



WILKES-BARRE AREA CAREER AND TECHNICAL CENTER

STUDENT ACCEPTABLE USE POLICY

Technology Resources, Digital Citizenship,
Cybersecurity, and Electronic Communications

Prepared By: Joe Oliveri, Director of Technology
Adopted: June 22, 2026

Table of Contents

Table of Contents	2
1. Purpose	3
2. Scope	4
3. Authorized Use and Student Expectations	5
4. Account and Credential Security	7
5. Privacy and Protected Information	8
6. Internet, Email, and Electronic Communications	9
7. Artificial Intelligence and Emerging Technologies	11
8. Personal Devices and BYOD	12
9. Network Access and Security	14
10. Software, Hardware, and Technology Restrictions	15
11. Monitoring and Privacy	17
12. Prohibited Activities	19
13. Incident Reporting and Cybersecurity Responsibilities	20
14. Violations and Disciplinary Action	22
15. Administrative Authority and Policy Review	23
16. Acknowledgment	25

1. Purpose

The Wilkes-Barre Area Career and Technical Center ("WBACTC" or "the CTC") provides students with access to technology resources, network systems, internet services, cloud-based applications, communication platforms, instructional technology, and electronic devices to support education, career and technical training, communication, research, collaboration, and learning opportunities.

The purpose of this policy is to establish expectations for the responsible, ethical, safe, secure, and educational use of CTC technology resources while promoting digital citizenship, protecting the security and integrity of CTC systems, and supporting a positive learning environment.

This policy is intended to support:

- educational and instructional opportunities;
- responsible digital citizenship and online behavior;
- cybersecurity and data protection;
- student safety and privacy;
- protection and responsible care of CTC technology resources;
- compliance with applicable laws, regulations, and CTC policies; and
- the reliable operation of CTC technology systems and services.

Access to CTC technology resources is a privilege provided to support legitimate educational and school-related activities and may be limited, monitored, restricted, or revoked in accordance with this policy, administrative procedures, and applicable disciplinary requirements.

Students are expected to utilize CTC technology resources in a responsible, respectful, secure, and educationally appropriate manner consistent with the mission, educational objectives, and operational expectations of the CTC.

2. Scope

This policy applies to all WBACTC students and other authorized student users who access or utilize CTC technology resources, systems, networks, devices, accounts, applications, or internet services.

This policy applies to all CTC technology resources and systems, including but not limited to:

- desktop computers;
- laptops and Chromebook devices;
- mobile devices and tablets;
- classroom and instructional technology;
- computer laboratories and shop technology systems;
- Chromebook carts and shared device environments;
- audiovisual and presentation systems;
- wireless networks;
- internet access services;
- email and messaging systems;
- Google Workspace and other cloud-based platforms;
- learning management systems;
- student information systems;
- remote learning systems and communication platforms;
- authentication and login systems;
- shared storage systems;
- printers and peripheral devices;
- security-related technology systems; and
- any future technology systems or services owned, leased, managed, or operated by the CTC.

This policy applies to:

- technology resources utilized on CTC property;
- technology resources utilized during remote learning or off-campus educational activities;

- personally owned devices used to access CTC systems, accounts, applications, networks, or services;
- school-issued or assigned student devices;
- shared classroom or laboratory technology resources; and
- CTC technology resources accessed through third-party internet connections or external networks.

Students are responsible for complying with this policy whether access occurs:

- during school hours or school-related activities;
- on or off CTC property;
- through school-issued devices;
- through personally owned devices;
- through shared classroom or laboratory devices; or
- through remote access, cloud-based platforms, or internet-connected systems.

Students may also be held responsible for damage, misuse, vandalism, theft, loss, unauthorized modification, or improper handling of CTC technology resources assigned to them, utilized under their supervision, or accessed through their accounts or credentials in accordance with applicable CTC policies and administrative procedures.

3. Authorized Use and Student Expectations

CTC technology resources are provided to support approved educational, instructional, career and technical training, research, communication, collaboration, and school-related activities consistent with the mission and educational objectives of the CTC.

Students are expected to use CTC technology resources in a responsible, respectful, safe, secure, ethical, and educationally appropriate manner. Technology use must support classroom instruction, assigned coursework, program requirements, and other CTC-approved activities.

All use of CTC technology resources must comply with:

- applicable laws and regulations;
- CTC policies, rules, procedures, and the Student Code of Conduct;
- teacher, administrator, and technology staff directions;

- software licensing and copyright requirements;
- cybersecurity and data protection expectations;
- student privacy and safety requirements; and
- responsible digital citizenship expectations.

Students are expected to:

- use technology resources only for authorized educational or school-related purposes;
- follow directions from teachers, administrators, and technology staff regarding the use of devices, accounts, networks, systems, and applications;
- use respectful and appropriate language, behavior, and communication when using technology resources;
- respect the rights, privacy, property, and work of other users;
- protect assigned, shared, or accessed technology resources from damage, loss, theft, misuse, or unauthorized modification;
- handle Chromebooks, laptops, desktop computers, monitors, keyboards, mice, chargers, carts, cabling, printers, and other technology equipment responsibly;
- return shared devices and equipment to the proper cart, charging location, classroom, laboratory, shop, or assigned storage area as directed;
- use only accounts, devices, files, systems, or applications they are authorized to access;
- promptly report damaged, missing, malfunctioning, or improperly used technology equipment to a teacher, administrator, or technology staff member;
- avoid activities that interfere with instruction, CTC operations, network performance, cybersecurity, or the rights of others; and
- comply with filtering, monitoring, classroom management, login, access, and security requirements.

Limited incidental personal use of CTC technology resources may be permitted only when authorized by CTC staff, does not interfere with instruction or CTC operations, does not violate this policy or other CTC rules, and does not compromise the security, integrity, or availability of CTC technology resources.

Access to CTC technology resources is a privilege, not a right. Access may be limited, monitored, restricted, suspended, or revoked when a student violates this policy, misuses technology resources, damages technology equipment, interferes with instruction or operations, or creates a safety, security, disciplinary, or operational concern.

4. Account and Credential Security

Student accounts, usernames, passwords, authentication methods, and access credentials issued or authorized by the CTC are intended only for use by the assigned student and for approved educational or school-related purposes.

Students are responsible for all activity conducted under their assigned accounts and credentials. Students are expected to protect their accounts, passwords, and access credentials from unauthorized use.

Students shall:

- maintain the confidentiality of passwords, authentication codes, and other access credentials;
- not share usernames, passwords, accounts, authentication codes, or login information with any other student or unauthorized individual;
- not use another student's account, staff account, or unauthorized account to access CTC technology resources;
- not allow another person to use their assigned account or credentials;
- log out, lock, or otherwise secure devices and accounts when finished using them or when leaving a device unattended;
- immediately report suspected unauthorized access, compromised passwords, suspicious login activity, or misuse of their account to a teacher, administrator, or technology staff member;
- comply with CTC login, authentication, password, and account security requirements; and
- use only authorized accounts and approved access methods when accessing CTC systems, networks, applications, or cloud-based services.

The use of unauthorized credential sharing, impersonation, password disclosure, phishing activity, or attempts to gain unauthorized access to systems, accounts, files, applications, or data is strictly prohibited.

Students shall not attempt to bypass, disable, interfere with, or circumvent authentication systems, login requirements, security controls, monitoring systems, filtering systems, or other cybersecurity protections implemented by the CTC.

The CTC reserves the right to restrict, suspend, disable, or revoke account access privileges at any time in response to policy violations, cybersecurity concerns, unauthorized activity, suspected account compromise, operational needs, or security risks.

5. Privacy and Protected Information

Students may have access to information, files, records, images, communications, or other data through CTC technology resources. Students are expected to respect the privacy, rights, and information of others when using CTC systems, devices, applications, and networks.

Protected or private information may include, but is not limited to:

- student names, addresses, phone numbers, or personal information;
- student educational records, grades, schedules, or assignments;
- health, discipline, or counseling-related information;
- usernames, passwords, or login information;
- files, documents, photos, videos, or communications belonging to another student, staff member, or the CTC;
- screenshots, recordings, or images captured from CTC systems or devices; and
- any other information that is not intended for public access or sharing.

Students shall:

- access only the files, accounts, systems, information, or data they are authorized to use;
- respect the privacy and work of other students, staff members, and CTC users;
- protect personal information from unauthorized sharing, posting, or disclosure;
- use CTC systems and information only for approved educational or school-related purposes;
- promptly report accidental access to private, sensitive, or unauthorized information to a teacher, administrator, or technology staff member; and
- follow all teacher, administrator, and CTC directions regarding the use, sharing, or submission of digital information.

Students shall not:

- access, view, copy, change, delete, photograph, screenshot, record, share, or distribute another person's files, information, account activity, grades, communications, or personal information without authorization;
- use another person's login, device, account, or files to access private or protected information;
- post, send, upload, or share private information, images, recordings, screenshots, or communications without authorization;
- attempt to access student records, staff files, administrative systems, grade information, or other protected CTC information without authorization; or
- use personal email, personal cloud storage, messaging apps, social media, or other unauthorized services to store, send, or share private or protected information obtained through CTC technology resources.

The CTC may monitor, review, inspect, retain, or investigate the use, access, transmission, storage, or sharing of information through CTC technology resources in accordance with applicable laws, policies, administrative procedures, and operational requirements.

6. Internet, Email, and Electronic Communications

CTC-provided internet access, email accounts, communication platforms, cloud-based services, and electronic communication tools are provided to support approved educational, instructional, career and technical training, communication, collaboration, and school-related activities.

Students may be provided access to CTC-issued accounts, sending school district accounts, Google Workspace, email, learning platforms, shared documents, cloud-based tools, and other electronic communication systems. Use of these systems must be responsible, respectful, safe, secure, and educationally appropriate.

Students are expected to:

- use internet access, email, messaging, shared documents, cloud platforms, and electronic communication tools only for approved educational or school-related purposes;
- communicate respectfully and appropriately with students, staff members, instructors, administrators, and other users;
- follow teacher, administrator, and technology staff directions regarding the use of internet resources, email, cloud platforms, and communication tools;

- use appropriate language, tone, and content in all electronic communications;
- exercise caution when opening attachments, clicking links, downloading files, or responding to unfamiliar or suspicious messages;
- promptly report suspected phishing attempts, threatening messages, inappropriate communications, suspicious links, or harmful content to a teacher, administrator, or technology staff member;
- respect copyright, intellectual property, privacy, and acceptable use expectations when accessing or sharing digital content; and
- comply with CTC filtering, monitoring, classroom management, cybersecurity, and communication requirements.

Students shall not:

- use CTC internet access, email, communication platforms, or cloud-based services for unlawful, threatening, harassing, bullying, cyberbullying, discriminatory, obscene, disruptive, or inappropriate purposes;
- send, post, share, forward, or distribute messages, images, videos, recordings, files, or content that are threatening, harassing, bullying, sexually explicit, obscene, discriminatory, harmful, or disruptive to the educational environment;
- impersonate another student, staff member, administrator, or other individual through email, messaging, shared documents, accounts, or electronic communications;
- use anonymous messaging services, unauthorized communication applications, personal email accounts, social media platforms, or unapproved external services in a manner that violates CTC rules, teacher directions, or this policy;
- record, photograph, screenshot, post, share, or distribute images, audio, video, communications, or classroom/shop/lab activity without authorization;
- access, distribute, or intentionally transmit malicious software, spam, chain messages, fraudulent messages, or harmful content;
- access or attempt to access websites, applications, games, services, or content that are blocked, restricted, or prohibited by the CTC; or
- attempt to bypass internet filtering, monitoring systems, classroom management systems, cybersecurity protections, or network restrictions through cellular data, personal hotspots, VPNs, proxy services, extensions, anonymizers, or other methods.

Electronic communications and internet activity conducted using CTC technology resources may be monitored, logged, retained, reviewed, restricted, or disclosed by the CTC in accordance with

applicable laws, policies, administrative procedures, operational requirements, and cybersecurity responsibilities.

Students should have no expectation of privacy regarding internet usage, email communications, electronic communications, files, documents, messages, or data created, transmitted, received, stored, or accessed using CTC technology resources, except as otherwise provided by law.

7. Artificial Intelligence and Emerging Technologies

The CTC recognizes that artificial intelligence (AI), generative AI tools, automated systems, and emerging technologies may support learning, creativity, research, productivity, and career and technical education when used appropriately and responsibly.

Students may use AI tools or emerging technologies only when permitted by a teacher, administrator, or CTC-approved instructional activity. AI use must support educational purposes and must comply with this policy, teacher expectations, academic integrity requirements, and the Student Code of Conduct.

Students are expected to:

- use AI tools only when authorized for an assignment, project, instructional activity, or school-related purpose;
- follow teacher directions regarding when and how AI tools may be used;
- disclose or identify AI-generated content when required by a teacher, assignment, or CTC procedure;
- review AI-generated content for accuracy, appropriateness, bias, and reliability before using or submitting it;
- understand that students remain responsible for the work they submit, even when AI tools are used;
- protect personal, private, confidential, or protected information when using online tools or external platforms; and
- use AI tools in a responsible, ethical, safe, and educationally appropriate manner.

Students shall not:

- submit AI-generated work as their own original work when such use is not authorized;

- use AI tools to cheat, plagiarize, avoid assigned work, or violate academic integrity expectations;
- input student records, personal information, private communications, images, login credentials, or other protected information into unauthorized AI systems or external platforms;
- use AI tools to create, alter, or distribute false, misleading, harmful, harassing, threatening, discriminatory, sexually explicit, obscene, or inappropriate content;
- use AI tools to impersonate another person or create fake images, audio, video, messages, documents, or communications involving students, staff, or the CTC;
- use AI tools to bypass CTC filtering, monitoring, cybersecurity protections, classroom management systems, or assignment requirements; or
- use AI tools in any manner that violates CTC policies, teacher directions, applicable laws, or the Student Code of Conduct.

The CTC reserves the right to restrict, monitor, review, approve, prohibit, or remove the use of AI tools, automated systems, or emerging technologies on CTC systems, accounts, devices, or networks in accordance with educational, operational, legal, cybersecurity, or administrative requirements.

8. Personal Devices and BYOD

The CTC may permit students to use personally owned devices, sending school district-issued devices, or other approved devices to access authorized CTC systems, applications, wireless networks, cloud platforms, instructional resources, or educational technology services when permitted by CTC administration, authorized staff, or instructional requirements.

Use of personally owned devices or sending school district-issued devices at the CTC must comply with this policy, the CTC Electronic Communication Device Policy, teacher directions, administrative rules, cybersecurity requirements, and the Student Code of Conduct.

Personal devices may include, but are not limited to:

- smartphones;
- tablets;

- laptops;
- smartwatches;
- earbuds or headphones;
- personally owned computers;
- hotspot-capable devices; and
- other personal technology devices.

Students are expected to:

- use personal or approved external devices only when authorized;
- follow all teacher, administrator, and technology staff directions regarding device use;
- connect only to authorized CTC networks or services when permitted;
- comply with CTC filtering, monitoring, classroom management, cybersecurity, and access requirements;
- use personal or sending school district-issued devices in a responsible, respectful, safe, and educationally appropriate manner;
- keep personal devices secured and under their control; and
- report lost, stolen, damaged, compromised, or improperly used devices when the issue involves CTC systems, networks, accounts, or instructional activities.

Students shall not use personal devices or sending school district-issued devices to:

- bypass CTC content filtering, monitoring systems, classroom management systems, cybersecurity protections, or network restrictions;
- access the internet through cellular data, personal hotspots, VPNs, proxy services, anonymizers, extensions, or other methods intended to avoid CTC rules or security controls;
- create unauthorized wireless networks, hotspots, network bridges, or external connections on CTC property or networks;
- record, photograph, livestream, screenshot, post, or share classroom, shop, lab, student, staff, or CTC activity without authorization;
- access, store, transmit, or share private, protected, inappropriate, or unauthorized information;
- interfere with instruction, CTC operations, network performance, cybersecurity protections, or the rights of others; or

- violate the CTC Electronic Communication Device Policy, this policy, teacher directions, administrative rules, or the Student Code of Conduct.

The CTC is not responsible for the loss, theft, damage, maintenance, technical support, compatibility, or personal data loss involving personally owned devices brought to the CTC or used during CTC-sponsored activities.

Use of sending school district-issued devices at the CTC may also be subject to the sending school district's rules, monitoring, filtering, device management, and acceptable use requirements. While used at the CTC or to access CTC systems, such devices are also subject to applicable CTC policies, rules, and directions.

The CTC reserves the right to restrict, limit, suspend, or revoke personally owned device access or external device access to CTC systems, networks, applications, or services at any time based upon instructional, operational, administrative, legal, safety, or cybersecurity requirements.

9. Network Access and Security

CTC networks, wireless services, internet access, cloud-based systems, and related technology resources are provided to support approved educational, instructional, career and technical training, communication, collaboration, and school-related activities.

Students may access CTC networks, systems, applications, and services only through authorized accounts, approved devices, and permitted access methods.

Students are expected to:

- use CTC networks and internet access only for approved educational or school-related purposes;
- follow all teacher, administrator, and technology staff directions regarding network access, wireless access, internet use, and online systems;
- connect only to authorized CTC networks or services when permitted;
- comply with CTC login, filtering, monitoring, classroom management, cybersecurity, and access requirements;

- immediately report suspicious network activity, unauthorized access, compromised accounts, or cybersecurity concerns to a teacher, administrator, or technology staff member; and
- use CTC network resources in a manner that does not interfere with instruction, operations, network performance, cybersecurity protections, or the rights of others.

Students shall not:

- attempt to access networks, systems, accounts, applications, files, or services they are not authorized to use;
- bypass, disable, interfere with, or attempt to circumvent network security protections, monitoring systems, filtering systems, firewalls, authentication systems, classroom management systems, or access controls;
- use unauthorized VPNs, proxy services, anonymizers, tunneling services, browser extensions, or similar tools to hide activity or bypass CTC restrictions;
- create or use unauthorized wireless networks, hotspots, network bridges, or external connections on CTC property or networks;
- scan, test, monitor, intercept, disrupt, or attempt to exploit CTC networks, systems, devices, applications, or services without authorization;
- connect unauthorized devices, equipment, or network hardware to CTC systems or infrastructure; or
- use CTC network access in a way that creates a safety, security, disciplinary, operational, or cybersecurity concern.

The CTC reserves the right to monitor, restrict, suspend, disable, or revoke network access, wireless access, internet access, account access, or related services at any time in accordance with instructional, operational, administrative, legal, safety, or cybersecurity requirements.

10. Software, Hardware, and Technology Restrictions

CTC technology resources, including computers, Chromebooks, carts, classroom technology, laboratory systems, shop technology, software, applications, networks, and related equipment, are provided to support approved educational and school-related activities.

Students may use only hardware, software, applications, systems, websites, browser extensions, and technology services that are authorized or permitted by the CTC, a teacher, administrator, or technology staff member.

Students are expected to:

- use CTC hardware, software, applications, and equipment only as directed;
- handle all technology equipment carefully and responsibly;
- keep devices, chargers, cables, monitors, keyboards, mice, printers, carts, and other equipment in proper working condition;
- return shared devices and equipment to the proper location when finished;
- report damaged, missing, malfunctioning, or improperly used equipment to a teacher, administrator, or technology staff member;
- follow all classroom, lab, shop, and cart-related technology expectations; and
- allow authorized technology staff to inspect, maintain, update, repair, inventory, secure, or manage CTC-owned technology resources.

Students shall not:

- intentionally damage, vandalize, misuse, hide, remove, or steal CTC technology resources;
- pull, cut, unplug, remove, damage, or tamper with cables, chargers, wires, wall plates, ports, keyboards, mice, monitors, computers, carts, printers, projectors, or other technology equipment;
- remove devices, chargers, peripherals, or equipment from classrooms, labs, shops, carts, or assigned areas without authorization;
- install, download, run, modify, or distribute unauthorized software, applications, games, browser extensions, utilities, scripts, or executable files;
- change system settings, device settings, network settings, security settings, management settings, or administrative controls without authorization;
- bypass, disable, remove, or interfere with security software, endpoint protection, web filtering, classroom management systems, device management systems, monitoring tools, or other CTC technology controls;
- connect unauthorized hardware, USB devices, storage devices, wireless devices, network equipment, or peripheral devices to CTC systems or networks;
- attempt to gain administrative access, elevated privileges, or unauthorized permissions on any CTC system, device, application, or account;

- use CTC technology resources for unauthorized gaming, streaming, downloads, file sharing, or other non-instructional activities;
- duplicate, copy, distribute, or use software, media, files, or digital content in violation of copyright, licensing, or intellectual property requirements; or
- use technology resources in any manner that creates a safety, security, instructional, operational, legal, or cybersecurity concern.

The CTC reserves the right to remove, disable, restrict, inspect, monitor, repair, replace, or prohibit any hardware, software, application, device, service, file, extension, or technology resource connected to or used within CTC systems or networks that presents an instructional, operational, legal, safety, disciplinary, or cybersecurity concern.

11. Monitoring and Privacy

CTC technology resources, including networks, accounts, devices, applications, internet access, email, cloud platforms, communication systems, classroom management systems, filtering systems, and related technology services, are provided to support approved educational and school-related activities.

To protect students, staff, CTC systems, instructional activities, cybersecurity, legal compliance, and the operational needs of the CTC, the CTC reserves the right to monitor, log, access, review, inspect, retain, investigate, restrict, disclose, or remove information, communications, files, records, internet activity, network activity, device activity, or other data created, transmitted, received, stored, or accessed using CTC technology resources.

Monitoring may include, but is not limited to:

- internet usage and browsing activity;
- email and electronic communications;
- cloud platform activity;
- files, documents, and shared content;
- device activity and security status;
- login and account activity;
- network traffic and connectivity activity;
- filtering and classroom management activity;

- cybersecurity monitoring and threat detection; and
- operational, safety, security, and system management activity.

Students should have no expectation of privacy when using:

- CTC-owned devices;
- CTC accounts or login credentials;
- CTC networks or Wi-Fi;
- CTC internet access;
- CTC email or communication systems;
- CTC cloud platforms or applications;
- CTC classroom management, filtering, or monitoring systems; or
- files, messages, documents, activity, or data created, transmitted, received, stored, or accessed using CTC technology resources, except as otherwise provided by law.

The CTC may access, review, disclose, preserve, or provide information related to CTC technology resources when necessary to:

- support instructional, operational, or administrative needs;
- investigate suspected policy violations, misconduct, unauthorized activity, damage, misuse, or cybersecurity incidents;
- comply with legal obligations, court orders, subpoenas, lawful requests, or administrative requirements;
- protect the safety, security, integrity, or operational continuity of CTC systems, users, devices, or services; or
- support maintenance, troubleshooting, auditing, inventory management, technology support, or administrative oversight.

Use of personally owned devices or sending school district-issued devices to access CTC systems, networks, accounts, applications, cloud services, or instructional resources may subject certain CTC-related activity, communications, records, or data to monitoring, logging, review, restriction, disclosure, or investigation in accordance with applicable laws, CTC policies, administrative procedures, and operational requirements.

12. Prohibited Activities

Students shall not use CTC technology resources in any manner that is unlawful, unauthorized, disruptive, harmful, unsafe, unethical, inappropriate, or inconsistent with the educational, operational, safety, or cybersecurity needs of the CTC.

Prohibited activities include, but are not limited to:

- accessing or attempting to access accounts, devices, files, systems, applications, networks, or information without authorization;
- sharing passwords, using another person's account, impersonating another person, or attempting to obtain another person's login information;
- bypassing, disabling, interfering with, or attempting to circumvent cybersecurity protections, filtering systems, monitoring systems, classroom management systems, authentication controls, or administrative restrictions;
- using cellular data, personal hotspots, VPNs, proxy services, anonymizers, browser extensions, tunneling services, or other methods to bypass CTC rules, filtering, monitoring, or network restrictions;
- using CTC technology resources for unauthorized games, gaming websites, downloads, streaming, file sharing, entertainment, or other non-instructional activities;
- installing, downloading, running, or distributing unauthorized software, applications, games, browser extensions, scripts, utilities, files, or executable content;
- damaging, vandalizing, stealing, hiding, removing, tampering with, or misusing CTC technology resources, devices, chargers, carts, cables, monitors, keyboards, mice, printers, projectors, network equipment, or other technology equipment;
- unplugging, cutting, pulling, removing, altering, or damaging cables, wires, wall plates, ports, chargers, peripherals, or connected equipment without authorization;
- creating or using unauthorized wireless networks, hotspots, network bridges, or external connections on CTC property or networks;
- accessing, creating, sending, posting, sharing, or distributing threatening, harassing, bullying, cyberbullying, discriminatory, sexually explicit, obscene, violent, harmful, or inappropriate content;
- recording, photographing, screenshotting, livestreaming, posting, sharing, or distributing images, audio, video, communications, classroom activity, shop activity, lab activity, student activity, staff activity, or CTC activity without authorization;

- accessing, copying, changing, deleting, photographing, screenshotting, recording, sharing, or distributing private, protected, confidential, personal, academic, or CTC information without authorization;
- using AI tools, automated systems, or technology resources to cheat, plagiarize, impersonate others, create fake content, generate harmful content, bypass assignment expectations, or violate academic integrity;
- introducing malicious software, viruses, spyware, ransomware, unauthorized scripts, or other harmful code into CTC systems or networks;
- scanning, testing, monitoring, intercepting, disrupting, or attempting to exploit CTC networks, systems, devices, applications, accounts, or services without authorization;
- violating copyright, software licensing, intellectual property, or digital content restrictions;
- using CTC technology resources for commercial, political, fraudulent, or unlawful purposes;
- interfering with instruction, CTC operations, network performance, cybersecurity protections, safety, or the rights of others; or
- engaging in any activity that creates a safety, security, disciplinary, operational, legal, instructional, or cybersecurity concern.

The CTC reserves the right to investigate, restrict, suspend, disable, remove, report, or take other appropriate action regarding prohibited activities involving CTC technology resources in accordance with applicable laws, policies, administrative procedures, the Student Code of Conduct, and operational requirements.

13. Incident Reporting and Cybersecurity Responsibilities

Students share responsibility for helping maintain the safety, security, reliability, and responsible use of CTC technology resources.

Students are expected to promptly report technology concerns, misuse, damage, unsafe activity, or suspected cybersecurity issues to a teacher, administrator, or technology staff member.

Students shall report:

- damaged, missing, stolen, malfunctioning, or improperly used technology equipment;
- lost, stolen, compromised, or improperly accessed accounts, passwords, devices, or login credentials;
- suspected phishing emails, suspicious links, fraudulent messages, malicious files, or harmful communications;
- threatening, harassing, bullying, cyberbullying, discriminatory, obscene, or inappropriate electronic communications or content;
- unauthorized access to accounts, systems, applications, files, networks, or information;
- accidental access to private, protected, confidential, personal, academic, or CTC information;
- suspected viruses, malware, ransomware, spyware, unauthorized software, or abnormal device/network activity;
- unsafe, disruptive, or unauthorized use of technology resources; and
- suspected violations of this policy, the Electronic Communication Device Policy, the Student Code of Conduct, or other CTC rules involving technology.

Students are expected to cooperate with CTC staff during technology-related investigations, incident response activities, device inspections, account reviews, cybersecurity responses, or administrative reviews.

Students shall not:

- intentionally conceal damaged, missing, stolen, misused, or improperly used technology equipment;
- intentionally conceal cybersecurity incidents, unauthorized access, account misuse, policy violations, or unsafe technology activity;
- interfere with technology investigations, cybersecurity responses, monitoring activities, or administrative reviews; or
- continue using accounts, devices, systems, applications, or networks known or reasonably believed to be compromised, unauthorized, unsafe, or improperly functioning.

The CTC reserves the right to take appropriate action to protect students, staff, technology resources, instructional activities, CTC systems, and cybersecurity interests, including account restrictions, device restrictions, network limitations, access suspension, device inspection, or other administrative safeguards.

14. Violations and Disciplinary Action

Violations of this policy, the Electronic Communication Device Policy, the Student Code of Conduct, related administrative procedures, cybersecurity requirements, or applicable laws involving CTC technology resources may result in disciplinary, administrative, legal, or other corrective action as determined appropriate by the CTC.

The CTC reserves the right to investigate suspected violations involving technology resources, systems, accounts, devices, applications, communications, network activity, electronic content, student information, or other technology-related activity.

Violations may result in actions including, but not limited to:

- verbal or written warning;
- parent/guardian notification;
- teacher or administrative conference;
- restriction, suspension, or loss of technology privileges;
- restriction, suspension, or loss of network, internet, account, device, or application access;
- removal from or restriction of access to shared technology resources, Chromebook carts, labs, or other equipment;
- disciplinary action consistent with the Student Code of Conduct and applicable CTC policies;
- restitution, repair, or replacement responsibility where permitted by law and CTC procedures;
- referral to law enforcement or other appropriate authorities where warranted; or
- other corrective action determined appropriate by CTC administration.

The severity of disciplinary or corrective action may depend upon factors including:

- the nature and severity of the violation;
- whether the activity was intentional, reckless, negligent, or accidental;
- whether damage, theft, disruption, harassment, cyberbullying, unauthorized access, privacy violation, or cybersecurity risk occurred;
- the impact on students, staff, instruction, CTC operations, technology resources, or network security;

- prior violations or repeated misconduct; and
- any applicable legal, safety, administrative, or disciplinary considerations.

The CTC reserves the right to immediately suspend, restrict, disable, or remove access to technology systems, accounts, devices, applications, services, networks, or internet access when necessary to:

- protect students, staff, or CTC technology resources;
- respond to suspected misuse, damage, unauthorized activity, or cybersecurity concerns;
- protect private, protected, personal, academic, or CTC information;
- support investigations or administrative reviews; or
- maintain safety, instruction, operations, or cybersecurity.

Nothing within this policy limits the authority of the CTC to take lawful and appropriate disciplinary, administrative, legal, operational, or cybersecurity action as necessary.

15. Administrative Authority and Policy Review

The Administrative Director or designee is responsible for the implementation, administration, interpretation, and enforcement of this policy.

The CTC administration, technology staff, teachers, and other authorized staff may establish procedures, guidelines, expectations, restrictions, security measures, and instructional requirements to support the safe, responsible, secure, and appropriate use of CTC technology resources.

The CTC reserves the right to:

- establish and revise technology procedures, rules, and expectations;
- manage, monitor, restrict, approve, or deny access to CTC technology resources;
- determine appropriate access levels for students, accounts, devices, applications, systems, networks, and services;
- implement cybersecurity, filtering, monitoring, classroom management, and device management controls;

- require students to comply with updated technology expectations, procedures, or security requirements;
- restrict or remove access to technology resources when necessary for instructional, operational, administrative, legal, safety, or cybersecurity reasons; and
- take appropriate action to protect CTC students, staff, systems, data, devices, networks, and technology resources.

This policy may be reviewed, revised, or updated as needed to address changes in technology, instructional needs, cybersecurity risks, legal requirements, administrative expectations, or CTC operations.

Students are responsible for complying with this policy, related procedures, teacher directions, administrative rules, and the Student Code of Conduct whenever using CTC technology resources.

16. Acknowledgment

I acknowledge that I have received, reviewed, and understand the Wilkes-Barre Area Career and Technical Center Student Acceptable Use Policy.

I understand that access to CTC technology resources, including computers, Chromebooks, networks, internet access, email, cloud-based platforms, applications, accounts, devices, and related systems, is provided to support approved educational and school-related purposes.

I understand that use of CTC technology resources is a privilege and may be monitored, filtered, reviewed, restricted, suspended, or revoked in accordance with this policy, CTC rules, administrative procedures, and applicable laws.

I agree to use CTC technology resources in a responsible, respectful, safe, secure, ethical, and educationally appropriate manner.

I understand that violations of this policy may result in disciplinary action, restriction or loss of technology privileges, parent/guardian notification, restitution or repair/replacement responsibility where applicable, referral to law enforcement where warranted, or other corrective action determined appropriate by the CTC.

I understand that this policy applies whenever I use CTC technology resources, access CTC systems or networks, use CTC accounts or applications, or use personal or sending school district-issued devices to access CTC resources.

I understand that I am responsible for my assigned accounts, passwords, devices, files, activity, and use of CTC technology resources.

Student Name: _____

Student Signature: _____

Program/Grade: _____

Date: _____

Parent/Guardian Acknowledgment

I acknowledge that I have received, reviewed, and understand the Wilkes-Barre Area Career and Technical Center Student Acceptable Use Policy.

I understand that my child's access to CTC technology resources is provided for approved educational and school-related purposes and is subject to monitoring, filtering, review, restriction, discipline, and other actions as described in this policy.

Parent/Guardian Name: _____

Parent/Guardian Signature: _____

Date: _____