Baldwin County School
Acceptable Use Policy

The Baldwin County School District supports the rights of students and staff to have reasonable access, in school, to various information formats and believes it is incumbent upon students and staff to use this educational advantage in an appropriate and responsible manner.

District Technology can be defined as any electronic device, tool, system, service, or other property owned by the Baldwin County School District.

Responsible Use

This policy outlines the guidelines and behaviors that all users are expected to follow when using technology. It is the responsibility of both Baldwin County Schools and parents to help prepare students to be responsible members of a digital society and digital citizens who:

Understand human, cultural, and societal issues related to technology.

Practice legal and ethical behavior online.

Advocate and practice safe, legal, and responsible use of information and technology.

Exhibit a positive attitude toward using technology to support collaboration, communication, creativity, and critical thinking.

Demonstrate personal responsibility for lifelong learning.

Exhibit leadership for digital citizenship.

Policies, guidelines and rules refer to all computing devices including but not limited to computers, mobile web enabled devices, iPads, MP3 players, portable memory storage devices, calculators with interfacing capability, cell phones or electronic communication devices, digital cameras, etc., as well as technology infrastructure, associated peripheral devices and/or software that access the Baldwin County Schools internet/computer network; and all computers and devices owned by the Baldwin County Schools.

Prohibited Use

Unacceptable uses of school electronic resources include, but are not limited to:

1. Accessing or Communicating Inappropriate Materials–Users may not access, submit,

post, publish, forward, download, scan or display defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing, bullying and/or illegal materials or messages.

2. Illegal Activities– Users may not use the school district's computers, electronic devices, networks, or internet services for any illegal activity or in violation of any school district policy/procedure or rules. Baldwin County Schools and its employees and agents assume no responsibility for illegal activities of users while using school computers or school-issued electronic resources.

3. Violating Copyrights or Software Licenses– Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is prohibited, except when the use falls within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

4. Plagiarism– Users may not represent as their own work any materials obtained on the internet (such as term papers, articles, music, etc.). When using other sources, credit must be given to the copyright holder. Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the internet should be appropriately cited, giving credit to the original author.

5. Cyberbullying– Cyberbullying will not be tolerated. Harassing, denigrating, impersonating, and cyberstalking are all examples of cyberbullying. Do not send emails or post comments with the intent of scaring, hurting, or intimidating others. Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime.

6. Misuse of Passwords/Unauthorized Access– Users may not share passwords; use any user account/password that is not assigned to them; or attempt to circumvent network security systems.

7. Malicious Use/Vandalism– Users may not engage in any malicious use, disruption or harm to the school district's computers, electronic devices, network and internet services, including but not limited to hacking activities and creation/uploading of computer viruses.

8. Avoiding School Filters– Users may not attempt to use any software, utilities or other means to access internet sites or content blocked by the school filters.

9. Unauthorized Access to Blogs/Social Networking Sites, Etc.– Users may not access blogs, social networking sites, etc. prohibited by school administration or the Technology Department. Teachers and students using authorized social networking sites for educational projects or activities shall follow the age requirements and legal requirements

that govern the use of social networking sites in addition to the guidelines established in this policy.

10. Degrade System Resources– Users shall not use the network in such a way that would degrade the performance system resources or disrupt the use of the network by others. This includes but is not limited to excessive printing, file storage, online games, and video/audio streaming not directly related to educational projects, as determined by the supervising instructor or school administrator.

11. Unauthorized Equipment– Users may not attach unauthorized equipment, including personal laptops, tablets, and handheld devices, to the district network without permission from the school administration or the Technology Department.

Safety/Security

All users are given accounts upon entry into Baldwin County Schools. Any user account given is intended for the sole use of that user only. Each user is responsible for the security of the system. Passwords should not be shared. If a user shares a password with another, that user will be held accountable.

Users may not reveal personal information, including a home address and phone number, about themselves or another individual on any unsecured electronic medium, such as web sites, blogs, podcasts, videos, wikis, or social networking sites. If users encounter dangerous or inappropriate information or messages, they shall notify the school administration immediately.

Staff may post student pictures on district/ school/classroom "public" websites as long as the student's name or other identifying information is not included. Students' grades, test results, or identifying pictures may be stored only on district-approved secure sites that require a username and password for authorized individuals to access.

Using electronic devices to make video/sound recordings or digital images of others without the consent of those being recorded is strictly prohibited. Restrictions against inappropriate language apply to all communication throughout the district network, including but not limited to public messages, private messages, and material posted on web pages. The use of cameras in any type of electronic device is strictly prohibited in locker rooms and restrooms.

School staff must maintain the confidentiality of student data in accordance with the Family Education Rights and Privacy Act (FERPA).

Students may be issued a school email address to improve student communication and collaboration on school projects. Email shall be used only for educational purposes that directly relates to a school project or assignment.

Damage/Liability
Users may be responsible for compensating the school district for any losses, costs or damages incurred for violations of Board policies/procedures and school rules, including the cost of investigating such violations. The school district assumes no responsibility for any unauthorized charges or costs incurred by users while using school district computers, devices, or the school network.

Expectation of Privacy

No right of privacy exists in the use of technological resources provided by the school. School system administrators or individuals designated by the Superintendent may review files, internet history logs, monitor communications/content activities, and intercept email messages to maintain system integrity and to ensure compliance with board policy and applicable laws and regulations. School system personnel shall monitor online activities of individuals who access the internet via school owned computers.

Terms of Use
Baldwin County Schools reserves the right to deny, revoke or suspend specific user privileges and/or take other disciplinary action, including suspensions or expulsion from school, for violations of this policy. District and technology administration reserves the right to examine, use and disclose any data found in the district network and/or equipment in order to further the health, safety, discipline or security of the school community. Additionally, all handbook regulations apply to the use of the district network, internet, and electronic resources.

Disclaimer
Baldwin County Schools, its employees and agents, make no warranties of any kind, neither expressed nor implied, concerning the network, internet access, and electronic resources it is providing. Furthermore, the district is not responsible for:
- The accuracy, nature, quality, or privacy of information stored on local servers or devices or information gathered through internet access.
- Any damages suffered by a user (whether the cause is accidental or not) including but not limited to, loss of data, delays or interruptions in service, and the infection of viruses or other malware on personal computers or other devices.
- Unauthorized financial obligations resulting from the use of BCSD electronic resources.

Examples of Acceptable Use
I will:
1. Use school technologies for school-related activities.
2. Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline. Be courteous and respectful.
3. Not post any information that I would not want students, parents, teachers, or future colleges or employers to see (once something is online, it is available to the world).

4. Treat school resources carefully, and alert staff if there is any problem with their operation.
5. Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
6. Alert a teacher or other staff member if I see threatening, inappropriate, or harmful content (images, messages, and posts) online.
7. Use school technologies at appropriate times and in approved places, for educational pursuits.
   Cite sources when using online sites and resources for research.
8. Recognize that use of school technologies is a privilege and treat it as such.
   Be cautious to protect the safety of others and myself.
9. Help to protect the security of school resources.

Examples of Unacceptable Use

I will not:
1. Use school technologies in a way that could be personally or physically harmful
2. Attempt to find inappropriate images or content; intent to seek inappropriate images or content is a violation of this Responsible Use Policy.

3. Create a personal mobile "hot-spot" or utilize a "proxy site" for the purpose of circumventing network safety measures and filtering tools.

4. Create, distribute or deploy multi-user servers or gaming software on or within the MPS network.
5. Engage in cyberbullying, harassment, or disrespectful conduct toward others.
6. Try to find ways to circumvent the school's safety measures and filtering tools; intent to circumvent safety measures and filtering tools is a violation of this Responsible Use Policy.
7. Use school technologies to send spam or chain mail.
8. Plagiarize content I find online.
9. Post or otherwise disclose personally identifying information, about others or myself.
10. Agree to meet someone I meet online in real life.
11. Use language online that would be unacceptable in the classroom.
12. Use school technologies for illegal activities or to pursue information on such activities.
13. Attempt to hack or access sites, servers, or content that isn't intended for my use.
    This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

CIPA

Baldwin County Schools is in compliance with the Children's internet Protection Act (CIPA) and has installed technology protection measures for all computers in the school corporation. A technology protection measure is in place that blocks or filters internet access. This filter protects against access by adults and minors to visual depictions that are obscene, child pornography, or — with respect to use of computers with internet access by minors — harmful to minors. The content filter does monitor the online activities of minors and may be reviewed when deemed necessary.

The district has the right to place reasonable restrictions on the material you access or post through the system. Students who violate the RUP will be subject to student disciplinary code outlined in the Medford Student/Parent handbooks.

The Acceptable Use Policy (AUP) applies to:

School-owned technology on the district internet/network, on non-school networks and offline

Privately owned technology that is connected to the district internet/network and on privately owned networks while on school property