TALBOT COUNTY
PUBLIC SCHOOLS
EASTON, MD 21601

POLICY CODE
10.32-AR
ENDORSED: 07/17/96
REVISED: 08/22/07
REVIEWED: 03/13/13

ACCEPTABLE USE OF TECHNOLOGY AND INTERNET SAFETY FOR STUDENTS - AR

I. Technology and the Internet - Students are expected to use technology in a manner appropriate to the academic mission of Talbot County Public Schools and in accordance with all legal and ethical standards. Technology includes, but is not limited to, computers, electronic devices, software, Internet, and all other network services. The use of computer resources is a revocable privilege. Failure to abide by this policy may render the student ineligible to use the school's computing facilities and may bring disciplinary or even legal action. Students must make available for inspection by a teacher or administrator upon request any computer, messages or files sent or received. The school has the right to review these items for appropriateness, and to limit or revoke a student's access at any time, and for any reason.

A. General Conditions of Use: Computers and network access are provided to students for school-related purposes. Prohibited activities include, but are not limited to:

1. Transmission of any material in violation of Federal, State, or local law or ordinance.
2. Use of technology for commercial activities by students or student groups. Commercial activity includes, but is not limited to the following:
   a. Any activity that requires an exchange of money and/or credit card numbers;
   b. Any activity that requires entry into an area of service for which the school may be charged a fee;
   c. Any purchases or sales of any kind;
   d. Solicitation of donations; and
   e. Any use for product advertisement or political lobbying.
3. Non-moderated communication methods such as instant messaging, chat rooms, and e-mail, except as explicitly authorized by a teacher or administrator.

B. Files and File Management: The permission to store files on school system computers or computer networks is subject to responsible and ethical use.

1. Images, sounds, music, video, or materials that are pornographic, obscene, or vulgar, or depict the use of illegal drugs, alcohol, tobacco or illegal and/or violent behavior (and/or would violate school rules if in non-digital formats) may not be downloaded, uploaded, imported or used.
   Illegal use, distribution or transfer of copyrighted material to school computers including text, music, video, images, or audio files is prohibited. Students must

2. abide by copyright laws and download/import only music or other files to a school-owned computer that he/she is authorized or legally permitted to reproduce, or for which he/she has the copyright.
3. File sharing must be approved and directed by the teacher.
4. Copying, changing, reading, or using files in another user's storage area (such as hard disk space, optical media, flash media, server space, personal folders, etc.) without the user's permission and/or for the purpose of academic cheating is prohibited.
5. Files may be stored only in locations and formats authorized for the student's use. Storing non-school related material (files) on a school system file server is prohibited.
6. For students issued a computer for their individual use, it is the responsibility of each student to ensure that student-loaded files and programs do not consume hard drive space needed for instructional or educational requirements.

C. Network and Internet Access: Access to the school system's computing facilities is granted with a computer account. Accounts are assigned to individuals and are not to be shared.

1. The account owner is responsible for all activity performed from his/her account. Activity on a user's account may be monitored and recorded. It is a violation of this policy to allow others to use this account or to use another person's account, with or without that person's permission.
2. Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent or assume the identity of other users.
3. To protect students while at school and to meet the Children's Internet Protection Act (CIPA) requirements, access to the Internet is filtered through a commercial filtering system. Attempts to in any way bypass or negate the filtering of Internet content is prohibited.
4. The Internet is a powerful learning tool, but must be used safely. Students are not to reveal identifying or personal information about themselves or others when using the Internet.
5. Posting harmful material about others to make them the subject of ridicule or damage their reputations (so called cyberbullying) is prohibited.
6. Harassment, threats or intimidation via Internet or Local Area Network (LAN) is strictly prohibited, and subject to disciplinary action. Students should report to school administrators or other staff any such activity that they have observed or have knowledge of, particularly if these actions occurred while using school-owned technology.

D. Student Use of Email: All student Electronic Mail (email) accounts are property of Talbot County Public Schools. Email activities must comply with Board of Education Policy (ACCEPTABLE USE OF TECHNOLOGY AND INTERNET SAFETY FOR STUDENTS). The user accepts all responsibilities and understands the policy.

1. The student will be removed from the system after graduation, leaving the school district, or infractions outlined below.
2. The primary purpose of the student electronic mail system is for students to communicate with school staff, outside resources related school assignments, and fellow students to collaborate on school activities. Account user names and passwords will be provided to parents so those parents can monitor the account and communicate with teachers. Use of the district's email system is a privilege. Communication through the district's email system will exhibit common sense and civility. It will abide by the community's mode of acceptable behavior. Students are responsible for messages sent from their accounts. Students should not share their passwords.
3. Messages posted on the district's email system cannot cause disruption to the school environment or normal and acceptable school operations. Occasional and reasonable personal use of the district's email is permitted, providing that this does not interfere with the performance of the electronic mail system or disrupt the operation of the schools. Electronic mail can be checked from home or from school computers, as long as it does not disrupt the operation of the classroom or school.
4. The email system cannot be used to operate a personal business. The account may not be reassigned. The account may be revoked if used inappropriately.
5. Students will report any unusual activities such as "spam" communications, obscene email, attempts by adults to lure them into dangerous behaviors, and the like to a teacher, administrator or helpdesk personnel for action. Students should not forward chain letters, jokes, or graphics files.
6. Students will not identify their home telephone numbers, or home addresses in any email correspondence unless required for the college admission process or internship.
7. Electronic mail sent or received are not confidential. Although the administration does not make a practice of monitoring electronic mail, the administration reserves the right to retrieve the contents of user mailboxes for legitimate reasons, such as to find lost messages, to conduct internal investigations, to comply with investigations of wrongful acts or to recover from system failure.
8. System administrators may create filters to scan for and eliminate viruses and large graphic files (i.e. animated holiday card during December) that are unrelated to the school district’s operation.

9. When issues arise, the department will deal directly with the student, school administration and/or parents/guardians. Improper use of the system will result in discipline and possible revocation of the student email account. Illegal activities on the system will be referred to law enforcement authorities for appropriate legal action.
10. The Department of Student Services is responsible to ensure the efficient use of the electronic mail system. The interpretation of appropriate use and future revisions of this guideline are the responsibility the department of Student Services.

If necessary, the administration, at its discretion, may close the accounts at any time. Any updates or changes to this electronic mail agreement by the Board of Education or administration will be in effect.

E. Security: Security on any computer system is a necessity and a high priority. All security problems must be reported to an administrator.

1. Attempts by a user to log on to the TCPS administrative network or servers using another's identity are prohibited.
2. Bypassing or attempting to bypass the school's filtering software is prohibited.
3. The use or attempt to connect a home computer or personal electronic devices to any part of the TCPS network unless instructed by an administrator is prohibited.
4. Sharing passwords with another person for any reason is prohibited and every effort should be made to keep all passwords secure and private.
5. Students must not knowingly introduce or knowingly allow the introduction of any computer virus to any school computer.

F. Care, Service, and Repair of school-system technology: Students are responsible for all technology resources provided for their use or in their possession.

1. Any broken or malfunctioning computer component, software application, operating system, network service, or peripheral should be reported to the technicians or to a teacher or administrator.
2. All equipment, software, and network configurations will be maintained by TCPS Technology Department.
3. Vandalizing or defacing hardware by writing upon, placing stickers upon, etching, staining, or otherwise intentionally altering the surface of hardware is prohibited.
4. Removing inventory and identification tags from any technology equipment is prohibited.

5. Students issued a computer for their individual use should:
    a. Carry their computers in the case provided by the school system, especially when the computers are taken out of school.
    b. Have his/her computer fully charged at the start of each school day.

G. Hacking and Electronic Trespassing: Altering or modifying the pre-installed software is prohibited. Examples include, but are not limited to the following:

1. Installing any additional software applications;
2. Changing the computer name;
3. Altering, or removing pre-installed software components including, but not limited to: productivity applications, security and/or utility software, and operating system components;
4. Altering user accounts or file permissions granted to them;
5. Taking apart the computer for access to internal parts or in an attempt to "repair" the computer.

Violations of these regulations will result in disciplinary action and may also result in criminal charges.

H. Violations of this policy: Student misbehavior in a technology setting often has a non-technology parallel and should be handled using the same progressive discipline steps as for other infractions of school rules. However, some violations are specific to the nature of electronic devices and media, and should be guided by the following.

1. Technology tools are increasingly central to teachers' lessons and student learning. Full loss of computing privileges should be a final recourse when other disciplinary measures have failed to modify inappropriate behaviors; or in response to a serious violation that threaten the safety or wellbeing of students, the security of the school system's servers or networks, or is a violation that could result in criminal charges.
2. Steps in a progressive discipline strategy appropriate to misuse of computing privileges may include:
    a. Progressive restriction of permitted access (independent Internet search capabilities, use of multimedia tools, access to external ports, etc.).
    b. Revocation of take-home privileges in the case of an individually issued computer.
    c. Other restrictions deemed necessary to maintain the intended and appropriate uses of technology.

ACCEPTABLE USE OF TECHNOLOGY
AND INTERNET SAFETY FOR STUDENTS

I. Student Agreement: This policy will be reviewed annually with students in grades 4-12 in an age-appropriate manner.

1. An *Acceptable Use Agreement* must be signed
   a. annually by students in grades 7-12,
   b. by students in grades 4-6 who will be allowed use of school system computers or networks for independent Internet searches or use not directly supervised by staff.
2. It is presumed that all computer use by students in grades K-3 will be closely and continuously monitored.

-END-