One to One

Device Handbook

Table of Contents

Overview

Cornwall-Lebanon School District is committed to the strategic approach of enhancing our students' learning process through a One-to-One (1-to-1) program, which means one student with one device. The One-to-One program is defined as a flexible and personalized educational program that integrates new instructional strategies using a mixture of technology with the goal of transforming classrooms from teacher-centric to student-centered personalized learning environments. The program will focus on high academics and the integration of future learning skills to improve the students' learning process.

After extensive research, planning, and preparation, the District will lend each student a device which will assist the student with course work throughout the year. The device is a tool which will complement the lessons and assist with knowledge creation in the classroom. Key components of the 1-to-1 program include the expertise of the classroom teacher, use of a learning management system, Office 365, and Microsoft OneDrive for Business. Teachers will blend the classroom experience to offer traditional and digital learning resources while mentoring students to become independent learners. The learning management system enables teachers to organize curriculum content, provide formative assessments, and create a more personalized learning path for students. The 1-to-1 devices provide the anytime-anywhere access to learning that is needed for our students to become proficient, life-long learners. Student-centered instructional strategies being introduced include project-based learning, active inquiry, computer-based formative assessments, and blended learning. The district continues to provide our educators with ongoing professional development for best practices in using technology and new instructional strategies.

1-to-1 Student Questions and Answers

Q: What are the goals of the 1-to-1 program?

- To promote an environment where students have access to anytime-anywhere learning.
- To equip teachers with technology necessary to differentiate instruction for personalized learning.
- To prepare students with essential digital literacy skills needed to compete in a global workforce.
- To provide for deeper learning opportunities that reach beyond a traditional classroom setting.
- To encourage & motivate students to think critically and apply future learning skills needed for real-world innovation.
- To cultivate self-directed life-long learning, responsibility, & collaboration using digital communication and productivity technology.

Q: What is the 1-to-1 program?

A: It is a District program to provide students with a District-owned device as a tool to help integrate new instructional strategies in order to integrate future learning skills in the classroom.

Q: How will the 1-to-1 program help me academically?

A: Educational research shows that when students effectively use technology devices in the classroom, students are provided with deeper learning experiences and are more effectively able to apply future learning skills. To compete in our global economy and equip our students for post-secondary education, the District needs to provide a learning environment that integrates today's digital tools, accommodates mobile lifestyles, and encourages students to work collaboratively in team environments. Through providing this learning environment, we will meet these globally competitive demands which will allow students to manage their own learning at any time and any location. This program is designed to enhance current teaching/instructional strategies through the effective use of technology and future teaching methods.

Q: When will I receive the District-issued device?

A: Students will receive a District-issued device before or during the beginning of the school year and after the District receives all the appropriately signed policies. Depending on your grade level, policies and forms will be issued at the beginning of the school year and must be returned before a device will be distributed.

Q: Who owns the District-issued device?

A: The Cornwall-Lebanon School District owns the District-issued device. Therefore, it's very important that you take good care of it, leave the id tags in place, don't damage it or write on it, as it doesn't actually belong to you.

Q: May I take the District-issued device home?

A: Secondary students (grades 6-12) may take the device home once the Student Agreement and Insurance forms have been signed. Devices at the Elementary level (grades K-5) will be stored in the

classroom and, unless otherwise directed by your teacher or administration, should stay in the classroom.

Q: May I access the Internet at home with the District-issued device?

A: You may use the device at home and access your home internet in support of academics. There is a content filter installed, however; parents should not rely on the filter as a catch all for inappropriate content. There is no such thing as a perfect filter. Under no circumstances should anyone try to tamper with the installed filter. Any attempts to remove or manipulate the filter will be considered a violation of the **Internet Acceptable Use Policy (#815)**.

Q: What do I do if my District device doesn't work or is damaged?

A: Please report any incidents to Technology Services as soon as possible. It's important not to delay as one problem can lead to another if not solved right away. If your computer is damaged, we will fix it or send it out for repair. If it needs to be repaired, we will loan you a device to use until it's returned. Under no circumstances should you or anyone else take the device to a third party to attempt repairs. District-issued devices are the property of the Cornwall-Lebanon School District and District personnel shall fix related problems.

Q: May I put games or software on a District-issued device?

A: The device is meant for academic use. You may install software and/or apps to assist in your educational experience. The District is not responsible for making the software work on the device. All installed software must be licensed and legal. Any hacking or sniffing software installed on the device will result in immediate loss of privilege with no insurance refund. All software fees and subscriptions are the responsibility of the student and/or guardian. The loss of software due to maintenance of the device by the District is not the District's responsibility.

Q: Can I print from the District-issued device?

A: The device will not print to any District printers. All assignments should be delivered through our learning management system, emailed, or shared using Office 365. Home printers may be installed on the device, but the District is not responsible for compatibility or troubleshooting.

Q: Where do I keep my District-issued device while at school?

A: At school, you will use your device for nearly all your classes. For any classes not requiring your device, or during lunch, you must store your device in your locker or a provided charging station. You are responsible for the device and should never leave it unattended or unsecured.

Q: Is there anything special I should do with my District-issued device at home?

A: Be sure you plug it in overnight so you come to school with a fully charged battery. Also, be sure to bring your device and power cord with you every day to school. You will be responsible if your device is not ready for classwork every day. It will be viewed as if you have left your textbook at home if your device is not charged and ready to go every class period.

Q: How long will I have the District-issued device?

A: The device is yours to use during the school year. High School students will hold onto their computer over the Summers through their senior year. For middle school and elementary students, prior to the beginning of summer or a student withdraw, Technology Services will collect the device. Once school starts again the following year, you will receive a District-issued device after all of the proper forms have been signed.

Q: Should I back up my documents?

A: Yes. All of the data on the device is the responsibility of the student. If the device becomes damaged and requires repair, technology services may need to erase all data on the device. Students are highly encouraged to save all their data in Microsoft's OneDrive for Business or another cloud-based storage. This will allow students to access their data from any device and not lose any documents.

1-to-1 Program Device Responsible Use Policy

As the Cornwall-Lebanon School District embarks on the journey to enrich learning experiences, students are encouraged to use District resources such as computers, software, email, and the internet for educational or school-related activities and for the exchange of useful information. The device is the property of the District and is to be used solely by the student it is being issued to for academic reasons.

Appropriate or acceptable educational uses of the device include:

- ✓ The use of software, hardware, email, and the intranet/internet for academic purposes.
- ✓ Accessing the Internet to retrieve information from libraries, databases, and websites to enrich and expand learning opportunities.
- ✓ Email and online work to facilitate communication and for school projects and/or assignments.

All users are expected to conduct their online activities in an ethical and legal fashion. ***The use of these resources is a privilege, not a right.*** Misuse of these resources will result in the suspension or loss of these privileges, as well as possible disciplinary, legal, or other action necessary.

Examples of inappropriate or unacceptable use(s) of these resources include, but are not limited to:

- × Uses that violate the law or the **Internet Acceptable Use Policy** (School Board Policy #815), the rules of network etiquette, and that would disrupt the educational environment or hamper the integrity or security of the district network.
- × The use of Instant Messaging or screen-sharing programs with other students during school hours without permission from a teacher.

- Transmission of any material in violation of any U.S. or state law, including but not limited to: copyrighted material without the written permission of the author or creator; threatening, harassing, pornographic, or obscene material; or material protected by trade secret.
- As with all forms of communications, email or other network resources may not be used in a manner that is disruptive to the work or educational environment. The display or transmission of messages, images, cartoons or the transmission or use of email or other computer messages that are sexually explicit constitute harassment, which is prohibited by the Cornwall-Lebanon School District.
- The use for personal financial, political, or commercial gain, product advertisement, or the sending of unsolicited junk mail or chain letters is prohibited.
- The forgery, reading, deleting, copying, or modifying of electronic mail messages of other users is prohibited.
- The creation, propagation, and/or use of computer viruses or other malicious logic is prohibited.
- Deleting, examining, copying, or modifying files and/or data belonging to other users are prohibited.
- Unauthorized copying/installation of software programs belonging to the District are prohibited.
- Intentional destruction, deletion, or disablement of installed software on any device is prohibited.
- Vandalism is prohibited. This includes, but is not limited to, any attempt to harm or destroy the data of another user, the network/Internet, or any networks or sites connected to the network /Internet. Attempts to breach security codes and/or passwords are considered a form of vandalism.
- Destruction of hardware or software or attempts to exceed or modify the parameters of the system is prohibited.
- Intentional overloading of school computer resources.

Access to school email and similar electronic communication systems is a privilege, and certain responsibilities accompany that privilege. District users are expected to demonstrate the same level of ethical and professional manner as is required in face-to-face or written communications. All users are required to maintain and safeguard password protected access to both personal and confidential District files and folders.

Unauthorized attempts to access another person's email or similar electronic communications or to use another's name, email, or computer address or workstation to send email or similar electronic communications are prohibited and will subject the individual to disciplinary action. Anonymous or forged messages will be treated as violations of this policy. Nothing in this policy shall prohibit the District from intercepting and stopping email messages that have the capacity to overload the computer resources. All users must understand that the District cannot guarantee the privacy or confidentiality of electronic documents and any messages that are confidential as a matter of law should not be communicated over email.

The District reserves the right to access email to retrieve information and records, to engage in routine computer maintenance and housekeeping, to carry out internal investigations, to check Internet access history, or to disclose messages, data, or files to law enforcement authorities. Any information contained on any computer, cloud, or internet transmitted through or purchased by the Cornwall-Lebanon School District is considered the property of the District. Files stored or

transmitted on District equipment, cloud services, or the network are property of the District and are subject to review and monitoring. The District reserves the right to confiscate the property at any time.

This agreement applies to stand-alone devices as well as devices connected to the network or Internet. Any attempt to violate the provisions of this agreement will result in revocation of the user's privileges, regardless of the success or failure of the attempt. In addition, school disciplinary action, and/or appropriate legal action may be taken. The decision of the District regarding inappropriate use of the technology or telecommunication resources is final. Monetary remuneration may be sought for damage necessitating repair, loss, or replacement of equipment and/or services.

Liability

The device issued to the student is the only authorized user of that device. Although each student accepts responsibility for the care and use of the device, the device remains the sole property of the District. The District owns licenses for the software installed on the device. Under no circumstances may any of this software be transferred to any other device.

Daily Use

Middle school and high school students are expected to arrive at school every day with their device battery fully charged and with the device power adapter. Students that fail to bring these items in or have their battery fully charged will be subject to appropriate disciplinary action. Elementary students that are issued a device are expected to return their device to the cart in the classroom and plug it in to be charged at the end of the day.

Network Access

Use of the District network is governed by the District's **Internet Acceptable Use Policy** (#815). An up-to-date copy of this policy can be found on the district website.

Digital Communication

Students will utilize email, chat messaging, and/or their account within the learning management system (LMS) to communicate with teachers and administrators. Students are expected to follow the guidelines listed in the student handbook.

Care

Devices should not be left in temperatures below 35 degrees or above 90 degrees. Food, drinks, or pets should not be near the device or charger to avoid damage. Rain, wet hands, and high humidity are risky to devices and should be avoided. Devices are not to be left in a vehicle; this encourages theft and exposes the device to temperature changes outside of their operating limits. This is considered negligence.

Students may not personalize the device or peripherals in any way. This constitutes vandalism and will be subject to appropriate disciplinary action and where appropriate, monetary restitution.

Security

For middle school and high school students, the device should be with the student, locked in his or her locker, or in a charging station in the school building at all times. Students should always guard their device closely. It must not be left on car seats, on benches, or anywhere that might be tempting to others. The student is responsible for any loss or theft of the device.

For elementary students, unless directed otherwise by their teacher or administrators, the device should be kept in the classroom or in the classroom cart.

Loaner Devices

Should a District-issued device become inoperable, a student will be issued a loaner device while their device is being repaired. The loaner device assumes all aspects and policies of the student originally issued device.

Backing Up

Students are responsible for backing up personal files on District-issued devices. Files that are saved to the desktop or documents folder are not backed up. The District highly encourages students to store their files on Microsoft's OneDrive for Business or other free cloud-based storage solution. This will allow the students to access their files anytime, anywhere, and from any device.

The District is not responsible for students who lose files or data. If a device fails or has a virus, it will be wiped clean and imaged. Technology Services will not take any measures to save or recover data stored on the device.

Troubleshooting

Students should report any device problems (i.e. software issues, syncing, etc.) to the classroom teacher or to Technology Services as soon as possible. Students are prohibited from trying to troubleshoot any hardware problem. Under no circumstances shall the District-issued device be taken to a third party for repair or troubleshooting. All issues relating to the functionality of the device shall be reported to Technology Services.

Failure to abide by this policy, regardless of the resolution, will be considered vandalism and/or negligence.

Damage / Theft

All physical damage to the device must be reported immediately to Technology Services. It must be reported to Technology Services no later than the next school day. Technology Services will arrange for repair and a loaner, as needed. The parent/student is responsible for all damages to District-issued devices and subject to the cost of repair or replacement according to the District device insurance policy. The student is responsible for any loss or theft of the device. Please take precautions to secure the device.

Guidelines for Cyber Safety

The District needs to provide a learning environment that integrates today's digital tools, accommodates mobile lifestyles, and encourages students to work collaboratively in team environments. Through providing this learning environment, we will meet these demands which will allow students to manage their own learning at any time and any location. However, the Internet is not the place for an all-access pass. Students of all ages need supervision. Below are a few tips that can help keep your child safe online.

- You should spend time with your child on-line by having them show you his/her favorite online destinations. At the same time, explain online dangers. Make sure your child keeps passwords secret from everyone (except you). Even best friends have been known to turn against one another and seize control of each other's online accounts.
- Instruct your child that the computer is to be used in a common open room in the house, not in their bedroom. It is much more difficult for children to fall prey to predators when the computer screen is actively being watched by others.
- If you can, utilize additional content filters at the modem/router level. Remember that even though the District has a filter on the device, it will not be able to block all objectionable material. Content filters are not 100% fail safe. Do not rely on the content filter to protect your child.
- Always maintain access to your child's social networking and other on-line accounts and randomly check his/her email. Be up front with your child about your access and reasons why. Tell him/her that protecting them is your job as a guardian.
- Teach your child the responsible use of the resources online. Instruct your child:
    - To never arrange a face-to-face meeting with someone they met online;
    - To never upload (post) pictures of themselves onto the Internet or online service to people they do not personally know;
    - To never give out identifying information such as their name, home address, school name, or telephone number. Teach your child to be generic and anonymous on the Internet. If a site encourages kids to submit their names to personalize the web content, help your child create online nicknames that do not give away personal information;
    - To never download pictures from an unknown source, as there is a good chance there could be sexually explicit images;
    - To never respond to messages or bulletin board postings that are suggestive, obscene, belligerent, or harassing;
    - That whatever they are told online may or may not be true.
- Set clear expectations for your child. Does your child have a list of websites that he/she needs to adhere to when doing research? Is your child allowed to use a search engine to find appropriate sites? What sites is your child allowed to visit just for fun? Write down the rules and make sure that he/she knows them.
- Stay involved with your child's school by remaining in close contact with your child's teachers and counselors. If trouble is brewing among students online, it may affect school. Knowing what's going on at school will increase the chances that you'll hear about what's happening online.

- Tell your child that people who introduce themselves on the Internet are often not who they say they are. Show your child how easy it is to assume another identity online. Don't assume your child knows everything about the Internet.
- Video-sharing sites are incredibly popular with children. With a free account, users can also create and post their own videos and give and receive feedback. With access to millions of videos comes the risk that your child will stumble upon something disturbing or inappropriate. YouTube has a policy against sexually explicit content and hate speech, but it relies on users to flag content as objectionable. Sit down with your child when they log onto video-sharing sites so you can guide their choices. Tell them that if you're not with them and they see something upsetting, they should get you.
- Remind your child to stop and consider the consequences before sending or posting anything online. They should ask themselves, "Would I want my parents, my principal, my teacher, and my grandparents to see this?" If the answer is no, then they shouldn't send it.
- Learn to use privacy settings. Social networking sites, instant messaging programs, even some online games offer ways to control who your child can chat with online or what they can say to each other. Visit the sites where your child goes and look for the sections marked "parents," "privacy," or "safety."

Cyberbullying

The Cornwall-Lebanon School District is committed to providing all students with a safe, healthy, and civil school environment in which all members of the school community are treated with mutual respect, tolerance, and dignity. The District recognizes that bullying creates an atmosphere of fear and intimidation, detracts from the safe environment necessary for student learning, and may lead to more serious violence. Therefore, the School Board will not tolerate bullying by District students. For more information, please see **School Board Policy #249 - Bullying/Cyberbullying**.

1. What Is a Cyberbully?

A cyberbully is someone who uses technology to act cruelly toward another person. Online attacks often hurt more than face-to-face bullying because children can be anonymous over the Internet and behave in ways they never would in person. Online attacks can take on a life of their own: A false rumor or a cruel prank can spread quickly among classmates and live on forever in personal computers and cell phones. A fresh new attack threatens wherever there's an Internet connection, including the one place where they should feel safe: home.

2. A cyberbully might:
    - Use a phone to make repeated prank calls or send unwanted text messages to the victim.
    - Post cruel comments to the victim's social network site, send unkind emails or IMs to the victim.
    - Create a fake social networking profile to embarrass the victim.
    - Use a victim's password to break into his/her account, change settings, lock the victim out, or impersonate the victim.
    - Forward the victim's private messages or photos to others. The bully may trick the victim into revealing personal information for this purpose.

- Forward or post embarrassing or unflattering photos or videos of the victim.
- Spread rumors through IM, text messages, social network sites, or other public forums.
- Gang up on or humiliate the victim in online virtual worlds or online games.

3. Here are five suggestions to protect your child:
    1) Remind your child never to share his/her passwords, even with good friends.
    2) If your child has a bad experience online, he/she should tell you right away. If possible, save the evidence in case you need to take further action.
    3) Don't respond to the bully. If the bully sees that your child is upset, he/she is likely to torment even more. Ignore the harassment if possible, if not; block the bully from contacting your child by using privacy settings and preferences.
    4) Remind your child to treat others as he/she wants to be treated. This means not striking back when someone is mean and to support friends and others who are being cyber-bullied.
    5) Finally, limit the amount of social time your child is online. Studies show that children are more likely to get into trouble on the Internet—including bullying others or being bullied—the more time they spend online. If you need to, limit the computer time to strictly academics.

4. Is your child a victim?

Most children won't tell their parents that they're being bullied because they're afraid their parents will take away the Internet or insist on complaining to the bully's parents. Sometimes children who are bullied are ashamed and blame themselves. Reassure your child that nobody deserves to be mistreated. Tell them that some people try to hurt others to make themselves feel better or because they've been bullied themselves. Let your child know that it's important for you to know what's going on so you can help.

5. Signs that your child is being bullied can be hard to spot but may include:
    - Seeming nervous or unusually quiet, especially after being online.
    - Wanting to spend more or less time than usual on online activities.
    - Not wanting to go outdoors or to school.
    - Problems sleeping or eating.
    - Headaches or stomachaches.
    - Trouble focusing on schoolwork.

6. If you suspect your child is being cyber-bullied, talk to him/her. Tell your child that by talking it over, you can work out a plan to deal with bullying. You might:
    - Contact the bully's parents. Be careful if you decide to do this because it can backfire and make the bullying worse. It's best if you already know the other child's parents and get along with them.
    - Contact your school officials. Make them aware of the problem and ask them to be on the lookout for signs that your child is being bullied at school. The school counselor or principal may have some strategies or even programs in place for handling bullying in school.

- Look into filing a complaint against the bully if the behavior persists. Most internet service providers, websites, and cell phone companies have policies against harassment. You may be able to have the bully's account revoked.
- Contact the police if you fear for your child's safety. Cyber-bullying can cross into criminal behavior if it includes threats of violence, extortion, child pornography, obscenity, stalking, extreme harassment, or hate crimes.

7. If you learn that your child is being cruel to someone online, find out why. Often, cyber-bullies are victims themselves. If this is the case with your child, go over the suggestions to help protect them against being bullied. But remind them that bullying someone online or off is never ok.
8. If your child notices someone else being picked on, encourage him/her to support the victim. Many social websites, such as YouTube and Facebook, allow users to report abuse. Bullies often back down when others make it clear they won't tolerate rude or nasty behavior.
9. Cyber-bullying may be the most common online danger, but as a parent, talking openly about the issue is the best way to give your child the tools to protect him/herself from virtual sticks and stones.

Device Use and Classroom Routines

Lockers

- Your device should be stored at all times in your locker or a charging station, if it is not with you.
- Never pile things on top of your device.
- Never leave your device on the bottom of the locker.

Hallways

- Hold your device by the handle or have it in your case.
- Never leave the device unattended for any reason.
- Close the lid of your laptop before you change classes to put the computer asleep. Do not shutdown the computer.

Classroom Habits

- Center the device on the desk.
- Close the lid of the laptop before standing up.
- Lock the computer before walking away from it.
- Do not put any foreign objects (i.e. pencil) on the laptop keyboard (if the lid closes, it will break the screen).
- Follow all directions and rules provided by the teacher.

Care of Device at Home

- Fully charge the device each night.
- Use the device in a common room of the home.
- Store the device on a desk or table - never on the floor!
- Protect the device and power charger from:
    - Extreme heat or cold
    - Food and drinks
    - Small children
    - Pets