



Technology Acceptable Usage Agreement (AUA)

Contents

PURPOSE.....	2
POLICY STATEMENT	2
INTRODUCTION.....	2
ACCESS.....	3
DATA PRIVACY & SECURITY.....	5
APPLICATIONS, SOFTWARE AND WEB SERVICES	6
GUIDELINES REGARDING EMPLOYEES & STUDENTS BRINGING PERSONAL DIGITAL DEVICES TO SCHOOL AND SCHOOL-SPONSORED ACTIVITIES	8
PURCHASING HARDWARE, SOFTWARE, APPLICATIONS AND WEB SERVICES.....	8
GUIDELINES FOR LIVE-STREAMING/RECORDING OF CLASSROOM INSTRUCTION.....	9
RECOMMENDED SYLLABUS STATEMENT	11
EXAMPLES OF INAPPROPRIATE USE OF RESOURCES:	12

PURPOSE

The purpose of the Baldwin County Board of Education (BCBOE) is to provide an effective, challenging, and engaging education for every one of our students. The intended use of technology is to enhance the educational experience of students by direct interaction with technology, and to indirectly enhance the educational experience of students by allowing faculty and staff to access and process important information in a timely and efficient fashion.

POLICY STATEMENT

An Acceptable Use Agreement (AUA) is a policy that outlines, in writing, how Baldwin County Board of Education expects its community members to behave with technology. Like a Terms of Service document, an AUA should define publicly what is deemed acceptable behavior from users of hardware and information systems such as the Internet, computers, laptops, tablets and any applicable networks.

The primary goal of the technology environment is to support the educational and instructional endeavors of students and employees of Baldwin County Public Schools. Use of any and all technology resources is a privilege and not a right.

Any questions about this agreement, its interpretation, or specific circumstances shall be directed to the Chief Technology Officer before proceeding. Violations of this policy will be handled in a manner consistent with comparable situations requiring disciplinary and/or legal action.

INTRODUCTION

To ensure that students receive a quality education and that employees can work in a professional and intellectually stimulating environment, it is the policy of the Baldwin County Public school district to provide all students and employees with access to a variety of technology resources. All Baldwin County students and staff must acknowledge and adhere to this policy.

The creation of a large and varied technology environment demands that technology usage be conducted in legally and ethically appropriate ways, consistent with the purpose statement and instructional goals of the Baldwin County Public school district. We recognize that the use of technology always requires attempts to balance the benefits against the possibilities of danger, security problems, and abuse. Rapid changes in technology and growth in the range of content available makes this a constant challenge.

Thus, it is the intention of the Baldwin County Public Schools that all technology resources be used in accordance with any and all board policies and procedures as well as local, state, and federal laws and/or guidelines governing the usage of technology and its component parts. Additionally, it is implied that all students and employees of Baldwin County Public Schools will use the provided technology resources so as not to waste them, abuse them, interfere with or cause harm to other individuals, institutions, or companies.

Aspects of this agreement may specifically address technology equipment personally owned by school system employees and/or students and brought into school facilities or onto school campuses to access school resources and/or personal resources. All personal technologies used on any Baldwin County Public campus are subject to this policy and may be used only if such usage is in compliance with all school system policies, procedures, and guidelines as well as local, state, and federal laws. No technologies may be purchased, brought on campus, or used to access school system resources that interfere with or adversely affect functions or operations of school system technology resources/infrastructure. All technology purchases must go through BCBOE Data Governance process.

The BCBOE Governance Committee will issue further specific guidelines detailing appropriate and legal use of copyright, email, technology resource purchasing and disposal, web page creation and maintenance, and the publication of student work. These guidelines are updated as best practices dictate and as case law emerges. These guidelines are considered appendices of the Baldwin County Board of Education Technology Acceptable Usage AUA. Students and staff are expected to be aware of and follow the guidelines which are updated annually and posted on BCBOE's public website Technology page and referenced in the Employee Handbook and/or the Student Handbook that must be signed annually.

BCBOE Superintendent, Assistant Superintendents, Chief Technology Officer, Security Manager, and/or School Principals will determine when inappropriate use has occurred, and they have the right to deny, revoke, or suspend specific user access and use of any technical resource.

ACCESS

Access to email, cloud or web services through the Internet use refers to internet access via all Baldwin County Public Schools/Private and public networks. The use of all Baldwin County Public Schools technology resources is a privilege, not a right, and inappropriate or suspected inappropriate use will result in a cancellation of those privileges, pending investigation. Moreover, users of BCBOE technology and infrastructure must be aware that Baldwin County Public Schools cannot assume any liability arising out of the illegal or inappropriate use of technology resources.

Users should not have any expectation that their use of technology resources, including files stored by them on the BCBOE's network, or data services, will be private and will be secure from access by others. Reasonable steps will be taken to maintain the security of technology resources, but no assurance can be given that penetration of such security will not occur.

In accordance with the requirements of the Children's Internet Protection Act (CIPA), all district computers that can access the Internet will be filtered. All traffic on BCBE devices, at school or home is filtered via web filtering appliance or application.

Once a student, employee, and or a guest accesses any of BCBOE technology resource they must comply with the Acceptable Use Agreement (AUA.)

- Individuals identified as a real or suspected security risk will be denied access. This access denial could include but not limited to Student Information System, Accounting Software, Human Resource Data Systems and network access. If a staff member fails to demonstrate the capacity of understanding how a system works that staff members can be denied access to that data. Defined data owners are accountable for quality, access and safety of the BCBOE data.
- Any use of technology resources, regardless of ownership, that reduces the efficiency of use for others will be considered a violation of this policy.
- Individuals must not attempt to disrupt any technology services or data integrity by engaging in inappropriate activities. Examples include, but are not limited to, spreading viruses, spamming, excessive network and/or Internet activity, or modification of equipment or infrastructure.
- Individuals must not attempt to modify technology resources, utilities, and configurations, and/or change the restrictions associated with his/her accounts, or attempt to breach any technology resources security system or filtering systems, either with or without malicious intent.
- Internet activity can and will be monitored, along with other aspects of technology usage.
- Successful or unsuccessful attempts to bypass the Internet filter by using proxies or other resources are a violation of this policy. Use of proxies are strictly prohibited!
- Access to BCBOE technical resources is limited to usage associated with activities of Baldwin County Public Schools. The technical resources cannot be used for profit, for commercial purposes, to express personal opinions, or to editorialize.
- Personal technology-related devices such as, but not limited to laptops, cell phones, smart-phones, iTouch/iPods/iPads, smartboards, cameras or other eDevices, etc. used on school grounds are subject to all items covered in this policy and other applicable published guidelines. The permission for such personal devices to be brought to school and the use of such devices will be at the discretion of the Superintendent, Assistant Superintendent, Chief Technology Officer or by a school nurse if it is a medical device. Public Internet access (guest wireless network) is designed for temporary use and is available for visiting devices. However long-term Wi-Fi access is provided for non-BCBOE employees that work within our district. Long term access requires a school principals' or senior administrators' authorization and must be renewed annually. All access to the guest Wi-Fi is subject to the conditions outlined in this policy and all other board policies and guidelines, as well as local, state, and federal laws.

DATA PRIVACY & SECURITY

BCBOE takes seriously its obligations to secure data systems and protect the privacy of students and employees. Strict processes help safeguard the confidentiality and security of the data. Students and Employees must:

- Employees may use only accounts, files, software, applications and/or other technology resources that are assigned to, provided, or approved for him/her. (Personal web drives (i.e., Dropbox, google drives and other web storage capabilities are unacceptable to use with district information and student records.)
- Staff and Students should not have any expectation that their usage of such resources is private. Reasonable efforts will be taken to maintain security of technology resources, but BCBOE cannot ensure that such security will not be penetrated or breached and cannot assume any liability arising out of any such penetration or breach of security.
- Employees are prohibited from emailing outside the school system or storing/saving on external storage devices or portable devices that do not remain on within official district systems, electronic copies of student or staff personal information. This information includes, but is not limited to data containing social security numbers, information protected by FERPA, and any other sensitive and/or protected information. If this type of information is stored on a portable or external device and said device is lost or stolen or if the security of this data is believed to have been breached in any way, the Chief Technology Officer should be notified immediately.
- All electronic content stored on any external storage medium or personal off-site storage location that is brought to or accessed from a BCBOE is subject to all Board policies and guidelines, as well as local, state, and federal laws.
- Because communications on the Internet are public in nature, all Staff and Students should be careful to maintain appropriate and responsible communications.
- Staff and Students are encouraged to avoid storing personal and/or private information on the district and/or school's technology resources. Users must be careful of **social engineering**, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence tricks for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme. Users are still responsible for any type of data breach they create regardless of falling prey to social engineering.
- Staff and Students must take all reasonable precautions to prevent unauthorized access to accounts and data and any other unauthorized usage within and outside the Baldwin County Public Schools. Any such unauthorized usage shall be reported immediately to the BCBOE Chief Technology Officer.

- All Staff and Students shall be responsible for reporting suspected or actual breaches of data security whether due to inappropriate actions, carelessness, loss/theft of devices or failures of technical security measures.
- Staff and students may not attempt to log into the network or application using any account and/or password other than the login(s) assigned to him/her. Individuals may not allow someone to use his/her network account and/or password to access the network, email, specific software packages, or the Internet.
- Students and staff are expected to follow all local, state and federal laws and system policy regarding the protection of student and staff confidential data.

APPLICATIONS, SOFTWARE AND WEB SERVICES

Baldwin County Board of Education provides numerous accounts for employees such as Microsoft Office 365 and for students Google eMail, which will allow full use and participation of Google Apps for Education. However, students are only allowed/limited to communicate with iBaldwin.org and bcbe.org domains only. This means students can only email internally to BCBOE administrators, teachers and other students. E-mail accounts are provided to ensure all employees and students use technology to communicate in schools for school related purposes in an appropriate manner, and to support teaching and learning. Some of these learning activities may include collaborating on live digital projects, shared writing projects, peer editing, share presentations, collaborating with fellow students, using spreadsheets, documents, and presentations, etc. With this opportunity comes responsibility. It is important that all employees, parents and students read and understand this Acceptable Use Agreement and ask questions if needed. Please note that BCBOE will take all reasonable steps to preclude access to objectionable material. However, it is not possible to absolutely prevent such access. It will be the responsibility of employees and students to follow the rules of appropriate use.

- Baldwin County Board of Education provides email accounts for all employees, long-term substitutes, and, in our secure cloud (secure online applications and storage), for students. Privacy and state regulations limits email accounts to employees and enrolled students only. Short term subs or non-BCBOE employees will not be provided with an E-mail address or iNow accounts. Data Governance Committee recommend exceptions for Superintendent's approval.
- Personal use of email or web service by BCBOE Staff is permitted if it does not violate Baldwin County Board of Education policy and/or adversely affect others or the speed of the network.
- Use of Baldwin County Public Schools' email or web service accounts for harassing or threatening is strictly prohibited.
- Baldwin County Public Schools' email or web service type of accounts may not be used for political activity, personal gain, commercial purposes, or profit.

- When using email, web and cloud service, all users are responsible for maintaining professionalism at all times. Avoid impulsive and informal communication. Users must be constantly mindful of the need to review carefully and reconsider their content and communications before responding to and/or sending any type of digital communication. As a rule, the content of an email should be acceptable to a general audience.
- Baldwin County Public Schools' email, web and cloud service accounts may not be used for attempting to send or sending anonymous messages.
- Baldwin County Public Schools' email, web and cloud service accounts may not be used for sending mass emails and/or text messages unless to parent lists or for other educational purposes. All mass emails need to flow the Communications Department.
- Baldwin County Public Schools' email, web and cloud service accounts may not be used for posting or forwarding other user's personal communication without the author's consent.
- Because email, web and cloud service is not securely transmitted, discretion must be used when sending, or encouraging the receipt of email containing sensitive information about students, families, school system employees, or any individuals. There can be no assurance that email will be confidential and/or private.
- All users are responsible for their individual assigned account. All users are responsible for not sharing their passwords with others and will be held accountable if another person utilizes their account inappropriately.
- Incoming and outgoing email or web service are filtered by the district for inappropriate content, viruses, phishing, and/or malware.
- All BCBOE staff accounts including district-issued email, student information, human resources, and financial systems will **automatically** expire on the last full day of employment.
- All BCBOE student accounts including district-issued email and educational software accounts will be disabled following the last day of enrollment or upon graduation.
- At the discretion of the Superintendent, email or web services accounts may be locked without notice. Violation of the Acceptable Use Agreement can result in revocation of any system account, such as email, legal action in accordance with employee manual or student code of conduct, or applicable laws.

GUIDELINES REGARDING EMPLOYEES & STUDENTS BRINGING PERSONAL DIGITAL DEVICES TO SCHOOL AND SCHOOL-SPONSORED ACTIVITIES

- Staff and students are under the same guidelines with personal digital devices as they are when using computers and other digital devices at school and at school-sponsored events. The Acceptable Usage Agreement that all employees, students and parents sign each year applies to but is not limited to all digital devices, storage devices/media, and digital content. Staff and Students are subject to disciplinary action for misuse of personal devices during the school day or at school-sponsored activities. For example, cyberbullying, harassment, accessing of pornographic or other inappropriate content, and other misuses of technology—even personal technology—are subject to disciplinary action when they occur at school or at school-sponsored activities.
- School filters are automatically employed for Wi-Fi connections to Baldwin County Public Schools guest networks. However, schools have no way to filter content that comes to personal devices via cellular (4G/5G/LTE) data plans. Particularly at the elementary level, we recommend students NOT bring personal devices with data plans, but if they are brought, we recommend they not be used during the school day.
- Texting, making phone calls, taking pictures or making videos, emailing, messaging, gaming, and accessing digital content is a privilege that is extended in our schools, which can be withdrawn at any time at the discretion of the teacher or school administration. Violating any of these rules will result in losing digital device privileges for a period of time to be determined by the administration.
- The school system or school system employees are not responsible for any damages to or loss of personal devices brought to school by students or its employees.

PURCHASING HARDWARE, SOFTWARE, APPLICATIONS AND WEB SERVICES

With the 1:1 initiative and new state and federal privacy regulations we are now require changing our mindset on purchasing, sustaining and maintaining resources which requires an executive / centralized review process. This is becoming even more important as our student, financial, human resources, and administrative data is dependent on the exchange of data between systems and the escalation of legal review prior to entering and maintaining any service or agreement. To this end, we are putting in new controls to ensure that the technology infrastructure is consistent and stable. Based on this, we have instituted the Data Governance Committee (DGC). This governance board requires that any new hardware, software applications and web services be vetted for compliance and data quality to remove duplication of effort and data. A thorough review will take place and recommendations will be made for the Superintendent's /Board's approval to purchase. This procedure is intended to provide for the proper purchasing and disposal of technological devices only. Staff and must follow these guidelines:

- Staff and students should not purchase or dispose of software, hardware, peripherals, or other technology-related devices without consulting the Educational Technology staff and guidelines established for the district. Regardless of purchase date, location or funding source, all personnel should adhere to the *Technology Purchasing and Disposal Guidelines* regarding all purchases and disposals.
- Illegal copies of software/media may not be created or used on school equipment.
- Legal and ethical practices of appropriate use of technology resources are reviewed with students and employees in the system (i.e. as part of the Technology Education Curriculum, during orientation sessions, faculty meetings, or through online methods, etc). Again, all questions regarding legal and ethical practices of appropriate use should be directed to the district's Chief Technology Officer.
- Copyright is implied for all information (text, data, and graphics) published on the Internet. Student and employee web page authors will be held responsible for the contents of their pages. Do not "borrow" icons, sounds, or graphics from other pages without documented permission. It is the student's or employee's responsibility to secure proper usage permission.
- Duplication of any copyrighted software/media is prohibited unless specifically allowed in the license agreement and, then, should occur only with the knowledge of the technology staff.
- Free educational software and web services are always encouraged to be used within a classroom or for an educational endeavor. However, each staff member must not allow or encourage the use of any software or web service purchased for free if it requires student information that is not deemed student directory information without a contract/agreement in place to protect student privacy. Access to free software applications and web services must be approved by the Data Governance Committee.
- Data Governance Committee will post an authorized list of software and services. Superintendent or his/her designee is authorized to sign license acknowledgements for a school within the system. Copies of any system-wide license agreements must be maintained and inventoried by the district Chief Technology Officer and/or Superintendent and distributed to all schools that will use the software. All binding contracts/agreements must be signed by the Superintendent.

GUIDELINES FOR LIVE-STREAMING/RECORDING OF CLASSROOM INSTRUCTION

Federal and State laws safeguard students and their families against release of certain personally identifiable student information maintained by schools in a child's education records. The Baldwin County Public School System understands that from time to time teachers may wish to live-stream classroom instruction or record classroom instruction to aide student learning. Personally identifiable student information in a recording of a class may constitute an educational record protected under FERPA. To ensure compliance with any applicable Federal or State laws, the Baldwin County Public School System

provides the following as guidelines for each teacher's classroom should that teacher wish to live-stream or record classroom instruction.

- In accordance with FERPA, the Baldwin County Public School System has designated that photographs and/or video images of students constitutes "directory information" that may be disclosed without prior parental consent. When recording or live-streaming classroom instruction, certain information contained on video can go beyond a video image that the school system has classified as directory information. Put another way, when a teacher live streams or records classroom instruction, certain information within that video may go beyond routine activities of students, i.e. information on the live feed or recording may be directly related to a particular student and provide more than just a video image of the student. For example, if any of the following is shared within the live feed or recording, it may go beyond what has been classified as directory information under FERPA: disclosing a student's name, discussing confidential information about the student's status in the class, disclosing a particular student's schedule and location throughout the school day.
- To prevent the disclosure of personally identifiable information in a student's education record, if school staff intend to live stream or record classroom instruction, it is best practice that school staff provide notice to students and parents that recordings or live-streaming will take place, for what reason(s) the recording/live-streaming may be reviewed, and by whom. School staff should provide this information to students and parents in the class syllabus as well as in specific class sessions prior to an event.
- Teachers and staff should be aware of those students enrolled in their classrooms who have given notice to the Baldwin County Public School System that the parent or student has chosen not to have their "directory information" disclosed. Those students who have opted out of FERPA directory information should not be included in any video recordings or live streaming.
- Teachers and staff should avoid directly recording student faces during classroom instruction. If the recording (audio and video) includes only the instructor, it is not a student educational record and not subject to FERPA guidelines. Teachers should try to plan recordings so that they do not show students who are asking questions, don't refer to students by name, and avoid repeating a student's name in a recording. If a student happens to appear on camera during classroom instruction, his or her identity can be edited out or a written consent obtained as discussed below.
- If students are personally identifiable in the live-stream or recording of any classroom instruction, school staff should make sure the live stream or video recording does not indicate the time of day or actual class period where the student is located.
- If students are personally identifiable in the live-stream or recording of classroom instruction, school staff can limit those who access the live-stream or video recording to only other students currently enrolled in the class. This limitation would allow instructors to create access for only those students enrolled in the class to watch or re-watch past class sessions and would not be a disclosure of education records under FERPA.
- If students enrolled in the class will be permitted to review a recording in which a student is identifiable, the syllabus should clearly outline that students are prohibited from capturing or copying the live-stream feed or recording by any means and sharing with others. It should be noted in a classroom teacher's syllabus that students violating this prohibition would be

violating the Baldwin County Public School System's Acceptable Use Policy and could result in disciplinary action against the student.

- Should school staff wish to use a recording outside of the classroom, with access being provided to individuals not enrolled in the class, the teacher or staff member should do one of the following:
 - Edit to either omit any student who has not consented to the use of their voice or image, or edit to de-identify the student in the recording (which can include avoiding or removing any mention of the student's name, blurring the student's image, altering voice recordings etc.);
 - Obtain individualized written FERPA consent from the parent of the student in the recording to allow the use of the recording. This can be requested of all students at the outset of a class or be obtained on a case-by-case basis in the event the teacher knows that a videos or live-streaming will be made accessible to individuals not enrolled in the class. A template for consent for educational use is provided below. Teachers or staff members should ensure the exclusion of students in classroom videos based on denial of parental permission.
 - A parent's consent to his or her child to appear in a recording must be both informed and voluntary. The request for consent must inform the parent of all the intended uses of the recording. Voluntary means that a consent is freely given without persuasion or coercion and that the student receives neither advantage nor disadvantage by providing consent.
 - The parent's consent must be in writing, signed and dated. The consent should be included with the classroom syllabus and specify the records that may be disclosed, the purpose of the disclosure, and identify the parties to whom disclosure must be made.
 - A student must have the same educational experience as students willing to be recorded if a parent chooses to not have his or her student appear in a recording. Any student whose parent has opted him or her opted out of the disclosure of "directory information" as discussed above, should also have the same educational experience as students whose parents have not opted out.
 - If a parent wishes for his or her child to be excluded from any recordings, a recording may still be made as long as it contains no record of that student.
 - The practices and guidelines contained herein specifically apply to video recordings or live-streaming of a teacher's classroom instruction. In regards to any other filming or photographing of students, all school system staff are still expected to comply with FERPA in regards to the disclosure of personally identifiable information within a student's education record when such records are maintained by the Baldwin County Public School System. Accordingly, prior parental consent is not required for photographing or videotaping of students when the photograph or video falls under the definition of "directory information" as identified by the Baldwin County Public School System.
 - Videos involving incidents of student discipline should not be posted or shared with anyone.
 - School system staff should not take videos or photographs of students in areas where an individual might have a legitimate expectation of privacy such as a rest room or locker room.

RECOMMENDED SYLLABUS STATEMENT

Class Recordings: Instruction in this class might be recorded or streamed live. Any recordings will be available to students enrolled in this class. This is intended to supplement the classroom

experience. Students are expected to follow appropriate school system and campus-wide policies and maintain the security of passwords used to access classroom recordings. Live streaming and recordings may not be captured or reproduced, shared with those not in the class, or uploaded to other online environments. Doing so would be a breach of the Baldwin County Public School System's Acceptable Use Policy. If I, or an administrator plan to use any recordings, beyond the classroom environment, students identifiable in the recordings will either be de-identified or will be notified prior to in order to obtain proper consent prior to such use.

EXAMPLES OF INAPPROPRIATE USE OF RESOURCES:

This list is not all-inclusive but is intended to provide general guidance. Anything that would be considered inappropriate in "paper form" or "verbal form" is also considered inappropriate in electronic form. Information, such as but not limited to Student Information System (SIS) data, accessed through school system technologies may not be used for any private business activity. The following are examples of inappropriate activities when using any Baldwin County Public Schools' network, email system, hardware, software, technology services, and/or Internet access:

- Sharing passwords
- Using another user's password or attempting to discover another user's password
- Trespassing in another user's files, folders, home directory, or work
- Saving information on any network drive or directory other than your personal home directory or a teacher-specified and approved location
- Downloading, installing, or copying software of any kind onto a computer, laptop, home directory, network drive, or other electronic device (except for approved updates or apps)
- Harassing, insulting, embarrassing, or attacking others via technology resources
- Damaging/abusing technology resources, including, but not limited to, printers, telephones, computers, computer systems, any e-device, or computer networks (this includes changing workstation configurations such as screen savers, backgrounds, printers, BIOS information, preset passwords, etc.)
- Intentionally wasting limited resources such as Internet bandwidth, disk space and printing capacity
- Accessing inappropriate material stored on resources such as, but not limited to, digital cameras, flash drives, iPods, online storage, cell phones, web sites, etc.
- Accessing inappropriate material from web sites or attempting to bypass the Internet filter to access web sites that have been blocked (Examples: information that is violent; illegal; satanic; sexual; demeaning; racist; inflammatory; and/or categorized as a social networking, blogging, or journaling sites, etc.)
- Sending, displaying, or downloading offensive messages or pictures
- Using obscene, racist, profane, discriminatory, threatening, or inflammatory language in a document, email, etc.
- Using a digital camera, camera phone, or any other device capable of storing a still or video image to take inappropriate, harassing, and/or embarrassing pictures
- Editing or modifying digital pictures with the intent to embarrass, harass or bully is prohibited

- Participating in unsupervised or non-instructional on-line chat rooms without the permission/supervision of an adult staff member
- Posting any false or damaging information about other people, the school system, or other organizations
- Posting of any personal information as defined previously in this document
- Broadcasting network messages or participating in sending/perpetuating chain letters
- Violating copyright laws
- Plagiarism of materials
- Use of technology resources to create illegal materials (i.e. counterfeit money, fake identification, etc.)
- Use of any Baldwin County Public Schools Technology resource for personal gain, commercial or political purposes
- Accessing any website or other resources by falsifying information
- Downloading games or playing games on-line that are not instructional in nature or directed
- Streaming video or audio not related to the core business of the School System