

EACS Staff Technology Handbook



EAST ALLEN COUNTY SCHOOLS

DREAM IT. DO IT.

2017-2018

Revised June 2, 2017

Table of Contents

1. Technology Goals

2. Responsible Use Agreement

- a. Usage Policies
- b. Internet Access
- c. Web 2.0 (Email and Collaborative Content)
- d. Security and Passwords
- e. Downloads and Streaming Content
- f. Netiquette
- g. Personal Safety
- h. Cyber-bullying
- i. Examples of Responsible/Irresponsible Use
- j. Limitation of Liability
- k. Violations of the Responsible Use Agreement

3. iPad Policy

- a. Terms
- b. Title
- c. Loss or Damage
- d. Repossession
- e. Term of Agreement
- f. Unlawful Appropriation

4. Financial Terms of Mobile Technology Use

- a. iPad Costs
- b. Table of Estimated Repair Pricing
- c. Stolen, Lost, or Damaged iPads

5. Mobile Technology Precautions

- a. Handling and Care of the iPad
- b. Power Management
- c. Transport
- d. Monitoring and Supervision

1. Technology Goals

1. Equip all stakeholders to safely use technology to interact with, and impact, the world around them.
2. Teach the ethical use of technology.
3. Improve the quality of learning and promote greater academic achievement.
4. Develop a new set of knowledge and skills for teaching the 21st century learner.
5. Provide greater access to educational opportunities and differentiated instruction by utilizing access to technology for anytime, anywhere learning.
6. Improve communication and widen our sense of community by expanding the way teachers, students, and parents are able to interact with each other.
7. Expand integration of digital resources.

2. Responsible Use Agreement

A. Introduction

This Responsible Use Agreement (RUA) outlines the guidelines and behaviors that users are expected to follow when using school technologies or when using personally owned devices on the school campus. In addition to this policy, the use of any district provided technology requires students and staff to abide by the EACS Staff Technology Handbook Policies.

1. The EACS network is intended for educational purposes only.
2. All activity over the network or while using district technologies will be monitored and/or retained.
3. Access to online content via the network may be filtered in accordance with our policies and federal regulations, including the Children's Internet Protection Act (CIPA).
4. Users are expected to follow the same rules for good behavior and respectful conduct online as offline. Misuse of school resources can result in disciplinary action.
5. EACS makes a reasonable effort to ensure users' safety and security online, but will not be held accountable for any harm or damages that result from use of school technologies.
6. Users of the district network or other technologies are expected to immediately alert district personnel by the end of the next school day of any concerns for safety or security (duty to inform).

B. Technologies Covered

EACS may provide Internet access, desktop computers, iPads, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more. As new technologies emerge, EACS will assess the educational value and attempt to provide access to them. The policies outlined in this document are intended to cover *all* available technologies, not just those specifically listed.

C. Usage Policies

All technologies provided by the district are intended for educational purposes. All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, be appropriate, and be kind; use common sense, and ask if you do not know.

1. Users should abide by the same Responsible Use policies when using school devices off the school network as on the school network.
2. Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care.
3. Users should report any loss, damage, or malfunction to school personnel immediately.
4. Users may be financially accountable for any damage resulting from negligence or misuse.

D. Internet Access

District Provided Access- EACS provides its users with access to the Internet, including websites, resources, content, and online tools while on campus. That access will be restricted in compliance with CIPA regulations and school policies. Internet activity will be monitored and records will be retained indefinitely.

1. Users must understand that the Internet filter is a mandatory and vital safety precaution.
2. **Users must not circumvent the Internet filter.**
3. Users should follow district protocol to alert the Technology Department or submit a site for review if a site is blocked and the user believes it should not be.
4. Users should follow district protocol to report sites that are not blocked, but that the user feels should be blocked.
5. EACS will not provide wifi access on personal devices or non-district devices.
6. EACS will provide a limited media network access to the members of the media only.
7. EACS will provide a limited guest network for visiting presenters only.

Non-District Provided Access- EACS staff-utilized devices may be used on other wireless networks while off campus, but are subject to the restrictions outlined in the EACS Staff Technology Handbook.

E. Web 2.0 (Email and Collaborative Content)

Recognizing the benefits collaboration brings to education, EACS may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users. Availability and use may be restricted based on district policies.

1. District provided email accounts should be used with care.
2. Users' email usage may be monitored and archived to meet legal obligations.
3. Users should be careful not to share personally identifying information online. **Sharing inappropriate personal information or content is strictly prohibited.**
4. Users should be aware when opening files or following links from unknown or untrusted origin.
5. Users should communicate with appropriate, safe, mindful, and courteous conduct.
6. Users should be aware that third-party cloud-based storage tools such as iCloud Drive, Google Drive, and Canvas are not owned nor controlled by EACS.

F. Security and Passwords

Users are expected to take reasonable safeguards against the transmission of security threats (viruses, worms, spyware, etc.) over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin.

If a device is believed to be infected with a virus, please alert school personnel and HELPdesk immediately. The user should not attempt to remove the virus or download any programs to help remove the virus.

A User's access to any EACS computer system or the Network is by the use of a User ID and password combination. The password is required to be changed every 60 days. The password will be a minimum of 8 characters in length, and contain numeric and alphabetic characters. It is every User's obligation to maintain password security by not sharing their password, by logging off of devices when finished, and by changing the password at the required 60 day intervals. Each user will receive four emailed reminders to change the password during a 14-day span prior to the end of the 60 day interval.

G. Downloads and Streaming Content

Users may be able to download file types, such as images or videos; however, for the security of the district's network, such downloads should only be from reputable sites, and only for educational purposes. Streaming video and audio via video streaming services such as YouTube should also be used for educational purposes only, and in short clips of 10 minutes or less. EACS reserves the right to block all streaming audio and video services during periods of standardized testing. i.e. NWEA and ISTEP testing.

Examples of streaming media sites that are unacceptable include: Pandora, Spotify, Netflix, and Hulu.

H. Netiquette

1. Users should always use the Internet, network resources, and online sites in a courteous and respectful manner.
2. Users should recognize that among the valuable content online, there is also unverified, incorrect, or

inappropriate content.

I. Personal Safety

1. Users should recognize that communicating over the Internet brings the risks associated with the lack of face to face contact.
2. Users should carefully safeguard the personal information of themselves and others.
3. Users should be cautious when sharing personal information, including phone number, address, social security number, birthday, or financial information, over the Internet.
4. If the user sees a message, comment, image, or anything else online that makes him or her concerned for his/her personal safety, it should be brought to the attention of school personnel immediately.

J. Cyber-bullying

The National Crime Prevention Council defines cyber-bullying as: “When the Internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person.”

EACS Position on Cyber-bullying

1. Cyber-bullying will not be tolerated.
2. Engaging in cyber-bullying to harm (physically or emotionally) another person will result in severe disciplinary action and loss of privileges.
3. In some cases, cyber-bullying can be a crime.
4. The user should remember that activities are monitored and retained.
5. **Report cyber-bullying immediately to school personnel.**

K. Examples of Responsible/Irresponsible Use

Responsible:

- + Use school technologies for school-related activities.
- + Follow the same guidelines for respectful, responsible behavior online as offline.
- + Treat school resources carefully, and alert technology staff if there is any problem with their operation.
- + Upon creation of online collaborative discussions, it is a staff member’s responsibility to monitor student content and behavior within the online discussion.
- + Alert school personnel of threatening, inappropriate, or harmful content online.
- + Use school technologies at appropriate times, in approved places, for educational pursuits.
- + Recognize that use of school technologies is a privilege and treat it as such.
- + Communication with students should be via EACS’ Learning Management System (Canvas) or district Gmail accounts and **should be limited to educationally-related content.**
- + Communication with parents should occur via email, phone, or EACS’ Learning Management System.
- + Staff communication via social media with students/parents should be limited to educationally-related content

Irresponsible:

- Use school technologies in a way that could be personally or physically harmful.
- Attempt to find inappropriate images or content.
- Engage in cyber-bullying, harassment, or disrespectful conduct toward others.
- Try to find ways to circumvent the school’s safety measures and filtering tools.
- Use school technologies to send spam or chain mail.
- Plagiarize content found online.
- Agree to meet someone met online in real life.
- Illegal installation or transmission of copyrighted materials.
- Use language online that would be irresponsible in the classroom.
- Use school technologies for illegal activities or to pursue information on such activities.
- Attempt to hack or access sites, servers, or content that is inappropriate.
- **Downloading or viewing media labeled “Explicit”**
* This is not intended to be a complete list, just a few specific examples.

L. Limitation of Liability

1. EACS will not be responsible for damage or harm to persons, files, data, or hardware.
2. While EACS employs filtering and other safety and security mechanisms, and attempts to ensure their proper function; it makes no guarantees as to their effectiveness.
3. EACS will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

M. Violations of this Responsible Use Policy

Violations of this policy may have disciplinary repercussions, including:

1. Suspension of network, technology, or computer privileges
2. Suspension from duties
3. Legal action and/or prosecution
4. Financial Consequences

N. Social Media Use

Communication with students or parents via electronic communication such as texting, social media (social media includes, but is not limited to: Facebook, Instagram, and Twitter), blogs, and email *for educational purposes or co-curricular/extra-curricular events or activities only.*

3. iPad Policy

A. Terms

Users will comply at all times with the EACS Student Technology Handbook policies. Any failure to comply may terminate user rights of possession effective immediately and the district may repossess the property. **ANY LOST, STOLEN, OR DAMAGED iPad MUST BE REPORTED TO SCHOOL AUTHORITIES IMMEDIATELY, AND NO LATER THAN THE NEXT SCHOOL DAY.**

B. Title

Legal title to the property is in the District and shall at all times remain in the District. The user's right of possession and use is limited to and conditioned upon full and complete compliance with this agreement and the EACS Staff Technology Handbook policies.

C. Lost, Stolen or Damaged

If a staff or faculty member breaks or loses an iPad, the first time there will be no charge. If a staff or faculty member breaks an iPad a second time, he/she will pay the cost of repair/replacement. This applies for the duration of the cycle of iPad (or other device) adoption. Staff or faculty members may purchase the \$30 insurance through their building's treasurer, for their iPad, to protect against becoming damaged a second time.

D. Repossession

If the user does not fully comply with all terms of the EACS Staff Technology Handbook, including the timely return of the property, the District shall be entitled to take possession of the property.

E. Term of Agreement

The user's right to use and possess the device ceases upon termination from the district.

F. Unlawful Appropriation

Failure to return the device in a timely manner, and the continued use of the device for non-school purposes without the District's consent may be considered unlawful appropriation of the District's property.

4. Financial Terms of Mobile Technology Use

A. iPad Costs

If a staff or faculty member breaks or loses an iPad the first time, there will be no charge. If a staff or

faculty member breaks an iPad a second time, he/she will pay the cost of repair/replacement. This applies for the duration of the cycle of iPad adoption. Staff or faculty members may purchase the \$30 insurance for their iPad to protect against becoming damaged a second time through their building's treasurer.

B. Table of Estimated Repair Pricing

With insurance, and upon a 2nd incident of damage:

Repair/Replacement type	Estimated Repair/Replacement Costs
Broken Screen/Digitizer	\$100.00
Broken LCD	\$100.00
Power Adapter + Cord	\$10.00
District-Assigned iPad Case	\$26.00

Without insurance

Repair/Replacement type	Estimated Repair/Replacement Costs
Broken Screen/Digitizer	\$180.00 (subject to change)
Broken LCD	\$180.00 (subject to change)
Power Adapter + Cord	\$10.00
District-Assigned iPad Case	\$26.00

C. Stolen, Lost, Vandalized, or Damaged iPad

1. **ANY THEFT, LOSS, VANDALISM, OR DAMAGE MUST BE REPORTED TO SCHOOL AUTHORITIES WITHIN 24 HOURS OR THE NEXT SCHOOL DAY!**
2. Power cord/adaptor or case must be paid in full.

5. Mobile Technology Precautions

A. Handling and Care of the iPad

- The user must keep the iPad in the district provided protective case or be subject to full repair/fair market value of iPad if damages occur using an alternate case.
- iPads and cases must remain free of any writing, drawing, stickers, or labels that are not applied by EACS.
- Use the iPad on a flat, stable surface.
- Do not set books on the iPad.
- Do not have food or drinks around the iPad.
- Wipe surfaces with a clean, dry microfiber cloth.
- Avoid touching the screen with pens or pencils.
- Do not leave the iPad exposed to direct sunlight or near any heat or moisture sources for extended periods of time, i.e. car or window seat.

B. Power Management

It is the user's responsibility to recharge the iPad's battery so it is fully charged by the start of the next school day.

The iPad must remain on or in Sleep mode at school at all times (no exceptions).

C. Transport

- The iPad should be transported in its protective case.
- Do not leave iPad in a vehicle for extended periods of time or overnight.
- Do not leave iPad in visible sight when left in a vehicle.

D. Monitoring and Supervision

- Do not leave the iPad unattended in an unlocked classroom or during an extra-curricular activity.
- Do not lend your iPad to others. **You are responsible for the safety and security of the iPad and any activity on the device.**

EACS STAFF TECHNOLOGY AGREEMENT 2015-2016

Educator Name: Last _____ First _____
Address: _____
Home Phone: _____ Cell #: _____ Work #: _____
Email Address: _____

I have reviewed the EACS Staff Technology Handbook and understand/agree to the guidelines for:

1. District Technology Goals
2. Responsible Use Agreement
3. Use of District Mobile Technology
4. Financial Terms of Mobile Technology Use
5. Mobile Technology Precautions

Terms of Agreement

I am responsible at all times for the care and appropriate use of this mobile device. I understand if I violate the guidelines agreed to in the **EACS Staff Technology Handbook** my privilege to take the mobile device home may be restricted or removed and I may be subject to disciplinary action.

The mobile device remains the property of East Allen County Schools. Upon end of employment from the district, I agree to return the mobile device to the school in the same condition it was issued to me, less reasonable wear.

Signature

Educator Signature _____
Date