Greater Altoona CTC
Information Technology Acceptable Use Policy

What is an ITAUP?

The Information Technology Acceptable Use Policy ("ITAUP") is a written agreement, between GACTC and its students and staff, whose purpose is to identify permissible and prohibited uses of Information Technology while at school and during all school-sponsored activities. More simply, it is a basic set of ground rules for a user's use of Information Technology.

Why Does GACTC Need an ITAUP?

The Internet is a boundless source of detailed, current information that can enhance a user's productivity. The Internet also allows access to a vast amount of purely entertainment-related features. Providing access to the Internet carries the same potential for productivity drain as placing a television on every user's desk.
Many Internet sites offer unrestricted access to pictures, video, sound, and text that is sexually oriented. There is no educational reason for such material to be brought into the school, and its presence impairs the school's educational programs. Both state and federal law prohibit the viewing of obscene material, child pornography and other material that is harmful to minors on school Internet systems.

Financial and Technological Reasons for Implementing an ITAUP

Restricting use of Information Technology to school-related matters serves to prevent a drain on limited computer resources caused by frivolous or improper use. Access to the Internet costs the school money in fees to Internet Service Providers, and in hardware costs necessary to accommodate increased network traffic and data storage.

A user's inappropriate use of Information Technology may negatively affect other users' speed of access or storage space for work product. An ITAUP can guide users concerning the use of storage space and bandwidth on the system to ensure maximum utility to all users. Examples of restrictions serving this interest would be directives against downloading music, games, movies, personal e-mail or other non-school related files, as well as restrictions on downloading large files that can be obtained offline, and instructions to move old or seldom used files, programs or e-mail to alternative storage.

ELECTRONIC ACCESS POLICY

I. GENERAL

The Greater Altoona Career and Technology Center provides most users with electronic access, a network connection, and/or Internet/Intranet access. This policy governs all use of the School's network, Internet/Intranet access, and e-mail system at all locations. This policy applies to all information technology resources, including but not limited to, electronic mail, chat rooms, instant messaging, the Internet, news groups, electronic bulletin boards, the School's Intranet and all other Information electronic messaging systems.

II. DEFINITIONS

Child pornography – Any photograph, film, audio, video or other visual depiction involving a minor engaging in sexually explicit conduct.

Harmful to Minors – Any picture, image, graphic image file or other visual depiction that: (1) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion; (2) depicts, describes, or represents, in a patently offensive way with respect to what is suitable to minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted acts, or lewd exhibition of the genitalia; and (3) taken as a whole, lacks serious literary, artistic, or scientific value as to minors.

Obscenity – Any material or performance, if: (1) the average person applying contemporary community standards would find that the subject matter taken as a whole appeals to the prurient interest; (2) the subject matter depicts or describes in a patently offensive way, sexual conduct of a type described in this section; and (3) the subject matter, taken as a whole, lacks serious literary, artistic, political, educational or scientific value.

Information technology resources – Any tool or medium used for computing or communications that may include but is not limited to: computers, personal digital assistants, hand held micro-computer devices, the Internet, local and wide area networks, intranet and extranet, e-mail systems, fileservers, wireless systems, text paging systems, phone systems.

User – Any member of staff or student body using information technology resources. This term also includes school visitors and others connecting temporarily to the school's communication network.

NETWORK AND INTERNET POLICY

III. INTERNET SAFETY AND ACTIVE RESTRICTION MEASURES

In accordance with the federal Children's Internet Protection Act ("CIPA") and Act 197 of 2004, GACTC utilizes technology protection measures including web content and SPAM filtering to prevent user access to or receipt of obscene, pornographic, or sexually explicit material or material which is harmful to minors. The School strictly enforces the use of this filtering technology during all network and Internet use. Overriding blocked Internet or e-mail content is the sole responsibility of the School's Technology Director in consultation with the Executive Director. Users are prohibited from any attempt to override the established safeguards. Attempts to circumvent the School's filtering system will be viewed in the same way as deliberately visiting prohibited sites.

Due to the dynamic nature of the Internet there may be sites that are not filtered by the school's Internet content filter. Internet content and SPAM filters by their very nature are not 100% effective and users may encounter objectionable content or SPAM when using the school's Internet connection or e-mail system. Users must take responsibility for their use of the computer networks and Internet and avoid sites containing objectionable content that are unfiltered. If a user unintentionally accesses a site containing objectionable content, the user is required to exit the site, and, if a student, immediately advise the instructor.

Further Specific Provisions For Internet Safety

All prudent measures are taken to establish appropriate filtering of incoming and outgoing Internet traffic through the use of a border firewall designed for that purpose. That firewall employs a commercial filtering table that is updated by subscription to an appropriate service along with manual updating of the local filtering table by technology staff as deemed locally appropriate.

Teachers and other personnel who assist in the instructional function are required to closely supervise and monitor the activity of students using the Internet under their supervision. Students may never be granted unsupervised time in the use of the Internet.

Teachers are required to provide two Internet safety lessons annually to all of their students. The lesson must be appropriate to students' Internet activity and must be documented by content, time spent in delivery, and specific date of instruction. These lessons will serve to educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms as well as increasing cyberbullying awareness and appropriate response.

A link is provided on the GACTC's Internet site to resources related to Internet Acceptable Use Policy for the reference of students, parents, teachers, and other interested parties. Included under that link is information concerning how students can report cyberbullying along with a copy of this policy for parents' information.

Any activity in which a user is tormented, threatened, harassed, humiliated, embarrassed, or otherwise targeted by another user involving the Internet, interactive and digital technologies, or mobile phones is strictly prohibited. Such activity involving only minors is considered to be cyberbullying. If an adult becomes involved, the activity becomes cyberstalking. Students who are the target of such activity are encouraged to report it to a teacher or other school officials. An employee who is targeted is encouraged to report to his or her supervisor. All instances of cyberbullying or cyberstalking that come to the attention of school authorities either by report of victim or by other means will be fully investigated. All criminal activity or suspected criminal activity will be reported to the police or other legal authority with full cooperation in investigation. All GACTC employees or its agents are required to report suspected instances of cyberbullying or cyberstalking to their immediate supervisor at the earliest opportunity.

IV. PERSONAL RESPONSIBILITY

By accepting a user account and password, and accessing the School's Network or Internet system, a user agrees to adhere to the School's policies regarding their use. The user also agrees to report any misuse or policy violation(s) (including the reception of inappropriate materials) to your instructor, if a student, or the School's Technology Director.

V. PERMITTED USE AND TERM

Use of the Network and the Internet is a privilege, not a right. Use of Network and Internet access extends throughout a student's course of enrollment in an academic year, presuming the student does not violate the School's policies regarding Network, Internet or Intranet use. Student violations of this policy may result in the suspension of Network access including Internet and Intranet privileges and be subject to disciplinary measures up to expulsion and criminal prosecution.

VI. AVAILABILITY AND ACCESS

The School reserves the right to suspend access at any time, without notice, for technical reasons, possible policy violations, security or other concerns.

VII. CONTENT AND COMMUNICATIONS

The School, at its sole discretion, will determine what materials, files, information, software, communications, and other content and/or activity will be permitted or prohibited. Installing software from outside sources may introduce viruses to the entire system or corrupt computer software and is strictly prohibited. **Users may never install or attempt to install any software on school computers unless specifically authorized.**

VIII. PRIVACY

Network and Internet access is provided as a tool for educational and instructional purposes. The School reserves the right to monitor, inspect, copy, review, and store at any time, without prior notice, any and all usage of the Network and the Internet, as well as any and all materials, files, information, software, communications, and other content transmitted, received or stored in connection with this usage. All such information, content, and files are the property of the School. A user should have no expectation of privacy regarding them. School officials may review files and intercept communications for any reason, including but not limited to maintaining system integrity and ensuring users are using the system consistently with this Policy.

IX. DOWNLOADED FILES

Files may not be downloaded from the Internet without prior authorization. Any files authorized for download from the Internet must be scanned with virus detection software before being opened. Users are reminded that information obtained from the Internet is not always reliable and should be verified for accuracy before use.

X. CONFIDENTIAL INFORMATION

Users should not transmit confidential information through the School Internet and e-mail systems without first receiving authorization from school officials.

XI. PROHIBITED ACTIVITIES

Users are prohibited from using the School's e-mail system, network, or Internet/Intranet access for the following activities:

- Downloading software without the prior written approval of the School's Technology Director.
- Downloading, printing, or distributing copyrighted materials. This includes, but is not limited to, software, articles and graphics protected by copyright.
- Using software that is not licensed by the manufacturer or approved by the School.
- Sending, printing, or otherwise disseminating the School's proprietary data or any other

information deemed confidential by the School to unauthorized persons.

- Operating a business, soliciting money for personal gain or otherwise engaging in commercial activity outside the scope of the classroom.
- Making offensive or harassing statements based on race, color, religion, national origin, veteran status, ancestry, disability, age, sex, or sexual orientation.
- Sending or forwarding messages containing defamatory, obscene, offensive, or harassing statements; or any form of electronic bullying. A student is expected to notify his/her instructor and/or Principal immediately upon receiving such a message. This type of message may not be forwarded.
- Sending or forwarding a message that discloses personal information without School authorization. This shall also include accessing, transmitting, receiving, or seeking confidential information about fellow users without authorization.
- Sending ethnic, sexual-preference or gender-related slurs and/or jokes via e-mail.
- Sending or soliciting sexually oriented messages or images.
- Attempting to access or visit sites featuring pornography, terrorism, espionage, theft, or drugs.
- Gambling or engaging in any other criminal activity in violation of local, state, or federal law.
- Gaining, or attempting to gain, unauthorized access to computer files, data, or computer systems inside or outside of the School's network. This conduct is commonly known as "hacking" and is strictly prohibited.
- Participating in activities, including the preparation or dissemination of content, which could damage the School's professional image, reputation, record maintenance system, and/or have adverse financial consequences for the School.
- Permitting or granting use of an e-mail or system account to another employee or persons outside the School. Permitting another person to use an account or password to access the Network or the Internet, including, but not limited to, someone whose access has been denied or terminated, is a violation of this policy.
- Using other students' or employees' passwords or impersonating another person while communicating or accessing the Network or Internet.
- Introducing a virus, harmful component, corrupted data or the malicious tampering with any of the School's computer systems or files.
- Users are prohibited from employing any kind of service that requires connection to other computers or servers on the Internet such as weather services, Web Shots, and instant messaging services without prior authorization.
- Users are not permitted to reconfigure their computers without proper authorization.
- No computer or computer-related device may be moved from its location in the building or taken from the building without the permission of the School's administration.
- No network devices including, but not limited to, computers, PDA's, flash drives, and wireless access devices may be connected to the School's network without the specific authorization of administration.

XII. COMPUTER EQUIPMENT

The following protocols are designed to reduce repair costs, maintain the integrity of our system and protect the School's assets. Users are expected to adhere to the following:

- Do not keep liquids or magnets on or near the computer.
- Do not remove any computer from the building without written permission from your instructor or principal.
- Do not transport disks back and forth between home and office. This will help minimize exposure to viruses. If this is imperative to the completion of your job, users are to

coordinate this process with the user support technician within their building to ensure the home computer is adequately protected from viruses or other malicious code.

- Users are responsible for such routine computer maintenance activities as monitoring anti-virus software and performing Microsoft Updates.

E-MAIL

XIII. E-MAIL POLICIES AND PROCEDURES

The School e-mail system is designed to improve the education and training of users who need it as part of their schooling. Users requiring the use of the School's e-mail system must adhere to the following policies and procedures:

- The School's e-mail system, network, and Internet/Intranet access are intended for instructional or administrative use only. Users may access e-mail (if required) and the Internet for educational purposes only. Access to e-mail for personal or recreational use is strictly prohibited.
- All information created, sent, or received via the School e-mail system, network, Internet, or Intranet, including all e-mail messages and electronic files, is the property of the Greater Altoona Career and Technology Center and is archived in its entirety in compliance with all local, state, and federal laws and regulations. Users should have no expectation of privacy regarding this information. The School reserves the right to access, read, review, monitor and copy all messages and files on its computer systems at any time and without notice. When deemed necessary, the School reserves the right to disclose text or images to law enforcement agencies or other third parties without the user's consent.
- Any message or file sent via e-mail must have the user's name attached.
- Creating or accessing personal e-mail accounts is not permitted at school. Personal e-mail accounts being: accounts created for the sole purpose of personal use for users, employees, family or friends.
- Alternate Internet Service Provider connections to the School's internal network are not permitted.
- Confidential information should not be sent via e-mail. This includes the transmission of financial information, Social Security numbers, education records, or other confidential material.
- Users must provide the System Administrator and/or Technology Coordinator with all passwords when requested.
- Only authorized school personnel are permitted to access another person's e-mail without consent.
- Users should exercise sound judgment when distributing messages. Users must also abide by copyright laws, ethics rules, and other applicable laws.
- E-mail messages must contain professional and appropriate language at all times. Users are prohibited from sending abusive, harassing, intimidating, threatening, and discriminatory or otherwise offensive messages via e-mail. Sending abusive, harassing, intimidating, threatening, discriminatory, or otherwise offensive messages via e-mail will result in disciplinary action up to and including expulsion.
- Use of the School's e-mail system for solicitations for any purpose, personal or otherwise, without written permission of the authorized Administration is strictly prohibited.
- E-mail containing offensive subjects that elude email filters must be promptly deleted from the user's inbox and from "deleted items".
- Users are responsible to archive messages to prevent their being automatically deleted.

All messages archived in the School's computer system shall be deemed School property, as is all information on the School's systems. Users are responsible for knowing the School's e-mail retention policies which are established and maintained according to prevailing law

- Misuse and/or abuse of electronic access, including but not limited to personal use, copying or downloading copyrighted materials, visiting or attempting to visit pornographic sites, sending or participating in abusive e-mail messages, or any other violation of the provisions of this policy will result in disciplinary action, up to and including expulsion, termination of employment, and criminal prosecution.

XIV. PORTABLE COMPUTERS AND SIMILAR DEVICES

Users will be issued laptop computers and/or other portable computer-like devices based upon need. These devices may be issued on a continuing or temporary basis. The devices remain the property of the GACTC and are regulated under the following considerations:

- The user assumes responsibility for the security of the device and is required to take prudent measures to protect the device from theft and damage.
- Portable devices shall be returned to the custody of the GACTC during the summer break unless other arrangements have been made.
- The user may take the device home and to other locations necessary for the performance of the user's professional responsibilities.
- The device may not be used for personal activities or by anyone other than the person to whom the device is issued.
- All other provisions of this Information Technology Acceptable Use Policy apply to portable devices.

XV. COMPLIANCE

Though each individual is responsible for his/her own actions, management personnel are responsible for ensuring student and employee compliance with this policy. Any employee aware of a policy violation is expected to immediately report the violation to his/her supervisor, the School's Technology Director, instructor and/or the principal.

XVI. NONCOMPLIANCE

Violation of these policies will result in disciplinary action up to and including expulsion and termination of employment.

XVII. SUPERVISORY RESPONSIBILITY

All staff members having responsibility for students who are using computers are required to take every reasonable measure to enforce compliance with the Information Technology Acceptable Use Policy. Particular considerations in supervision are:

- Computer screen displays should be directed to be in easy view of the teacher or instructional assistant.
- All student activity on computers must have an educational purpose.
- Students may not be permitted free time to play games or surf the Internet unless clear educational purpose can be demonstrated.

SOFTWARE USAGE POLICY

XVII. SOFTWARE USAGE POLICIES AND PROCEDURES

Software piracy is both a crime and a violation of this policy. Users are required to use software strictly in accordance with its license agreement. Unless otherwise provided in the license, the duplication of copyrighted software (except for backup and archival purposes by designated school personnel) is a violation of copyright law. In addition to being in violation of the law, unauthorized duplication of software is contrary to the School's standards of employee conduct. To ensure compliance with software license agreements and the School's Software Usage Policy, employees must adhere to the following:

1. Users must use software in accordance with the manufacturer's license agreements and the School's Information Technology Acceptable Use Policy. The School licenses the use of computer software from a variety of outside companies. The School does not own the copyright to software licensed from other companies. Users acknowledge they do not own software or its related documentation. Users may not make additional copies of software media unless expressly authorized by the software publisher. The only exception will be a single copy, as authorized by designated school personnel, for backup or archival purposes. Students and employees may not maintain backup software unless directed to do so.

2. The School does not condone and prohibits the unauthorized duplication of software. Users illegally reproducing software will be subject to disciplinary action. In addition, users illegally reproducing software may be subject to civil and criminal penalties including fines and imprisonment.

NOTE: *Unauthorized reproduction of software is a federal offense under US and Canadian copyright laws. In the United States, violators may be subject to civil damages in amounts up to $150,000 per title copied. Criminal penalties include fines as high as $250,000 per software title copied, and imprisonment of up to 5 years.*

3. Any user who knowingly makes, acquires, or uses unauthorized copies of computer software licensed to the School, or who places or uses unauthorized software on the School's premises or equipment shall be subject to disciplinary action, up to and including expulsion, termination, and prosecution.

4. Users are not permitted to install their personal software onto the School's computer system. Users are not permitted to copy software from the School's computer system for installation on home or other computers.

5. In cases that require a user to use software at home, the School will provide an additional copy or license. Any user issued additional copy(s) of software for home use acknowledges that such additional copy(s) or license(s) purchased for home use are the property of the School. Users who are required to use software at home should consult with their instructor or Principal to determine if appropriate licenses allow for home use.

6. Users are prohibited from giving software to other users or persons outside of the School. Under no circumstances will the School use software from an unauthorized source, including, but not limited to, the Internet, home, friends and/or peers.

7. Users who have reasonable suspicion of software misuse are required to notify their instructor, Principal or Technology Director.

8. All software used on School-owned computers will be purchased through appropriate

procedures. Consult your instructor, Principal or Technology Director for proper procedures.

SOCIAL MEDIA POLICY

XIX. PURPOSE

The GACTC recognizes the ubiquity of Social Networking in personal and professional communications. This policy addresses employees' use of such networks, including: personal websites, web logs (blogs), wikis, social networks, online forums, virtual worlds, and any other kind of social media.

The GACTC takes no position on employees' decisions to participate in social media such as that described above, and is cognizant of the constitutional protections afford to employees speaking as private citizens on matters of public concern. However, employees are reminded that they are professionals and are representatives of the GACTC and the community in all aspects of their lives. At all times, including the course of communications via social media, employees should conduct themselves publicly in accordance with the responsibilities of public service. This policy is intended to assist the employee in making good decisions when communicating and obtaining information online in accordance with GACTC policy.

XX. GUIDELINES.

1. Interaction with Students through Blogs and Social Networking

   Employees are required to maintain a professional relationship with their students at all times and are prohibited from becoming friends and/or communicating with students via personal accounts on social media networks. Further, employees shall not engage students on either the employee's or the student's blog or social networking page regarding any other matter. Employees shall not participate in student social networking group pages or utilize these pages to communicate with students in a personal capacity.

   Only school-sponsored websites, wikis, email addresses or other GACTC-sponsored means should be utilized for communications with students and/or parents. In the event an employee receives a communication or request from a student or parent addressed to the employee's personal account, the employee should respond via other means that are GACTC-sponsored.

2. Identification and Authorship

   The GACTC encourages employees to be honest about their identity when utilizing social media. Tracking tools enable supposedly anonymous posts to be traced back to their authors. Employees should not pretend to be another person in order to pursue personal communications or agendas, and are prohibited from doing so when communicating about GACTC matters of private or internal concern regarding the GACTC, its staff, students or operations.

   Employees are prohibited from acting as a spokesperson for the GACTC or posting comments as a representative of the GACTC without express written consent. Any employee who chooses to identify him or herself as a GACTC employee on any social media network or offers any comment on any topic related to the GACTC, while on any social media network, is directed to include a disclaimer providing that follows:

"The views expressed [in the social media format] are mine alone and do not necessarily reflect the views of the Greater Altoona Career and Technology Center."

3. Monitoring and Liability

Employees should understand the public nature of the Internet and should understand that the GACTC is free to view and monitor employees' public websites, blogs, or other public internet communications at any time, without consent from the author of such communications. Furthermore, as representatives of the GACTC, employees are reminded that students, parents, and other partners of the GACTC community are able to view any public communication or private social media communication made accessible to them by GACTC employees.

Social media users may be held responsible and subject to discipline for commentary that references the GACTC, its staff, students, or operations in an inappropriate or illegal manner. In general, social media users should further be aware that they may incur liability arising from commentary deemed to be proprietary, copyrighted, defamatory, libelous, or obscene (as defined by law).

Social media users should take responsibility and monitor their own social media applications in order to review and approve any and all comments before they appear. This allows the employee to delete any spam comments, block inappropriate posts, and delete any offensive or frivolous comments.

Employees should not permit students to comment on their personal social networking page or on their blog.

4. Prohibited Conduct

Employees are hereby advised that any and all GACTC-related information published by the employee on their blog or social networking sites must comply with the GACTC's Acceptable Use and Personal Conduct Policies. Further, the employee must comply with confidentially obligations imposed by law, including HIPAA and FERPA. Employees must respect all copyright laws and must reference or cite all sources as required by law. Under no circumstances may the employee use GACTC logos, mascots, or images on a personal social media account, profile, site, or blog without express written consent. The use of images or photographs of students on a personal blog or social networking webpage is absolutely prohibited.

Under no circumstances shall employees discuss situations involving employee or student discipline on social media networks or sites. As a general guideline, employees should not post anything that they would not want to read in a newspaper or on a billboard.

Employees shall not use the GACTC's name to promote or endorse any product, cause, or political party or candidate.

5. Conduct in the Use of Social Media

Under no circumstances shall the use of social networking activities interfere with the employee's work obligations.

Employees should be aware that even privacy settings are not fool-proof. Search engines can turn up posts and pictures years after they have been published to the internet. It is recommended that employees keep their status as professionals and representatives of the GACTC in mind at all times when communicating via social media.

Employees should use care in posting or publishing photos of themselves. Only pictures that they would be comfortable sharing with the parents of GACTC students or their employer should be posted.

Employees should monitor pictures posted by their friends to ensure that a search for the employee's name does not bring up inappropriate or unauthorized images of the employee.

6. Discipline under this Policy

Violation of this policy will result in discipline as appropriate, up to and including termination, in accordance with all applicable GACTC disciplinary policies and procedures.

Employees will be held responsible for the disclosure, whether purposeful or inadvertent, of confidential or proprietary information, information that violates the privacy rights of others.

Exceptions to this policy may be recognized in instances where employees' speech is made as a private citizen, on matters of purely public concern, where appropriate.

7. Preservation and Compliance with Applicable Law

Nothing in this policy shall be interpreted in a manner that violates an employee's civil or other rights as set forth in state and federal law.

ACKNOWLEDGMENT OF UNDERSTANDING

XXI. Electronic Access Policy Acknowledgment of Receipt and Understanding

I hereby certify that I have read and fully understand the contents of the Information Technology Acceptable Use Policy. Furthermore, I have been given the opportunity to discuss any information contained therein or any concerns that I may have. I understand that my access to the School's technology resources is based upon my willingness to abide by and follow the School's policies, rules, regulations and procedures. I acknowledge that the Greater Altoona Career and Technology Center may modify or amend this policy at any time, and notice of these changes will be provided. This policy does not create any promises or contractual obligations between GACTC and its users regarding the use of the School's technology resources. My signature below certifies my knowledge, acceptance and adherence to GACTC's policies, rules, regulations and procedures regarding the Information Technology Acceptable Use Policy.

Category of User:
Student _____
Instructor _____
Staff _____
Temporary _____ Dates of use: _____

Signature _____ Date _____

Print Name _____