history that prevents the use of a repetitive password. After three (3) unsuccessful access attempts, an attempted user will be locked out and must contact the Principal or his/her designee. After a period of inactivity, the User will be automatically logged off the system.

Failure to adequately protect or update passwords could result in unauthorized access to personal or MITCS files. Users shall be responsible for safeguarding their passwords for access to MITCS's Technology Resources and for all transactions made using their passwords. To protect the integrity of MITCS Technology Resources and systems, the following guidelines shall be enforced:

- Students and other Users shall not reveal their passwords to another unauthorized individual.
- Passwords shall not be printed or stored online.
- Students and other Users are required to log off from the network when they complete working at a particular station.
- Users are not to use a computer that has been logged in under another student's, teacher's or user's name.
- Any User identified by the CEO or his/her designee as having a history of discipline problems involving Technology Resources may be denied access to any or all of MITCS's Technology Resources.
- Students and other Users shall not alter a communication originally received from another person or computer with the intent to deceive.
- Users shall not misrepresent the identity of a sender or source of communication.
- Users shall not disable or circumvent any MITCS security; software or hardware.
- Users shall not interfere with or disrupt MITCS's systems, network accounts, services or equipment.
- Files, system security software/hardware or any MITCS system shall not be altered or attempt to be altered without the written authorization of the CEO or his/her designee.
- Unauthorized hardware and electronic devices shall not be connected to MITCS systems.
- Users shall comply with requests from the CEO or his/her designee to discontinue activities that threaten the operation or integrity of the MITCS system.

Use of passwords to gain access to Technology Resources or to encode particular files or messages does not imply that Users have an expectation of privacy in the material they create or receive on Technology Resources. MITCS retains access to all material stored on the Technology Resources regardless of whether that material has been encoded with a particular User's password, subject to limitations as set forth in established Board policy as well as applicable law.

Users shall not alter or copy a file belonging to another user without first obtaining permission from the owner of the file. Ability to read, alter, or copy a file belonging to another User does not imply permission to read, alter, or copy that file. Users shall not use the Technology Resources to "snoop" or pry into the affairs of other Users by unnecessarily reviewing the files and e-mails of another.

A User's ability to connect to another computer's system through the network or by any other electronic means shall not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the administrators of those systems and the Principal.

Safety

To the greatest extent possible, Users of the network will be protected from harassment or unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall immediately bring them to the attention of a teacher, staff member or an administrator.

Communications through MITCS Technology Resources are limited to only that which serves a demonstrable educational purpose. For safety reasons, MITCS Users shall not reveal personal addresses or telephone numbers to other Users on MITCS networks or on the Internet.

The CEO or his/her designee shall be responsible for implementing protection measures to determine whether MITCS's computers, laptops, iPads, Kindles and other Technology Resources and technology related devices such as USB drives, digital cameras and video cameras, PDAs, MP3 players, printers, etc. are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include but not be limited to:

- Utilizing technology protection measures that block or filter Internet access for minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by minors by the Board of Trustees.
- Maintaining a listing of all employees and Users with access to the room which contains MITCS's server.
- Generate and maintain monitoring reports (including firewall logs) of user activity and remote access on MITCS's system by all Users, including but not limited to students, employees, contractors, consultants, and/or vendors.
- The report should include the date, time and reason for access, whether it was remote access, changes made and who made the changes.
- Maintaining documentation that students no longer enrolled at MITCS, terminated employees, and contractors/vendors with expired contracts or who are terminated are properly removed from MITCS's system in a timely manner.
- Analyzing the impact of proposed program changes in relation to other critical business functions before adopting the proposed program changes.
- Developing compensating controls to mitigate IT weakness and alert MITCS to unauthorized changes to student data, i.e. reconciliations to manual records, analysis of student trends, data entry procedures and review, etc.

Vendors

If MITCS shares internal sensitive or legally/contractually restricted MITCS data with parties outside the MITCS community, MITCS shall first enter into a Non-Disclosure Agreement with the party. The Non-Disclosure Agreement is needed to protect MITCS's proprietary or otherwise sensitive information. Non-Disclosure Agreements are typically needed when entering into a business relationship with vendors, consultants and contractors. All Non-Disclosure Agreements must be reviewed by MITCS's legal counsel before signing.

All vendors, consultants and/or contractors shall only be granted access to MITCS's Technology Resources to make changes or updates with prior written authorization from the CEO or his/her designee. Once the vendor, consultant and/or contractor, complete its work, access to MITCS's Technology Resources will be removed.

Vendors, consultants and contractors are required to assign unique user IDs and passwords to each of their employees authorized to access MITCS's system. Vendors, consultants and/or contractors may be terminated for violating this Policy and/or violating any state or federal laws.

All vendors, consultants and/or contractors and their employees who have direct contact with students must comply with the mandatory background check requirements for federal and state criminal history and child abuse. An official child abuse clearance statement for each of the vendors', consultants' and/or contractors' employees shall be submitted to MITCS prior to beginning employment with MITCS. Failure to comply with the background check requirements shall lead to immediate termination.

Closed Forum
MITCS's Technology Resources are not a public forum for expression of any kind and are to be considered a closed forum to the extent allowed by law.

All expressive activities involving MITCS Technology Resources that students, parents/guardians and members of the public might reasonably perceive to bear the approval of MITCS and that are designed to impart particular knowledge or skills to student participants and audiences are considered curricular publications. All curricular publications are subject to reasonable prior restraint, editing and deletion on behalf of MITCS for legitimate educational reasons. All other expressive activities involving MITCS's technology are subject to reasonable prior restraint and subject matter restrictions as allowed by law and Board of Trustees policies.

Records Retention
MITCS personnel shall establish a retention schedule for the regular archiving or deletion of data stored on MITCS Technology Resources that complies with MITCS's Record Retention and Destruction Policy as well as all Federal and Pennsylvania state laws and regulations. It is the User's responsibility to know which records are subject to these conditions and to comply with these laws and regulations or to contact the CEO for clarification.

In the case of pending or threatened litigation, MITCS's attorney will issue a litigation hold directive to the CEO or his/her designee. A hold directive will direct all MITCS administration and staff not to delete or destroy any electronic mail or other documentation on a computer as related to a specific student, employee, issue and/or for a specific time period. Failure to follow such a directive could result in negative legal consequences for the User and/or within the actual or threatened litigation. The litigation hold directive will override any records retention schedule that may have otherwise called for the transfer, disposal or destruction of relevant documents until the hold has been lifted by MITCS's attorney.

E-mail and computer accounts of separated employees that have been placed on a litigation hold will be maintained by MITCS until the hold is released. No employee, who has been so notified of a litigation hold, may alter or delete any electronic record that falls within the scope of the hold. Violation of the hold may subject the individual to disciplinary actions, up to and including termination of employment, as well as personal liability for civil and/or criminal sanctions by the courts or law enforcement agencies.

Damages
All damages incurred by MITCS due to a User's intentional or negligent misuse of MITCS's Technology Resources, including loss of property and staff time, may be charged to the User. MITCS administrators have the authority to sign any criminal complaint regarding damage to MITCS technology.

No Warranty/No Endorsement
MITCS makes no warranties of any kind, whether expressed or implied, for the services, products or access it provides.

The electronic information available to students and staff on the Internet or through web-based services does not imply endorsement of the content by MITCS, with the exception of resources approved and adopted by the Board of Trustees. Nor does MITCS guarantee the accuracy of information received using MITCS's Technology Resources.

MITCS is not and shall not be responsible for the loss of data, delays, non-deliveries, mis-deliveries or service interruptions. MITCS is not and shall not be responsible for any information that may be damaged or unavailable when using MITCS Technology Resources or for any information that is retrieved via the Internet. MITCS is not and shall not be responsible for any damages incurred as the result of using MITCS's Technology Resources, including but not limited to, the loss of personal property used to access Technology Resource. Further, MITCS is not and shall not be responsible for any unauthorized charges or fees resulting from access to the Internet or other commercial online services.

Unauthorized Disclosure of Information of Minors
It is a violation of state laws, including, but not limited to Chapter 12 of Title 22 of the Pennsylvania Code, FERPA and all other federal laws and regulations, to access data of a student the User does not have a legitimate educational interest in or to disclosure information about a student without parental permission or absent an exception to the disclosure requirements. Access and distribution of student data is recorded.

Questions regarding the disclosure of student information must be directed to the CEO prior to disclosure and must conform to MITCS's student records and confidentiality policies. Unauthorized disclosure, use and dissemination of personal information regarding minors is prohibited.

Compliance with Applicable Laws and Licenses
In their use of Technology Resources, Users must comply with all software licenses/copyrights and all other state, federal, and international laws governing intellectual property and online activities. Users shall not copy and distribute copyrighted material (e.g., software, database files, documentation, articles, graphics files, and downloaded information) through the e-mail system or by any other means unless it is confirmed in advance from appropriate sources that MITCS has the right to copy or distribute the material. Failure to observe a copyright may result in disciplinary action by MITCS, as well as legal action by the copyright owner. Any questions concerning these rights should be directed to the CEO or his/her designee.

Violations of Acceptable Technology Usage Policies and Procedures
Use of Technology Resources and equipment in a disruptive, manifestly inappropriate or illegal manner impairs MITCS's mission, squanders resources and shall not be tolerated. Therefore, a consistently high level of personal responsibility is expected of all Users granted access to MITCS's Technology Resources. Any violation of MITCS policies or procedures regarding technology usage may result in temporary, long-term or permanent suspension of user privileges. User privileges may be suspended pending investigation into the use of MITCS's Technology Resources and equipment.

Employees may be disciplined or terminated, and students suspended or expelled, for violating this Policy. Any attempted violation of MITCS's policies or procedures, regardless of the success or failure of the attempt, may result in the same discipline or suspension of privileges as that of an actual violation.

Consequences for Inappropriate Use
MITCS Users shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts. Illegal use of MITCS Technology Resources includes, but is not limited to: intentional copying, deletion or damage to files or data belonging to others; copyright violations; or theft of services. Any illegal usage of MITCS Technology Resources will be immediately reported to the appropriate legal authorities for possible prosecution.

General rules for behavior and communications apply when using the Internet or any MITCS Technology Resource. Suspension of access, loss of access and other disciplinary actions may be consequences for inappropriate use. Vandalism may result in cancellation of access privileges, discipline and possible criminal action.

Cessation of Access
Upon termination or ending of enrollment, employment or the termination of any contract with or from MITCS, no further access to or use of Technology Resources is permitted without the express authorization from the CEO.

Education of Technology Resource Users
MITCS shall implement a program which educates students and staff about acceptable use and internet safety associated with MITCS's Technology Resources. All students must complete a designated Technology Resources and Internet training prior to unsupervised use of MITCS's Technology Resources as required by the 2008 Broadband Data Improvement Act. This training includes, but is not limited to: appropriate online behavior, including interacting on social networking websites and in chat rooms; cyberbullying awareness and response; proper use of Technology Resources; restricted activities with Technology Resources; and access and monitoring of school-issued Technology Resources to students.

No Additional Rights
This Policy is not intended for and does not grant Users any contractual rights. Users of MITCS's Technology Resources must review this Policy closely and sign and return to MITCS a form acknowledging receipt and acceptance of the terms in this Policy, which is attached here to Venue for any legal action arising out of an alleged and/or actual violation of the attached Agreement (s) shall be in Beaver County, Pennsylvania.