

BALDWIN COUNTY PUBLIC SCHOOL SYSTEM
Acceptable Use and Internet Safety Policy
Updated January 2010

A. Background

Freedom of expression is an inalienable human right and the foundation for self-government. Freedom of expression encompasses the right to freedom of speech and the right to receive information. Such rights extend to minors as well as to adults. Schools facilitate the exercise of these rights by providing access to information regardless of format or technology. In a free and democratic society, access to information is a fundamental right of citizenship.

That right, however, when exercised using the Internet access provided by the Baldwin County Public School District, carries with it responsibilities and obligations as expressed in this Acceptable Use and Internet Safety Policy (AUP). The National Center for Educational Statistics (NCES) of the U.S. Department of Education defines an acceptable use policy as follows: “A policy designed to limit the ways in which a computer or network can be used. AUPs usually include explicit statements about the required procedures, rights, and responsibilities of a technology user. Users are expected to acknowledge and agree to all AUP stipulations as a condition of system use and should be certified on the AUP by the user's signature.” Many of the guidelines contained in the NCES publication Safeguarding Your Technology have been included in this AUP.

The provisions of the Children's Internet Protection Act (CIPA) have been taken into consideration and incorporated into this AUP. The act requires that a district have a policy in place that addresses Internet safety for minors and adults and that a public meeting is conducted to seek community input on the policy. The act also requires that a technology protection measure be implemented with respect to any of the District's computers with Internet access. Other provisions require that student Internet use be monitored and that “hacking” or unauthorized access to the district network, as well as, the revelation of personal information about students be addressed. The act further requires that users be prevented from accessing visual depictions that are obscene, child pornography, or harmful to minors. CIPA requirements have been addressed through a public meeting that was held on April 17, 2001. Other requirements are being met by the District's subscription to a filtering service for all computers on the District Wide Area Network (WAN). Schools using Digital Subscriber Line (DSL) or dial-up access to the Internet are required to install filtering software on all computers with Internet access. Other CIPA requirements are being addressed through monitoring measures and guidelines and responsibilities as outlined in this document.

The District Technology Committee has been authorized to develop guidelines for the use of the Internet that are in accordance with District policies, including the student disciplinary code.

B. Philosophy

The Baldwin County Public School District supports the use of technology resources including district wide access to the Internet in an effort to improve student learning, increase critical thinking skills, develop life-long learning skills, and improve administrative tasks.

C. Responsibilities for Internet Access and Other Technology Resources

District network and Internet users are responsible for appropriate behavior online, just as they are in a classroom or other areas of the school or central office. The same general rules for behavior and communications apply. Access to any and all technology resources is a privilege, not a right, and is provided for administrative and educational purposes. The term "educational purposes" includes use of the network for classroom activities, professional or career development, and research. The following responsibilities will ensure ethical, efficient, and legal use of the network and other technology resources:

- 1) ***The Superintendent***, or his designee, will serve as the coordinator to oversee the use of the district network resources, including the Internet.
- 2) ***The Division of Information Technology Services*** (IT Services) will:
 - a) assist the District Technology Committee in developing and updating the AUP.
 - b) disseminate materials to schools.
 - c) cooperate fully with local, state, and/or federal officials in any investigation concerning or relating to any illegal activities conducted through the district network.
 - d) promote the idea that all Baldwin County personnel with access to the Internet must read the AUP and sign the Administrative Workstation Policy.
- 3) ***The Division of Human Resources*** will:
 - a) ensure that all new employees receive a copy of the Administrative Workstation Policy in their employment packet.
- 4) ***The Division of Instructional Support*** will:
 - a) provide guidance to teachers and schools in the identification of Internet resources (and other technology products and services) appropriate for instructional use.
 - b) assist the District Technology Committee in developing and updating the AUP.
- 5) ***All divisions will:***
 - a) maintain a file of signed copies of Administrative Workstation Policy forms for all division employees.
- 6) ***Principals***, or their designees, will:
 - a) ensure the appropriate use of the Internet by students, faculty, and staff.
 - b) serve as the building level coordinator for the use of network resources.
 - c) interpret the AUP at the building level.
 - d) ensure that all school employees, including new employees, with access to the Internet read the AUP and sign the Administrative Workstation Policy.
 - e) ensure that teachers receive proper training in the use of the network and the requirements of this policy.

- f) establish a system to ensure adequate supervision of students using the network.
- g) ensure that the Pupil Responsibilities and Conduct Standards handbooks are provided to all students, including new admissions.
- h) maintain a file of Internet Policy: Requests for Alternative Activities forms as described in the Acceptable Use and Internet Safety Student Guidelines in the Pupil Responsibilities and Conduct Standards handbook.
- i) ensure that copies of the full AUP are available in the school office and library for review by interested parents or individuals in the community.

7) **Teachers** will:

- a) select and review age appropriate material relevant to course objectives.
- b) review materials and sites students will access to determine the appropriateness of the material contained on or accessed through the site.
- c) provide guidelines and resources to assist students in research activities.
- d) assist students in developing skills to distinguish fact from opinion and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.
- e) monitor/supervise use of the Internet by being actively involved with the students when they are participating in online activities.
- f) provide alternative assignments for students who have Internet Policy: Request for Alternative Activities forms on file at the school.

8) **Parents** will:

- a) review and discuss with their child the Pupil Responsibilities and Conduct Standards handbook.
- b) complete the Internet Policy: Request for Alternative Activities form and return to the school if the parent does not want the child to have access to resources on the Internet.

9) **All Users** (students, teachers, administrators, and staff) will adhere to guidelines for use as listed in Section F of this policy. **District employees are expected to adhere to and enforce Board policies and administrative procedures.**

D. Filtering

The District subscribes to an enterprise level content filter to block inappropriate material including specific Uniform Resource Locators (URLS), Internet Protocol (IP) addresses, as well as inappropriate Internet Popup Ads. All school and office computers connected to the District network are protected by ISP-provided Internet content filter. Schools accessing the Internet through dial-up or DSL must provide software such as Net Nanny 4.0, CyberPatrol, or Norton Internet Security to ensure the user's traffic is properly filtered and protected. Any requests for DSL, dial-up or broadband service at a BCBE location must be approved by IT Services. BCBE users are prohibited from accessing the Internet without a content filtering measure being in effect. Further, students are prohibited from accessing the Internet without teacher or administrator supervision.

Should a teacher encounter a blocked site that is necessary for educational purposes, a request to reclassify the site can be made by clicking the link on the "Restricted Access" page and following the directions provided. If a user encounters a site that is inappropriate and should be blocked, please notify IT Services for review and appropriate action.

E. Monitoring

Students utilizing District Internet access must have the permission of and must be supervised by the Baldwin County Public School District's professional staff. Student use of the Internet must be directly related to teacher specified objectives. Teachers are to be directly involved with the students when they are participating in online activities. In addition, the District has purchased software that will enable the technical support staff to trace Internet usage.

F. Guidelines for Internet Access and Other Technologies

The following guidelines will govern the use of Internet access and other technologies in the District:

1. All use of the Internet must be in support of instructional or administrative activities and consistent with the purposes of the Baldwin County Public School District.
2. District officials will determine whether specific uses of the network are consistent with this acceptable use policy.
3. Any activity that occurs on equipment provided by the District IS NOT PRIVATE and can be monitored by administrators, or in the case of student users, monitored by teachers. These activities include messages (e-mail and chat), files created or modified, transmitted, received, or stored on any District equipment.
4. Student users must sign-in legibly on the appropriate log or register (i.e. a seating chart or log for an individual computer) in the classroom, lab, or media center each time they use the network.
5. Students may participate in chat room activities **ONLY** under the direct supervision of a teacher.
6. The guidelines listed below should be followed by all users of the district network, Internet, and e-mail:

Network

- Users will report any technical problems encountered online to the School Technology Coordinator.
- Users should not engage in the following prohibited network activities, which may be either illegal or inappropriate:
 - violate any local, state, or federal statute, such as engaging in any illegal act, unauthorized access, including so-called "**hacking**," and other unlawful activities such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of a person, etc.

- access inappropriate text files or files dangerous to the integrity of the network.
- install illegally copyrighted software on district equipment.
- use the network for commercial or for profit purposes, as well as use the network extensively for personal and private business.
- use the network for product advertisement or political lobbying.
- seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, as well as misrepresent other users on the network.
- destroy, modify, or abuse hardware, software, or other advanced technologies.
- use the network for malicious purposes, such as using the network to develop programs that harass other users or infiltrate a computer or computing network and/or damage the hardware and/or software components of a computer or computing network. This includes, but is not limited to, the uploading or creating of computer viruses.
- seek to gain unauthorized access to the resources on the network. This includes attempting to log in with another person's account or accessing another person's files.
- provide a password to another person.

Internet

- Users who accidentally encounter inappropriate material should report the access immediately to the teacher, or, if encountered by a teacher, to the school technology coordinator, who should contact IT Services to request that the site be blocked.
- Users should not engage in the following prohibited Internet activities, which may be either illegal or inappropriate
 - Access visual depictions that are obscene, child pornography, or harmful to minors.
 - Plagiarize works accessed on the Internet, violating copyright law, or otherwise using the intellectual property of another individual or organization without permission.
 - Browse randomly [a.k.a. "surfing"] Internet sites without an instructional purpose. Students will use Internet equipment only for school-related activities with teacher permission.
 - Use Internet games, including MUDs (Multi User Domains) and IRCs (Internet Relay Chats).
 - Attempt to bypass the Internet content filter via commercial or personal proxy sites or proxy servers or any other means or method. This is a violation regardless of the deemed appropriateness of the site(s) ultimately visited/viewed through the use of proxies or similar means/methods.
 - Use vulgarities, threatening or any other disrespectful or inappropriate language (also applies to e-mail).
 - Reveal your personal address or phone number or reveal the personal address or phone number of others (also applies to e-mail).

E-mail

- Users should check their e-mail frequently, respond promptly, and delete unwanted messages promptly. Important e-mail messages should be placed in appropriate folders and e-mails older than 90 days should be deleted.

- Users should be aware that e-mail IS NOT PRIVATE and should be considered as PERMANENT in the sense that the user cannot really delete it from the system.
- Employees subscribing to listservs must monitor their communications each school day and delete the mail from the personal mail directory to avoid excessive use of file server hard-disk space.
- E-mail is provided for administrators, faculty, and selected staff. Although student e-mail is not allowed, teachers may request a class account that can be used for instructional projects that involve the use of e-mail.
- Users should not engage in the following prohibited e-mail activities, which may be either illegal or inappropriate
 - subscribe to listservs by students. (An automated system for sending and receiving e-mail.)
 - post chain letters or engage in “**spamming**.” Spamming is sending an annoying or unnecessary message to a large number of people. Do not reply or forward this type of e-mail. If you are receiving a number of inappropriate e-mails or spam, please alert IT Services with an e-mail to your zone technician.
 - send or post hate mail, harassment, discriminatory remarks, and other antisocial behaviors.
 - use my BCBE email account to register for non-work related web sites (such as Facebook, MySpace, etc.) or any Internet services that send non-work related email notifications

G. Penalties for Violations

Any violation of District policies and procedures by any person accessing the Internet through District resources may result in loss of district provided access to the Internet. Additional disciplinary action may be determined at the building level in keeping with existing procedures and practices regarding inappropriate language or behavior. When and where applicable, law enforcement agencies may be involved. Penalties will be based on the severity and frequency of the offense. Users may appeal a penalty following appropriate procedures defined in District policy.

All Users

1. The progression of penalties may involve, but not be limited to, increasing periods of time that access to the network will be denied.
2. Violations involving illegal activities or network security will result in severe penalties including denial of access for one or more years. If the conduct violates local, state, or federal law, the District will cooperate with those authorities.
3. Violations that result in a cost for repair or replacement of equipment or data will result in a fine to recover the cost. Access to technology will be denied until the fine is paid.

Students

1. Violations could result in the student’s removal from a class or lab.
2. Other consequences such as detention, suspension, or expulsion may be applied in accordance with the Pupil Responsibilities and Conduct Standards District policies and procedures.

Employees

Violations by District employees shall subject them to disciplinary action and penalties that are applicable under District policies and procedures.

Notice: This policy and all its provisions are subordinate to local, state, and federal statutes.