One-to-One

IPAD AND LAPTOP MANUAL 2024-2025

Table of Contents

**Parent will confirm they and their student(s) have read and accept the Acceptable Use (Appendix A) and policies and procedures outlined in this One-to-One iPad and Laptop Program Manual on online registration.

Introduction to One-to-One

In order to advance educational opportunities and provide equitable access to students, Effingham CUSD #40 provides laptops or iPads to students with its one-to-one (1:1) program. One-to-one means each student is issued a district-owned device and district account(s). These devices allow students access to a world of new information and avenues for learning under the guidance of teachers and school personnel. However, this program increases the level of responsibility from students, parents, and school staff.

The policies, procedures, and information within this manual apply to all iPads, laptops, and related accessories (cases, power cords, etc) used or provided by Effingham CUSD #40. Teachers may set additional requirements for use in their individual classrooms. As technology is ever-changing, the policies and procedures covered in this manual are not "all inclusive" and may be modified over time.

Use of Personal Electronic Devices

The district does not allow students to opt-out of receiving a district device or substituting a personal laptop. District iPads and laptops are configured with on-going support, district-approved software, and security to offer the best experience for students. Further, personal devices are not allowed on the Unit #40 network.

District devices have applications subject to licensing agreements, which do not permit installation on personal devices. Student safety is a district priority, and personally-owned devices may not provide the same digital safeguards.

Authorization to Use Device & Network

Students and their parent/guardian will need to complete the following before a student will be issued a device and granted access to our network:

- Read the **One-to-One iPad and Laptop Program Manual**
- Demonstrate understanding of the use and care of the device
- Read the **Acceptable Use of the District's Electronic Networks** (Appendix A)
- Read the **Exhibit- Student Authorization for Access to District's Electronic Networks** (Appendix B)
- On online registration, confirm you have read and agree to the policies and procedures outlined within this manual by clicking "I have read and I agree to…" the **Authorization for Access to District's Electronic Networks** form (Appendix C) and the **Acknowledgement of Responsibility Form** (Appendix D)

We are excited to provide this opportunity to enhance learning at Effingham CUSD #40 and prepare students to function more effectively in a technology-driven society.

Information on Student Assigned Devices

Device Distribution

The Technology Director will maintain a log of all devices. This includes the device serial number, asset tag, and name and ID number of the device assigned to your student.

Pre-K and Kindergarten students will be issued an iPad device
- These devices will be housed inside a cart in the individual teacher's classroom.
- These devices will be kept in the classroom daily.
- These devices may be sent home for special projects, special circumstances, or during remote learning. Parents will be required to sign a check-out form prior to taking the device home.
- Each device will have a rubber case to help protect the device against damage.

Grades 1 to 5 will be issued a laptop device
- These devices will be housed inside a cart in the individual teacher's classroom.
- These devices will be kept in the classroom daily.
- These devices may be sent home for special projects, special circumstances, or during remote learning. Parents will be required to sign a check-out form prior to taking the device home.
- Each device will be issued a case that will be used anytime the device is sent home.

Grades 6 to 12 will be issued a laptop device
- These devices will travel from classroom to classroom with students and will be taken home by the student each night.
- These laptops will be required at school each day and will be a vital part of the curriculum plan. Teachers will be designing many of their lessons based on students' access to their laptops. Students should get into a habit of fully charging their laptops at night in a safe, secure location so they are prepared for school the next day.
- Each device will be issued a case to help protect against damage.
- Routine cleaning is encouraged, and students will be trained and directed to clean their laptops periodically at school. Only a dry, microfiber cloth should be used on the device.
- In most cases and as funding permits, your student will be issued a device in 6th grade that will be reissued to them each year through their 8th grade year. In 9th grade, the student will receive a new laptop that will be reissued to them each year through 12th grade.

Device Collection/Returning the Device
- **End of Year Collection** – At the end of the school year, students will turn in their device, charger, and case. Failure to turn in any or all of these items on collection day will result in the student being charged for any missing or broken items. See "Technology Price List" on pg. 7. The District may also file a report of stolen property with local law enforcement agency.
- **Transfer/Withdrawn/Expelled Students** – Students that transfer out, withdraw, or are expelled from Effingham CUSD #40 must return their device, charger, and case **on or before their last day of attendance** to the school the student is enrolled. Failure to turn in any or all of these items will result in the student being charged for any missing or broken items. See "Technology Price List" on pg. 7. The District may also file a report of stolen property with local law enforcement.

Proper Use & Care of the Device

Student Responsibilities
Students are responsible for the general care of the device while in use by the student. Devices that are broken or that fail to work properly must be taken to the classroom teacher, technology integrationist, or technician for an evaluation of the equipment. Please see the "Technology Support" section on p. 6-7 for more information regarding repairs/replacements/lost/stolen devices.

Acceptable Use
District device and network use must support educational inquiry and the district's mission. Expectations for student behavior online are no different from face-to-face interactions. All users are expected to abide by the policies in this manual, and those contained in Effingham CUSD #40 Acceptable Use Policy (AUP) (Appendix A). Students must use district devices per Board Policy 6:235- AP1 (Appendix A). Students are responsible for the general care of their district device.

Prohibited Use
Students are prohibited from engaging in any activity considered contrary to the mission of Effingham CUSD #40 and must abide by Board Policy 6:235- AP1 (Appendix A). Effingham CUSD #40 reserves the right to inspect all devices at any point.

No Expectation of Privacy
Students have no expectation of confidentiality or privacy with respect to any usage of an Effingham CUSD #40 device or district account, regardless of whether that use is for district-related or personal purposes, other than specifically provided by law. Without prior notice or consent, the District may supervise, access, view, monitor, and record use of student devices and accounts at any time for any reason related to the operation of the District. By using an Effingham CUSD #40 device, students agree to such access, monitoring, and recording of their use.

General Precautions
- No food or drink should be used or placed next to devices; always keep the device dry.
- Insert cords and cables carefully into the device.
- Devices should always be transported with care.
- Devices must remain free of any writing, drawing, stickers, and labels.
- Use only a clean, lint-free cloth to clean the device. DO NOT spray liquid directly onto the screen. Avoid getting moisture in any openings.
- Devices should only be charged using the charger provided by the Technology Department. Other chargers will damage the device and students will be charged full replacement cost.
- Use strong passwords.
- Screen Care- The screens are particularly sensitive to damage from rough treatment or excessive pressure on the screen. Laptops should never be lifted by the screen or carried with the screen open. Do not lean or put items on the top of the laptop when it is closed. Do not store a laptop with the screen open. Make sure there is nothing on the keyboard before closing the lid (e.g. pens, pencils, etc)
- Keyboard Care- Keyboards can be damaged if subjected to rough treatment. Do not remove keys for any reason. This will cause the entire keyboard to be replaced.
- Asset Tags

- - All devices will be labeled with District asset tags. Asset tags may not be modified, removed, or tampered with in anyway. Students may be charged up to the full replacement cost of a device for tampering with District asset tags.
- Backgrounds and Themes
    - Backgrounds and themes should not be placed on Effingham CUSD #40 devices. The presence of such media may result in disciplinary action.
- Sound
    - Sound must be muted at all times unless permission is obtained from an individual teacher of that class period.
    - Headphones may be used at the discretion of the teacher. Students must provide their own personal set of headphones for sanitary reasons.
- Software, Games, Apps, Extensions, and Music
    - Music, Games, etc. may not be downloaded to or played on the device. These devices are for educational use only.
    - **Students are not allowed to install any software programs, apps, or extensions on the device.** Students are encouraged to bring any software recommendation to the Technology Department if they feel that a specific software could be of educational value.
- Network Connectivity
    - Effingham CUSD #40 makes no guarantees that the school network will be up and running 100% of the time. In the rare case that the network is down, the school is not responsible for any lost or missing data.
    - Effingham CUSD #40 is not responsible for connectivity issues experienced at a student's home when connecting to a private internet vendor.

Classroom Use

Students will adhere to the following guidelines while at school:
- Devices are intended for school use each day in classrooms and should be charged before arrival.
- Students should use their device as directed by their teacher.
- Students must be prepared with their logins and passwords when they come to class each day.
- Students are not permitted to utilize the devices for personal use, including gaming, listening to music, or watching movies.
- Device should be kept in the provided protective case.
- Do not leave your device or accessories unattended when not stored in a secure, safe location.

When Not at School

Students will follow the following guidelines when not at school:
- Students are not permitted to utilize the devices for personal use, including gaming, listening to music, or watching movies.
- Devices should not be used or stored near pets and other possible hazardous conditions.
- Keep the device at a reasonable temperature. Do not leave the equipment outdoors or inside a car in extreme temperatures.
- When the device is in use or charging, ensure that proper airflow around the device is possible. Do not leave the device on soft surfaces like pillows and blankets.
- Do not leave your device unattended when not stored in a secure, safe location.

Digital Rights and Media Literacy

Digital rights include the norms of respectful, responsible, safe, and healthy behavior related to current technology use, including digital and media literacy, ethics, etiquette, and security. Digital rights include the ability to access, analyze, evaluate, develop, produce, and interpret media, as well as Internet safety, cybersecurity, and cyberbullying prevention and response. Instruction on digital citizenship and cybersecurity will be incorporated into the District's curriculum.

Electronic Resources and Internet Safety

Students are responsible for the proper use of electronic resources provided by the district. Information about student responsibilities on the district network, internet safety, copyright, and data privacy can be found in Appendix A or by going to https://consumer.ftc.gov/identity-theft-and-online-security/protecting-kids-online.

Parent/Guardian Responsibilities

The district encourages families to engage and participate in their student's learning at home by monitoring the student's use of district hardware and applications.

Suggestions:
- Help manage your student's password.
- Have your student use his/her device in a shared space at home.
- Promote safe, appropriate use for educational purposes only.
- Ask your student about what they are learning and assist with assignments.
- Please remind your student to charge his/her device overnight in a safe, secure location.

Technology Support

The Technology Department provides system maintenance, security upgrades, hardware repairs, and software or application support.

Software Application and Maintenance

The district reviews all requests for software and application use for staff and students. The review process includes the protection of student and staff data privacy, vendor security, and curricular alignment. The district performs routine maintenance on student devices throughout the year. The district manages all system, software, and application updates which run automatically. Therefore, students do not need to initiate any updates to their software. It is important that students shut down and restart their device on the District's network several times per week to ensure they are receiving updates. Student should never download software, apps, extensions, games, etc.

Filtering

The district utilizes an internet content filter that is in compliance with the federally mandated Children's Internet Protection Act (CIPA). All devices, regardless of physical location (in or out of school), will have internet activity protected and monitored by the district. If a website is blocked at school, then it will be blocked out of school. If an educationally valuable site is blocked, students should contact the Technology Department to request the site be checked and unblocked. **ALL activity on district-owned devices and district accounts is monitored and subject to inspection.**

Security

The District uses a variety of best security practices to protect students, including our content filter, firewall, anti-virus and malware platform, Google Suites security, and Windows security. We are compliant with the Student Online Personal Protection Act. Encourage your student to use strong passwords, not share logins, and to not download anything onto the device unless directed by staff.

Request Help

In grades PreK-5th, teachers will contact the appropriate technology staff to fix any student device issues. In grades 6th-12th, students must complete a Tech Help Ticket- Service Request located on the district's website and a student's laptop start-up page to receive technology support on their assigned device. We have technology integrationists and technicians that can help assist with device issues. If the technician needs to keep the device for repair, the school will exchange the broken laptop for a temporary loaner laptop until the assigned computer is repaired and returned. In some cases, the student may be issued a new device.

Device Damage/Loss/Theft

When a laptop is lost, stolen, or vandalized, students or guardians must report the incident immediately to the school administrator. The issue will be investigated to determine if a replacement device will be charged to the student's account.

Practicing responsible care routines with your student is the best way to prevent breakage or loss. Intentional or accidental damage is not covered under device warranty. In the event of a device being damaged or lost, we expect you to pay for the replacement just as we do for damaged or lost textbooks or library books. The technician will investigate the damage and may assess a fine to repair or replace the device. A charge may be applied and billed during the summer months as technicians discover damage during summer updates. *The pricing table below is based on the District's cost to repair or replace the device as of 2024 market pricing and is subject to change each year.*

Technology Price List

The list includes the most commonly needed replacement parts and does not encompass every issue that may be billed.

2024-2025 Technology Price List

Item	Cost
Charger	$25
Carrying Case	$25
Top or Bottom Cover	$35
Screen	$25
Cable Kit	$50
Keyboard	$60
Digitizer	$100
Full Replacement	$375

Payment of Fees

In the event a student is billed to repair or replace a device or any of its parts (including charger and case), the fee will be available in the Infinite Campus Parent Portal. Your student can also pay the fee by check or money in the office of his/her building. Unpaid bills may be reported to collections.

APPENDIX A

EFFINGHAM COMMUNITY UNIT SCHOOL DISTRICT #40
Effingham, Illinois

ACCEPTABLE USE OF THE DISTRICT'S ELECTRONIC NETWORKS

All use of the District's *electronic networks* shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. These procedures do not attempt to state all required or prohibited behavior by users. However, some specific examples are provided. **The failure of any user to follow these procedures will result in the loss of privileges, disciplinary action, and/or legal action.**

Terms and Conditions
The term *electronic networks* includes all of the District's technology resources, including, but not limited to:
1. The District's local-area and wide-area networks, including wireless networks (Wi-Fi), District-provided Wi-Fi hotspots, and any District servers or other networking infrastructure;
2. Access to the Internet or other online resources via the District's networking infrastructure or to any District-issued online account from any computer or device, regardless of location;
3. District-owned and District-issued computers, laptops, tablets, phones, or similar devices.

Acceptable Use - Access to the District's electronic networks must be: (a) for the purpose of education or research, and be consistent with the District's educational objectives, or (b) for legitimate business use.

Privileges - Use of the District's electronic networks is a privilege, not a right, and inappropriate use may result in a cancellation of those privileges, disciplinary action, and/or appropriate legal action. The system administrator or Building Principal will make all decisions regarding whether or not a user has violated these procedures and may deny, revoke, or suspend access at any time. His or her decision is final.

Unacceptable Use - The user is responsible for his or her actions and activities involving the electronic networks. Some examples of unacceptable uses are:

    a. Using the electronic networks for any illegal activity, including violation of copyright or other intellectual property rights or contracts, or transmitting any material in violation of any State or federal law;

    b. Using the electronic networks to engage in conduct prohibited by board policy;

    c. Unauthorized downloading of software or other files, regardless of whether it is copyrighted or scanned for malware;

    d. Unauthorized use of personal removable media devices (such as flash or thumb drives);

    e. Downloading of copyrighted material for other than personal use;

    f. Using the electronic networks for private financial or commercial gain;

    g. Wastefully using resources, such as file space;

    h. Hacking or attempting to hack or gain unauthorized access to files, accounts, resources, or entities by any means;

    i. Invading the privacy of individuals, including the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature, such as a photograph or video;

    j. Using another user's account or password;

    k. Disclosing any network or account password (including your own) to any other person, unless requested by the system administrator;

l.   Posting or sending material authored or created by another without his/her consent;

m.   Posting or sending anonymous messages;

n.   Creating or forwarding chain letters, spam, or other unsolicited messages;

o.   Using the electronic networks for commercial or private advertising;

p.   Accessing, sending, posting, publishing, or displaying any abusive, obscene, profane, sexual, threatening, harassing, illegal, or knowingly false material;

q.   Misrepresenting the user's identity or the identity of others; and

r.   Using the electronic networks while access privileges are suspended or revoked.

Network Etiquette - The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

a.   Be polite. Do not become abusive in messages to others.

b.   Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.

c.   Do not reveal personal information, including the addresses or telephone numbers, of students or colleagues.

d.   Recognize that the District's electronic networks are not private. People who operate District technology have access to all email and other data. Messages or other evidence relating to or in support of illegal activities may be reported to the authorities.

e.   Do not use the networks in any way that would disrupt its use by other users.

f.   Consider all communications and information accessible via the electronic networks to be private property.

No Warranties - The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Indemnification - By using the District's electronic networks, the user agrees to indemnify the District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any violation of these procedures.

Security - Network security is a high priority. If the user can identify or suspects a security problem on the network, the user must promptly notify the system administrator or Building Principal. Do not demonstrate the problem to other users. Keep user account(s) and password(s) confidential. Do not use another individual's account without written permission from that individual. Attempts to log-on to the network as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the networks.

Vandalism - Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of malware, such as viruses and spyware.

Telephone Charges - The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, texting or data use charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.

Copyright Web Publishing Rules - Copyright law and District policy prohibit the re-publishing of text or graphics found on the Internet or on District websites or file servers/cloud storage without explicit written permission.

a.   For each re-publication (on a website or file server) of a graphic or a text file that was produced externally,

there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the web address of the original source.

b.   Students and staff engaged in producing web pages must provide library media specialists with email or hard copy permissions before the web pages are published. Printed evidence of the status of *public domain* documents must be provided.

c.   The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the website displaying the material may not be considered a source of permission.

d.   The *fair use* rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.

e.   Student work may only be published if there is written permission from both the parent/guardian and student.

Use of Email - The District's email system, and its constituent software, hardware, and data files, are owned and controlled by the District. The District provides email to aid students and staff members in fulfilling their duties and responsibilities, and as an education tool.

a.   The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student   or staff member to an email account is strictly prohibited.

b.   Each person should use the same degree of care in drafting an email message as would be put   into a written memorandum or document. Nothing should be transmitted in an email message that would be inappropriate in a letter or memorandum.

c.   Electronic messages transmitted via the District's Internet gateway carry with them an identification of the user's Internet *domain*. This domain is a registered name and identifies the author as being with the District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of the District. Users will be held personally responsible for the content of any and all email messages transmitted to external recipients.

d.   Any message received from an unknown sender via the Internet, such as spam or potential phishing emails, should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.

e.   Use of the District's email system constitutes consent to these regulations.

Internet Safety

Internet access is limited to only those *acceptable uses* as detailed in these procedures. Internet safety is supported if users will not engage in *unacceptable uses*, as detailed in these procedures, and otherwise follow these procedures.

Staff members shall supervise students while students are using District Internet access to ensure that the students abide by the *Terms and Conditions* for Internet access contained in these procedures.

Each District computer with Internet access has a filtering device that blocks entry to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee.
The system administrator and Building Principals shall monitor student Internet access.

LEGAL REF.:   20 U.S.C. §7131, Elementary and Secondary Education Act. 47 U.S.C. §254(h) and (l), Children's Internet Protection Act. 720 ILCS 135/, Harassing and Obscene Communications Act.

Revised: July 16, 2001, May 18, 2009, September 26, 2016, July 26, 2021

APPENDIX B

EFFINGHAM COMMUNITY UNIT SCHOOL DISTRICT #40
Effingham, Illinois

Exhibit - Student Authorization for Access to the District's Electronic Networks

This form accompanies Administrative Procedure 6:235-AP1, Acceptable Use of the District's Electronic Networks.

Dear Parents/Guardians:

Our School District has the ability to enhance your child's education through the use of its electronic networks, including the Internet. Our goal in providing this service is to promote educational excellence by facilitating resource sharing, innovation, and communication.

The District *filters* access to materials that may be defamatory, inaccurate, offensive, or otherwise inappropriate in the school setting. If a filter has been disabled or malfunctions it is impossible to control all material and a user may discover inappropriate material. Ultimately, parents/guardians are responsible for setting and conveying the standards that their child should follow, and the School District respects each family's right to decide whether or not to authorize Internet access.

With this educational opportunity also comes responsibility. The use of inappropriate material or language, or violation of copyright laws, may result in the loss of the privilege to use this resource. Remember that you are legally responsible for your child's actions. If you agree to allow your child to have a network account, electronically confirm the *Authorization* form below on online registration.

APPENDIX C

Authorization for Access to the District's Electronic Networks Form

Students must have a parent/guardian read and agree to the following before being granted unsupervised access:

All use of the electronic networks shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. **The failure of any user to follow the terms of the** *Acceptable Use of the District's Electronic Networks* **will result in the loss of privileges, disciplinary action, and/or appropriate legal action.** The electronic confirmation on online registration is legally binding and indicate the parties have read the terms and conditions carefully and understand their significance.

> I have read this *Authorization* form. I understand that access is designed for educational purposes and that the District has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the District to restrict access to all controversial and inappropriate materials. I will hold harmless the District, its employees, agents, or Board members, for any harm caused by materials or software obtained via the network. I accept full responsibility for supervision if and when my child's use is not in a school setting. I have discussed the *Acceptable Use of the District's Electronic Networks* with my child. I hereby request that my child be allowed access to the District's electronic networks, including the Internet.

Students must also read and agree to the following before being granted unsupervised access:

> I understand and will abide by the *Acceptable Use of the District's Electronic Networks*. I understand that the District and/or its agents may access and monitor my use of the District's electronic networks, including the Internet, my email, and downloaded material, without prior notice to me. I further understand that should I commit any violation, my access privileges may be revoked, and school disciplinary action and/or legal action may be taken. In consideration for using the District's electronic network connection and having access to public networks, I hereby release the School District and its Board members, employees, and agents from any claims and damages arising from my use of, or inability to use the District's electronic networks, including the Internet.

Revised (formerly 6:235-E2): September 26, 2016, December 18, 2017, July 26, 2021

APPENDIX D

Acknowledgement of Responsibility Form

Student Responsibility:
As a student of Effingham CUSD #40, I have read and agree to the terms set forth in Effingham CUSD #40's Acceptable Use of Technology (AUP) and the One-to-One iPad and Laptop Program Manual. I also understand that a violation of the rules that govern the use of Effingham CUSD #40 network may result in the revoking of my access privileges and that use deemed offensive or illegal will be dealt with by school disciplinary action.

Parent or Guardian Responsibility:
As the parent or guardian of this student, I have read the terms and conditions for Internet use, as well as the One-to-One iPad and Laptop Program Manual. I understand that this access is designed for educational purposes and the school has taken available precautions to eliminate controversial materials. However, I also recognize that it is impossible to restrict access to all controversial material and I will not hold the school responsible for materials acquired on the Internet.

I hereby give permission for my child to use the Internet and iPads or laptops.