# Academy of Careers and Technology

## Plan for Assuring the Privacy, Safety and Security of Data


390 Stanaford Road
Beckley, West Virginia 25801
304-256-4615
Preparing Students for Their Future
http://wvact.net
http://facebook.com/wvact

At the Academy of Careers and Technology, we take the security of institutional data seriously. Every school employee is trained yearly on FERPA and written acknowledgment is obtained that any student information will not be released unless properly verified that student information can and would be released to the appropriate individual(s) or organization.

All employees with access to technology and the network are trained on and must agree and sign a Technology Use Consent form. This form will also be signed by every student before access to the school technology and network. This consent form is specific and outlines what users can and cannot do while using the network and technology within the school. Any violation of the Technology Use Consent form by either student of employee can/will result in disciplinary action and/or dismissal depending on the violation and damage caused by their actions.

On a larger scale, any device that is connected to the school network/internet is going through two different filter systems. Both of these filter systems are through a company called Lightspeed. The Raleigh County School District, which provides our network/internet access also locally uses a local filter to secure data. The West Virginia Department of Education also has a filter in place that must be passed in order to secure access to our network/internet. In addition to these multiple filters in place, each server in our school and district has a firewall set up on it to help assist with the security and privacy of data within our network system. All of these items are in place to help ensure the Privacy, Safety and Security of Data at the Academy of Careers and Technology.

# Employee Technology Acceptable Use Agreement Form

Employee Name: _____ Employee ID: **97400 __ __ __ __**

The use of the Internet and computer equipment at work is limited to employees who require such use as part of their job responsibilities as determined by the employee's immediate supervisor. Since access to the Internet and technology is widely available at schools and departments, all employees are required to abide by this agreement. While some materials accessible
via the Internet may contain items that are illegal, defamatory, or potentially offensive to some people, the Raleigh County school system does not condone the use of such materials. Raleigh County Schools Policy E.13 requires that all employees read, accept, and sign the following agreement for Technology Acceptable Use.

1. Employees are responsible for proper behavior on the Internet and appropriate use of technology resources.
2. Network and local data storage areas are not considered private. A network administrator may review files and communications to maintain system integrity and ensure compliance with acceptable use policies. Users should not expect their files to be private.
3. Specific examples of unauthorized use from state and local policies include, but are not limited to:

a. Downloading, executing or viewing non-educational activities (e.g. games, music, videos, shopping, messaging) b. Downloading, uploading and/or executing malicious code (e.g. viruses, trojans, worms, macros, etc.)
c. Unauthorized installation or willful altering of software, setup preferences, security or other system settings.
d. Corrupting, destroying, deleting or manipulating system data with malicious intent.

e. Creating, storing, transmitting or viewing materials of a violent, sexual, racist, obscene or other offensive nature. f. Using school equipment or resources in a harassing, threatening or insulting manner.
g. Employing the network, equipment or technology resources for commercial or unauthorized purposes.
h. Using school equipment or resources in any manner that violates any law or state/district policy.

i. Violating copyright laws.
j. Misrepresenting an individual's identity or sources of communication or data (e.g. plagiarism, language translators) k. Using another's logon/password to gain unauthorized access to email, electronic folders, files or online resources. l. Providing your logon/password to another to gain unauthorized access to secure network resources.
m. Unauthorized participation in chat rooms, wikis or blogs.
n. Connecting any computer or other device to the network without the consent of the network administrator.
o. Unauthorized or improper publishing to district or school websites.
p. Unauthorized disclosure, use, or dissemination of personal information regarding yourself (if student) or others.

4. Any violation of this agreement may result in the loss of computer use or access. Depending on the circumstances, such violation may further result in disciplinary actions such as warnings, reprimands, suspensions or termination. Legal actions may be initiated that could result in monetary compensation to the district for equipment or services required to correct issues resulting from any violation of this agreement.

5. All employees are required to abide by Raleigh County Schools Policy E.13 and West Virginia Board of Education Policy 2460. Copies of these policies are maintained in district and school offices, and links to these policies are available from the district website at:
https://wv01919578.schoolwires.net/cms/lib/WV01919578/Centricity/domain/392/section%20e/E.13_Acceptable_Use_of_Techn ology_by_Students_and_Employees.pdf

6. Employee acceptable use must adhere to applicable state and district policies, but schools or departments may develop additional acceptable use measures as required. Additional measures must be listed on the backside of this page, and are therein incorporated as a part of this agreement for that school or department.

I am aware that district and state policies may be modified at any time by governing boards, but that any such modification will be communicated to users in a timely manner. I hereby acknowledge that I have read this agreement for Technology Acceptable Use and agree to comply with state and district policies. Should I violate this agreement, I understand that I am subject to disciplinary action.

Employee Signature _____ Date _____

E. INSTRUCTIONAL PROGRAMS POLICY: E.13

Acceptable Use of Technology by Students and Employees

Raleigh County Schools provides students with the opportunity to become proficient in 21st Century learning skills and technology tools, necessary to become lifelong learners with the skills that prepare students to be successful in school, on the job, in life and community as defined in West Virginia Department of Education Policy 2520.14. Raleigh County Schools takes all precautions necessary to ensure that students are exposed to a safe digital environment as required by the FCC under the "Children's Internet Protection Act"(CIPA), "Children's Online Privacy Protection Act of 1998" and E-rate guidelines. Raleigh County Schools provide computers and other technology devices, access to the Internet, and various programs to enhance and promote the educational experience. Use of any district equipment is for the purpose of legitimate educational practices. Use of technology in Raleigh County Schools is a privilege, not a right. Usage of Raleigh County School's network suggests no expectation of privacy. All materials, emails, files, etc., are subject to monitoring or review, without notice, by Raleigh County and West Virginia Board of Education.

The Raleigh County Schools Technology Team shall develop written technology procedures which provide guidance to staff and students concerning the safe, appropriate and ethical use of the Board's network(s) based on State Policy 2460 – Educational Purpose and Acceptable Use of Electronic Resources, Technologies and the Internet.

The technology procedures shall also inform both staff and students about disciplinary actions that will be taken if Board technology and/or networks are abused in any way or used in an inappropriate, illegal or unethical manner. Unacceptable use of technology includes, but is not limited to:

1. Downloading, executing or viewing non-educational activities (e.g.,games, music, videos,).
2. Downloading, uploading and/or executing malicious code (e.g., viruses, trojans, worms, macros, etc.)
3. Unauthorized installation or willful altering of software, setup preferences, security or other system settings.
4. Corrupting, destroying, deleting or manipulating system data with malicious intent.
5. Creating, storing, transmitting or viewing materials of a violent, sexual, racist, obscene or other offensive nature.
6. Using school equipment or resources in a harassing, threatening or insulting manner. Cyber bullying, hate mail, defamation, harassment of any kind, discriminatory jokes/remarks, and other unauthorized uses as referenced in federal, state, and local policies and laws.
7. Employing the network, equipment or technology resources for commercial or unauthorized purposes.
8. Using school equipment or resources in any manner that violates any law or state/district policy.
9. Violating copyright laws.
10. Misrepresenting an individual's identity or sources of communication or data (e.g., plagiarism, language translators).
11. Using another's logon/password to gain unauthorized access to email electronic folders, files or online resources.
12. Providing your logon/password to another to gain unauthorized access to secure network resources.
13. Unsupervised or unauthorized participation in chat rooms, wikis or blogs.

14. Connecting any computer or other device to the network without the consent of the network administrator.
15. Unauthorized or improper publishing to district or school websites.
16. Unauthorized disclosure, use, or dissemination of personal information regarding yourself (if student) or others.
17. Using social media to engage in non-professional interaction between employees and students in an inappropriate manner.
18. All other prohibited activities as listed in WVDE Policy 2460 Section 6.3.

1

E. INSTRUCTIONAL PROGRAMS POLICY: E.13

Further, safeguards, methods and instructional models established by State Policy 2460 to address Internet safety will be implemented and documented by the District. Raleigh County will use the state provided tool to educate students on Cyber Safety and document their exposure to the Cyber Safety lessons. All network access to the Internet shall be filtered through WVDE filters to decrease the risk of students accessing inappropriate or harmful material and through local filtering devices as needed. Accordingly, students shall be educated about appropriate online behavior including, but not limited to (1) interacting with other individuals through electronic mail, on social networking websites and in chat rooms and (2) recognizing what constitutes cyber bullying, understanding cyber bullying is a violation of Board policy, and learning appropriate responses if they are victims of cyber bullying.

Student use of Internet-related or web-based applications must be authorized by the educator and parent or guardian through a signed Acceptable Use Authorization Form. No student is permitted to use the Internet unless authorized adult supervision is provided in the same room as the Internet computer. While WVDE does filter Internet traffic, filtering software is not 100% effective. Deliberate and consistent monitoring of student use of the Internet and technologies is vital to prevent access to inappropriate and harmful materials. While classroom educators have primary contact with students, acceptable and appropriate use of online resources, technologies and the Internet is the responsibility of all educational staff and employees.

The acceptable and appropriate use of telecommunications and/or access to the Internet and digital resources is an extension of the educator's responsibility in his/her classroom. Educators occupy a position of trust and stand in the place of a parent or guardian while a student is in school. Therefore, it is the educator's responsibility to ensure classroom activities focus on appropriate and specific learning goals and objectives when using Internet-related technologies. It is the educator's responsibility to avoid using technology in such a manner that places him/her in a position to abuse that trust.

Collaboration, resource sharing, and dialogue between the educational stakeholders (teachers, students, and/or parents) may be facilitated by the use of social media and other electronic communication. Such interactivity outside of the school walls can enhance classroom instruction. However, a clear line must be drawn between personal social networking and professional/educational networking to protect the safety of the students and the integrity of educational professionals and service staff. Use of social media and electronic communication must support the educational process and follow county technology procedures. Educators are discouraged from using personal accounts to contact students.

Professional development regarding the responsible use of the Internet and other technologies will be provided to employees. Employees who complete the training and sign Acceptable Use Forms may be provided with appropriate usernames and passwords to access to the Board's network and technologies.

Employees who receive training on State Policy 2460 may apply for a state e-mail account and password. A state e-mail address is required to receive information distributed through State and County distribution lists and list-serves and to access county servers and websites. Use of personal e-mail accounts to contact staff, students and parents is discouraged.

All information stored within the State's and District's computers, servers and other technology devices is the property of the state, county or schools, and the personnel using District equipment and networks have no expectations of privacy with respect to its content.

The West Virginia Education Information System (WVEIS) is to be used exclusively for the business of the County and its schools. All staff must maintain the confidentiality of student data in accordance with The Family Educational Rights and Privacy Act (FERPA).



E. INSTRUCTIONAL PROGRAMS POLICY: E.13

Raleigh County Schools recognize the educational benefits of school personnel and students publishing information on the Internet. The District also recognizes the importance of guidelines that address content, overall responsibility, quality, copyright laws and student protection.

The District shall follow the guidelines of federal and state law, the Children's Internet Protection Act (CIPA) and the Children's Online Privacy Protection federal statues (COPPA). Unauthorized or unacceptable use of the Internet or educational technologies as part of an educational program by students, educators or staff may result in suspension or revocation of such use and/or disciplinary actions involving local, county, state or federal agencies.

The Raleigh County Schools Technology Team shall annually review all technology procedures and forms and report any recommended and/or mandatory changes, amendments or revisions to the Superintendent and Board.

Approved: June 12, 2012