Echols County Schools

Technology Acceptable Use and Internet Safety Agreement

Students 2024-2025

Please read this agreement carefully as it contains important information, requirements, and expectations for your use of technology at Echols County Schools ("ECS"). While your signature is requested to acknowledge your receipt and understanding of this agreement, please note that that ***this agreement applies to your or your student's use of technology at ECS with or without your signature.***

Introduction

The goal of the Echols County Board of Education (the "Board") is to provide Internet/intranet service and technology to teachers, staff, and students to promote educational excellence and facilitate resource sharing, innovation, and communication. It is important to note that the use of this technology ***is a privilege, not a right***. To aid ECS's students in understanding and implementing appropriate technology practices, the Technology Acceptable Use and Internet Safety Agreement (the "AUA") is set forth and governs student use of ECS technology resources, defined as including any computer, server, network, digital storage media, mobile, cloud, software, or electronic device, including the Internet and intranet. The "user" is defined as a person authorized to use some or all ECS technology devices, subject to the AUA, Board policy, and state and federal law. Each user of ECS technology resources is responsible for their actions and activities involving ECS computers, technology, and the network.

Due to the nature of technology use and the Internet, it is neither practical nor possible for the Board, ECS school administration, or ECS staff to monitor student use and enforce compliance with this AUA at all times. Accordingly, parents and students must recognize that students will be required to make independent decisions and use good judgment in their use of the ECS technology resources and the Internet. Parents/guardians must participate in the decision whether and how to allow their children access to the Internet and must communicate their own expectations to their children regarding its use.

Penalties

Any user violating this AUA, applicable state and federal laws, posted classroom rules, or ECS policies is subject to loss of ECS technology resource privileges and any other ECS disciplinary options in accordance with the Students' Handbook and Code of Conduct, and if applicable to the conduct, possible involvement of law enforcement agencies. Illustrations of disciplinary options are contained in the Teachers' Handbook and Students' Handbook. Although some specific examples of prohibited uses are stated, these are intended as illustrations and are not to be considered an inclusive list. ECS school administrators will make the determination as to what constitutes unacceptable use of ECS technology resources, and their decision is final. The users and/or the users' parent(s)/legal guardian(s) shall be responsible for compensating ECS for any losses, costs, or damages incurred by ECS relating to or arising out of the user's violation of this AUA.

ECS Commitments

ECS is committed to:

- Preventing user access over the ECS network to, or transmission of, inappropriate material via Internet, electronic mail ("e-mail"), or other forms of electronic communications;
- Preventing unauthorized access to the ECS network and other unlawful activity;
- Preventing unauthorized and/or unlawful disclosure, use, access, or dissemination of ECS student records and other legally protected information; and
- Complying with the Children's Internet Protection Act ("CIPA") and all applicable state and federal laws.

ECS Monitoring, Filtering, and Threat Protection Scanning

To protect users against access to inappropriate materials on the intranet/Internet, ECS has installed a qualifying "technology protection measure" as that term is defined in CIPA. This firewall and filtering program is to designed to prevent access to visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors as those terms are defined by CIPA. This program filters and blocks only **known** sites that feature nudity, pornography, violence, hatred of others, inappropriate chat rooms, and inappropriate language. The list of restricted sites is updated daily; however, inappropriate sites are published frequently during the day, and no filtering software has proven to be 100% effective. Furthermore, the user is responsible for not seeking or initiating access to inappropriate material.

ECS reserves the right to review any information, files, or documents that are stored within or transmitted by an ECS technology resource or on the ECS network without the student's knowledge or consent. This monitoring is intended to determine whether specific uses of the network and technology are appropriate and for ECS to remain in compliance with state and federal law. ECS uses a monitoring and alert system to identify incidents of cyberbullying, violence, self-harm, inappropriate content, and violations of FERPA and CIPA in ECS-provided Office 365 accounts for all faculty, staff, and students. Scanning includes Outlook email and all Office 365 features (Documents, Spreadsheets, Presentations, PDFs, Images & Photos, Videos) and all file types supported in Microsoft One Drive. ECS seeks to provide improved data security and insights into potential exposures through this scanning process.

A list of software/applications used by ECS students is available on the district website https://echolscountyboe.schoolinsites.com/ at Technology>Technology Documents.

Expectations and Acceptable Use

- Usage of ECS technology resources must be in support of academic purposes and consistent with Board policy and this AUA. Students will use ECS technology resources in ways that are appropriate and meet ECS expectations--whether at school, at home, or anywhere else.
- Students will login using their ECS network assigned username and password (when provided to the student). Students will protect their password information and not share with anyone other than a teacher or ECS staff member or their parent/guardian.
- Students shall use their ECS-provided email account only for instructional purposes and as directed by his or her teacher (if provided an email account by ECS).

- Students shall notify the teacher if he or she inadvertently browses to an inappropriate site on the Internet.
- Students shall notify the teacher or school administrator if they receive any inappropriate messages that make them feel uncomfortable.
- Students will never loan out or share any ECS technology resources assigned to them.
- Students will keep food and beverages away from ECS technology resources to avoid damage.
- Students are responsible for not utilizing images that they do not own the copyright to. Students should only use images that are in the public domain, images of their own creation, or images that are permitted to be used by Creative Commons licenses for class projects.
- Students must give credit to and cite information used in a class project or paper to avoid plagiarism.
- Students should identify themselves by name only when posting on any wiki, blog, or other web-based tool provided by or authorized by ECS.
- Live streaming of video and audio, or any other streaming media, must be related to academic purposes and instructional objectives.
- Student computer files and activity are not private, and ECS staff and school administrators may see them at any time.

Unacceptable Use

These are intended as illustrations and are not an inclusive list. ECS school administrators will make the determination as to what constitutes unacceptable use of ECS technology resources, and their decision is final.

- Students may not use ECS technology resources for any illegal activity, including violation of copyright, cyberbullying, harassment, and any other violation of ECS policy, the Code of Conduct, state or federal law.
- Students will not use ECS technology resources to copy or download copyrighted software, music or images, or for other violation of copyright laws. Peer-to-peer, file-sharing, torrent software, and/or other forms of similar software may not be installed on an ECS computer or laptop.
- Students must not vandalize ECS technology resources or use them to harm, access, distribute, or destroy data of another user, individual, and/or the ECS network. This includes, but is not limited to, creating and/or uploading or downloading viruses, disconnecting, or disassembling any network or computer component.
- Students are not permitted to use the computer of a teacher, administrator, or other ECS staff member without permission or supervision. Students are not permitted to use the login or password of another user.
- Students cannot use ECS technology resources in such a way as to disrupt the ECS network's functionality or other users (sounds and/or excessive bandwidth usage, e.g., radio/audio streaming, video streaming).
- Students are not permitted to use ECS technology resources to access, monitor, or use personal websites and/or networks, for commercial gain, and/or for entertainment.
- Students are not permitted to bypass and/or attempt to circumvent ECS network security, virus protection, network filtering, and/or the ECS firewall.

- Students are prohibited from bullying and are not permitted to use ECS technology resources to threaten, harass, and/or intimidate others. Prohibited behaviors include, but are not limited to:
    - Accessing, contributing to, creating, or initiating inappropriate material on the Internet, including (but not limited to) abusive, obscene, sexually oriented material, or hate speech to communicate, or cause to be communicated through words, images, or language by or through the use of electronic mail or electronic communication, directed at or about a specific person, which may cause substantial emotional distress to that person or damage to their reputation.
    - Cyberbullying or the willful act of hostile or repeated harassing or intimidating of someone through digital technology, including but not limited to, email, blogs, social networking websites (ex: Facebook, Twitter, etc.), chat rooms, texts, and instant messaging.
    - Using cameras or camera phones to take embarrassing or inappropriate photographs or videos of student or school employees and posting them online.
    - Sending threatening or abusive text messages or instant messages or any social network or digital form.
    - Using the Internet, ECS technology resources, or email to propagate gossip or rumors to other students.
    - *Bullying and its consequences are described further in the ECBOE Bullying policy (JCDAG) and the Student Code of Conduct (JCDA).*
- Students are not permitted to connect any personal equipment to the ECS network.

No Warranties

ECS makes no warranties of any kind, whether express or implied, for the technology resources it provides. ECS will not be liable or responsible for any damages a user may suffer through use of ECS technology resources, including loss of data. ECS may not at any time be held responsible for any loss or damage to a student's personal device. Students bring devices at their own risk. Help and support will not be provided for personal devices.

Internet Safety Curriculum

To promote appropriate use of technology and to encourage students to be responsible digital citizens, the ECS Technology Department will develop and implement an Internet Safety Curriculum for all students PreK – 12th grade and ECS faculty/staff. The implemented curriculum is available upon request by contacting the ECS Technology Director.

Microsoft for Education (Office 365)

ECS adopted Microsoft for Education to provide online communication and productivity tools for students and teachers. Microsoft for Education accounts (Office 365) are provided to all students in grades Pre-K through 12. Active email accounts are only grades 6-12. Outlook (email) for grades Pre-K through 5 have not been activated at this time. Teachers and students will be able to create dynamic learning experiences in and outside of the classroom with an internet connection. Students will be able to share with teachers and collaborate with peers. MS for Education (Office 365) can be used to develop college and career ready skills of communication, collaboration, creativity and critical thinking.

ECS is providing this notification to the parents of children under the age of 13 to comply with the Children's Online Privacy Protection Act (COPPA). The only information ECS transfers to Microsoft in creating an account is the child's first name and last name. Student data will be used only to provide the student the Online Services including purposes compatible with providing those services. Microsoft will not use student data or derive information from it for any advertising or similar commercial purposes. Microsoft provides an overview of their commitment to student security and privacy at https://www.microsoft.com/online/legal/v2/?docid=31.

When there is reason to believe violations of law or district policies related to the AUA and Student Discipline Policy have occurred, ECS maintains the right to withdraw access to the student's Microsoft account. The alleged violation will be submitted to the ECS school administrator for further investigation as a written behavioral referral. Consequences for violations will be determined by the ECS Technology Director and the stated student discipline policy as deemed by the ECS school administrator.

Parents who object to their child using Microsoft for Education must contact their child's principal in writing within ten (10) days of the student's enrollment.

Please note that ECS student email accounts will remain active until July 1 following graduation for students to get their accounts in order.

Parents/Guardians:

I understand that the intranet/Internet access is designed for educational purposes and that ECS will attempt to discourage access to objectionable material and communications that are intended to exploit, harass, or abuse users. However, I recognize it is impossible for ECS to restrict access to all objectionable material, and I will not hold the school or district responsible for materials acquired or contacts made on the intranet/Internet network.

I understand that a variety of inappropriate and offensive materials are available over the Internet, and that it may be possible for my child to access these materials if he/she seeks these materials in contravention of this AUA or by accident. I also understand that it is possible for undesirable and/or unknown individuals to communicate with my child over the Internet, that there are no practical means for ECS to prevent this from happening, and that my child must take responsibility to avoid such communications if they are initiated. While I understand ECS may monitor any communications to or from my child and the Internet, I recognize that it is not possible for the school to monitor all such communications.

I have determined that the benefits of my child having access to the Internet outweigh potential risks. I understand that any conduct by my child that is in conflict with these responsibilities is inappropriate, and such behavior may result in the termination of access and possible disciplinary action and/or criminal prosecution.

I have reviewed these responsibilities with my child, and I hereby grant permission to the school to provide Internet and network access and ECS technology resources.

I agree to compensate ECS for any expenses or costs that incur as a result of my child's violation of the AUA, ECS policy, and/or the ECS Code of Conduct.

I understand that if I object to my child having access or rights to any portion of this AUA, as the parent/guardian, **I am required to submit a written letter to the school principal within ten (10) days of enrollment**. (If you have more than one child, a letter must be written for each child and presented to the appropriate school principal.) Students will only be excluded if written objection is presented to the principal of the school.

I understand that my child and I must complete the AUA sign-off or all student account(s) associated with my child will be suspended until all documentation is received. I understand, however, that my signature is not required on this AUA for its requirements to apply to my child.

Students:

I have read the AUA and understand and agree to abide by its requirements. I also understand that my signature is not required on this AUA for its requirements to apply to myself and my behavior.

Parent/Guardian Name (Printed)	**Date**
Parent/Guardian Signature	
Student Name (Printed)	**Date**
Student Signature (Grades 3-12 only)	**Grade**
Student Number (Lunch Number)	**1st Block or Homeroom Teacher**