

801 – Acceptable Use for Electronic-Technology Resources Policy

I. Purpose:

- A. Users of Bryan Allen Stevenson School of Excellence (BASSE) electronic-technology resources must acknowledge their understanding of the following guidelines as a condition of using the resources. Any questions regarding this policy are to be directed to the school administration and/or the Board of Directors. This policy works in conjunction with the State of Delaware Department of Technology and Information (DTI) Acceptable Use Policy, which holds authority over this policy.

II. Definition:

- A. “Electronic-Technology Resources: Those resources that are: (a) provided by the school; (b) paid for, in whole or in part, by the school; (c) used to conduct business or other activity for or on behalf of the school; or (d) used in or at a school facility. These resources include, without limitation, the following:
 1. E-mail: All electronic-mail accounts and services provided to users by the State or BASSE.
 2. Technology Resources: All computers and related resources whether stationary or portable, including but not limited to all related peripherals, components, disk space, storage devices, servers, and output devices such as telephones, hand-held devices, printers, scanners, copiers, whether owned or leased by the school.
 3. “Bryan Allen Stevenson School of Excellence”: The infrastructure used to transmit, store, and review data over an electronic medium, and includes any and all of the following technologies provided to authorized users:
 - a) Internet service;
 - b) Intranet system;
 - c) BASSE mainframe system; and
 - d) Any collaboration systems, including but not limited to calendaring, message boards, conference boards, blogs, text messaging, instant messaging, video conferencing, websites, and podcasting, whether the system is owned or contracted;
 4. Electronic Data: Any and all information, data, and material, accessed or posted through any Electronic Resource.
- B. Personal Communication Devices: Any cellular phone, smartphone, personal digital assistant, or another personal electronic communication device.
- C. Users: All whom the policy applies, which include:
 1. BASSE Board of Directors.
 2. All BASSE’s staff including employees, consultants, volunteers, interns, temporary, and other workers at the school, including all personnel affiliated with third parties.
 3. All BASSE students under the supervision of a staff member and/or parent/caregiver.
 4. Others who request Guest Accounts or electronic-technology resources.

5. Cyberbullying: Bullying by using information and communication technologies. Cyber-bullying may include but is not limited to:
 - a) Denigration: spreading information or pictures to embarrass;
 - b) Flaming: heated unequal argument online that includes making rude, insulting, or vulgar remarks.
 - c) Exclusion: isolating an individual from his or her peer group.
 - d) Impersonation: Using someone else's screen name and pretending to be them is impersonation.
 - e) Outing or Trickery: forwarding information or pictures meant to be private.

III. Policy Statement:

A. User Responsibilities:

1. All Users:

- a) Use of the Bryan Allen Stevenson School of Excellence electronic-technology resources and network services is a privilege, not a right. Failure to adhere to this policy and administrative procedures may result in disciplinary action or criminal penalties under applicable state and federal law. In addition, all Users have a duty to protect the security, integrity, and confidentiality of Electronic Resources, including the obligation to protect and report any unauthorized access or use, abuse, misuse, degradation, theft, or destruction.
- b) While using BASSE networks and equipment, users understand that they are monitored through school video cameras and tracking of users' online searches.

2. School:

- a) School officials are responsible for designating Users authorized to use Electronic Resources.
- b) The school provides for the education of students regarding the Acceptable Use Policy.
- c) The school will also educate students on the following topics:
 - i. Safety on the internet;
 - ii. Appropriate behavior while online, including interacting with other individuals on social networking websites and in chat rooms; and
 - iii. Cyber-bullying awareness and response.

3. Students:

- a) Students have a duty to take reasonable steps to protect their privacy and personal information when using Electronic Resources.
- b) Students must not disclose personal contact information, except to educational institutions for educational purposes, without prior advance approval.
- c) Students also must promptly disclose to a teacher or other appropriate school employee any violation of this Policy, including any message received that the student believes to be

inappropriate or makes the student feel uncomfortable.

4. Personnel:

- a) BASSE employees are expected to communicate with students and parents through the school-provided email and are strongly advised against using other forms of personal electronic communication with students, such as Instant Messaging or texting.
- b) School employees are required to take reasonable measures to protect their personal information and reputation when using Electronic Resources or otherwise participating in activities online.

B. Acceptable Uses:

1. Acceptable uses of electronic-technology resources and the network are activities that support learning and teaching. Users are encouraged to develop activities that meet their individual educational needs, and which take advantage of the network's functions.
2. The use of electronic-technology resources must be consistent with the academic goals of the school, curriculum standards, and BASSE's policies.
3. BASSE works in conjunction with the Department of Education in the blocking and filtering of resources to restrict access to inappropriate websites and other materials harmful to minors to ensure the safety and security of all students, and to comply with State law and /or regulation.

C. Internet Use Procedures:

1. Students may use the Internet in instructional areas where there is teacher or staff supervision. Teachers may allow students to use the Internet in the following ways:
 - a) Directed Searches: Teachers may work directly with small groups of students or with an entire class.
 - b) Internet access will be limited to those sites approved by the teacher and previewed in advance.
 - c) The use of directed searches does not require parental permission since the Internet sites will be screened in advance by the teacher.
 - d) Teachers will be responsible for reviewing the Internet policy and procedures with students prior to any directed searches.
2. Independent Searches:
 - a) Students wanting to use the Internet for independent educational searches must meet the following criteria:
 - i. Students must participate in an Internet training workshop conducted by the teacher, where proper Internet behavior and BASSE' School's Acceptable Use Policy for electronic technology will be discussed.
 - ii. This workshop will take place during orientation for all students, who will then sign off on it upon completion.

- iii. Parents may participate in the training with the student by requesting such from the teacher.
 - iv. An Acceptable Use Policy Agreement Form for use of electronic-technology resources must be signed by the student, parent, and teacher. The form will remain on file.
3. User Safety:
- a) To the extent practical, steps shall be taken to promote the safety and security of users of BASSE's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.
 - b) Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes:
 - i. Unauthorized access, including so-called 'hacking,' and other unlawful activities; and
 - ii. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors.
4. BASSE's Board of Directors, employees, and guest users must have a signed Acceptable Use Policy Agreement Form on file prior to the use of electronic technology resources.

D. Unacceptable Uses:

1. Unacceptable uses of electronic technology and the network include, but are not limited to:
- a) Violating the rights to privacy of students or employees of BASSE, or others outside the school system.
 - b) Using profanity, obscenity, or another language that may be offensive to another user.
 - c) Copying materials in violation of copyright law.
 - d) Plagiarizing (taking someone else's words, ideas, or findings and intentionally presenting them as your own without properly giving credit to their source).
 - e) Using the network for financial gain or for any commercial or illegal activity.
 - f) Attempting to degrade or disrupt system performance or unauthorized entry to and/or destruction of computer systems and files.
 - g) Re-posting personal communications without the author's prior consent.
 - h) Revealing home phone numbers, addresses, or other personal information or making personal purchases or unauthorized orders using BASSE's name.
 - i) Accessing, downloading, storing, or printing files or messages that are sexually explicit, obscene, or that offend or tend to degrade others.
 - j) Use of Cloud Services for Top Secret, Secret, and Confidential data, unless the contract includes cloud computing terms and conditions approved by DTI.

- k) Downloading or copying information onto disks or hard drives without prior teacher approval.
- l) Violating the policy as outlined in the BASSE Code of Student Conduct.
- m) Cyberbullying: Bullying by using information and communication technologies.
- n) Using any Electronic Resource in any way that threatens or violates the security of any Covered Technology, where such use:
 - i. Contains a virus, Trojan horse, logic bomb, malicious code, or another harmful component.
 - ii. Constitutes a chain letter, junk mail, spam, or other similar electronic mail.
 - iii. Constitutes unauthorized access or attempts to circumvent any security measures.
 - iv. Obtains access to or use of another User's account, password, files, or data, or attempts to so access or use, without the express authorization of that other User.
 - v. Deprives a User of access to authorized access of Electronic Resources.
 - vi. Engages in unauthorized or unlawful entry into a BASSE Network.
 - vii. Shares e-mail addresses or distribution lists for uses that violate this Policy or any other school Policy.
 - viii. Transmits sensitive or confidential information without appropriate security safeguards.
 - ix. Falsifies, tamper with, or makes unauthorized changes or deletions to data located on BASSE's network.
 - x. Obtains resources or BASSE Network accesses beyond those authorized.
 - xi. Distributes unauthorized information regarding another User's password or security data.
 - xii. Discloses confidential or proprietary information, including student record information, without authorization.
 - xiii. Involves the relocation of hardware (except for portable devices), installation of peripherals, or modification of settings to equipment without express prior authorization by the school administration or designee.
 - xiv. Installs, downloads, or uses unauthorized or unlicensed software or third-party system without express prior authorization by the school administration or designee.
 - xv. Involves a deliberate attempt to disrupt BASSE's Network.
- o) Personally Owned Devices:

1. It is the responsibility of the Users to follow the guidelines listed above. Failure to follow these guidelines could result in disciplinary actions, suspension of privileges, revocation of privileges, and/or criminal penalties. These guidelines are based off the DTI Acceptable Use Policy and do not excuse any user from following DTI Acceptable Use Policy.

Related Policies:

- A. Social Media Policy

Related Procedures and Documents:

- A. 47 U.S.C. § 254,
- B. Children’s Internet Protection Act (CIPA):
<https://www.fcc.gov/consumers/guides/childrens-internet-protection-act>
- C. State Acceptable Use Policy of Delaware, <http://www.delaware.gov> New Castle County Vocational-Technical School District Acceptable Use Policy, 7/28/10
Brandywine School District Acceptable Use Policy, 2/23/09
- D. Delaware Information Security Policy:
<https://webfiles.dti.delaware.gov/pdfs/pp/DelawareInformationSecurityPolicy.pdf>
- E. Department of Technology and Information Acceptable Use Policy:
<https://webfiles.dti.delaware.gov/pdfs/pp/AcceptableUsePolicy.pdf>

Approval:

Revision Dates:

Student Acceptable Use Policy Agreement Form

I have read, understand, and will follow all rules, regulations, and policies when accessing and using the Bryan Allen Stevenson School of Excellence Charter School's electronic/technology resources. I further understand that any violation of the policy is unethical and may constitute a criminal offense. Should I commit any violation of the policy, I understand and agree that my access privileges may be revoked and disciplinary action and/or legal action may be taken.

Teacher Signature _____ Date _____

Student Signature _____ Date _____

Parent Signature _____ Date _____

Employee/Guest Acceptable Use Policy Agreement Form

I have read, understand, and will follow all rules, regulations, and policies when accessing and using the Bryan Allen Stevenson School of Excellence Charter School electronic-technology resources. I further understand that any violation of the policy is unethical and may constitute a criminal offense. Should I commit any violation of the policy, I understand and agree that my access privileges may be revoked and disciplinary action and/or legal action may be taken.

Employee Signature _____ Date _____

Guest Signature _____ Date _____

Supervisor Signature _____ Date _____

DRAFT