



Cornwall-Lebanon School District

One-to-One Device Handbook

A Guide for Students and Families

2026–2027 School Year

Table of Contents

Welcome to the One-to-One Program.....	4
Student and Family Questions and Answers.....	4
Responsible Use Policy	6
Acceptable uses include:.....	6
Unacceptable uses include, but are not limited to:	6
Liability	7
Daily Use.....	7
Network Access.....	7
Digital Communication.....	8
Care of the Device.....	8
Security	8
Loaner Devices	8
Backing Up Your Work	8
Troubleshooting.....	8
Damage or Theft	8
Damage, Loss, and Repair Costs	9
What families pay for	9
Payment plans.....	9
Optional Device Insurance	9
Cost.....	9
What it covers.....	9
What it does not cover	9
How to enroll	10
Artificial Intelligence (AI).....	10
How the District Keeps Students Safe Online	10
Web Content Filtering (Securly).....	10
Student Safety Monitoring (Bark for Schools)	11
Requesting Stricter Filtering (Education-Only Access).....	11
Guidelines for Cyber Safety	11
Cyberbullying	12
What is a cyberbully?	12

A cyberbully might:	12
Five ways to protect your child:.....	13
Is your child a victim?	13
Warning signs can be hard to spot, but may include:.....	13
If you suspect cyberbullying:.....	13
Device Use and Classroom Routines	14
Lockers.....	14
Hallways	14
Classroom Habits	14
Care of the Device at Home	14

Welcome to the One-to-One Program

Cornwall-Lebanon School District is committed to helping every student learn and grow with the help of technology. Through our One-to-One (1-to-1) program, the District lends each student a device to use for schoolwork. “One-to-One” simply means one student with one device.

A device is a tool. It does not replace your teacher. It supports the lessons your teacher plans and gives you new ways to create, research, and share your work. With a device, learning can happen anytime and anywhere, not just during the school day.

Here is what each student receives, by grade level:

- **Kindergarten through Grade 1:** an iPad, used in the classroom.
- **Grades 2 through 12:** a Windows 11 laptop.

Along with the device, students use everyday learning tools such as Schoology (the District’s learning management system, where teachers post assignments and lessons), Microsoft 365 (Word, Excel, PowerPoint, and OneDrive for saving files online), Clever (a single sign-on portal that opens many programs with one login), and Edmentum programs like Exact Path and Study Island for practice and skill-building.

Teachers blend traditional lessons with digital resources and help students become confident, independent learners. The District also provides ongoing training so teachers can use these tools well.

Student and Family Questions and Answers

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

A: The program is designed to:

- Give students access to learning anytime and anywhere.
- Help teachers adjust lessons to fit each student’s needs.
- Build the digital skills students will need for college, careers, and everyday life.
- Open up learning opportunities that reach beyond the walls of the classroom.
- Encourage students to think critically and solve real-world problems.
- Support responsibility, collaboration, and a lifelong love of learning.

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

A: It is a District program that gives each student a District-owned device to use as a learning tool in and out of the classroom.

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

A: When students use technology well, they tend to dig deeper into their learning and build skills they will use for the rest of their lives. To prepare for college, careers, and a connected world, students need to be comfortable using digital tools, working with others, and managing their

own learning. The 1-to-1 program is built to strengthen good teaching with the smart use of technology.

Q: When will I receive my device?

A: Students receive a device at or near the start of the school year, once all required forms and agreements have been signed and returned. Depending on your grade level, those forms are handed out at the beginning of the year and must be returned before a device is given out.

Q: Who owns the device?

A: Cornwall-Lebanon School District owns every device. Because the device is borrowed, not yours to keep, it is important to take good care of it: leave all ID tags and labels in place, and never write on it, decorate it, or damage it.

Q: May I take my device home?

A: Students in grades 6–12 may take their laptops home once the Student Agreement and Insurance forms have been signed. Devices for students in grades K–5, iPads in grades K–1 and laptops in grades 2–5, stay at school in the classroom or charging cart unless a teacher or administrator says otherwise.

Q: May I use the Internet at home with my device?

A: Yes, you may use the device on your home Internet to support your schoolwork. The District places a content filter on the device, but no filter is perfect. Parents and guardians should not rely on the filter alone to block everything inappropriate. Never try to bypass, remove, or tamper with the filter, doing so violates the District's **Internet Acceptable Use Policy (#815)**.

Q: What do I do if my device does not work or is damaged?

A: Report any problem to Technology Services as soon as you can, usually through your teacher or your school's help desk. Do not wait, because a small problem can turn into a bigger one. If the device needs repair, the District will fix it, and you will be given a loaner device to use in the meantime. Never take a District device to an outside repair shop or try to open it yourself. Only District staff may repair these devices.

Q: May I install games or other software?

A: Your device is for learning. On laptops, you may install legal, properly licensed software or apps that support your schoolwork, but the District cannot promise that personal software will work or provide support for it. Any costs or subscriptions are the responsibility of the student and family. Installing hacking, monitoring, or "sniffing" software will result in immediate loss of device privileges with no insurance refund. If a software program is lost when the District repairs or re-images a device, the District is not responsible for replacing it. (Apps on K–1 iPads are managed and installed by the District.)

Q: Can I print from my device?

A: Devices do not print to school printers. Turn in your work through Schoology, by email, or by sharing it in Microsoft 365. You may set up a home printer on a laptop, but the District cannot guarantee it will work or help troubleshoot it.

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

A: You will use your device in most classes. When a class does not need it, or during lunch, store it in your locker or an assigned charging station. You are responsible for your device at all times, never leave it unattended or unsecured.

Q: Is there anything special I should do at home?

A: Plug your device in overnight so you arrive at school with a full battery, and bring both your device and its charger every day. You are responsible for being prepared for class, so come to class with a charged device.

Q: How long will I have my device?

A: Your device is yours to use for the school year. Middle school and high school students keep their laptops over the summer through their senior year. For elementary school students, Technology Services collects the device before summer break or if a student withdraws. When the next school year begins, students receive a device again after all required forms are signed.

Q: Should I back up my files?

A: Yes. You are responsible for your files. If a device needs repair, Technology Services may have to erase everything on it. Save your work in Microsoft OneDrive (included with Microsoft 365) or another cloud storage service. That way your files are safe and you can open them from any device.

Responsible Use Policy

Students are encouraged to use District resources (devices, software, email, and the Internet) for learning and school-related activities. The device belongs to the District and is meant to be used by the student it was issued to, for school purposes.

Acceptable uses include:

- Using software, hardware, email, and the Internet for schoolwork.
- Researching information from libraries, databases, and websites to support learning.
- Communicating and collaborating online for school projects and assignments.

Everyone is expected to act in an honest, ethical, and legal way online. **Using these resources is a privilege, not a right.** Misusing them can lead to loss of privileges as well as disciplinary, legal, or other action.

Unacceptable uses include, but are not limited to:

- Anything that breaks the law or the Internet Acceptable Use Policy (#815), violates online etiquette, disrupts learning, or threatens the security of the District network.
- Using instant messaging or screen-sharing with other students during school without a teacher's permission.
- Sharing material that breaks the law, including copyrighted work used without permission; or threatening, harassing, pornographic, or obscene content.

- Sending messages, images, or other content that is sexually explicit or that harasses others. This is prohibited by the District.
- Using the device for personal money-making, advertising, political activity, junk mail, or chain letters.
- Reading, deleting, copying, forging, or changing other people's email or files.
- Creating or spreading computer viruses or other harmful programs.
- Copying or installing District software without permission, or deleting and disabling installed software.
- Vandalism of any kind: harming data, networks, or websites, or trying to break security codes or passwords.
- Damaging hardware or software, or trying to change how the system is set up.
- Intentionally overloading school computer resources.

Email and other school communication systems come with responsibilities. Students are expected to communicate as respectfully online as they would in person or in writing, and to keep their passwords private. Trying to access someone else's account, or pretending to be another person online, is prohibited and will lead to disciplinary action. Anonymous or forged messages are treated as violations.

Students should understand that the District cannot guarantee privacy on its systems. The District may access email and files for maintenance, investigations, checking Internet history, or sharing information with law enforcement when required. Anything created, stored, or sent on District devices, accounts, cloud services, or the network is District property and may be reviewed at any time.

This agreement applies whether the device is online or offline. Any attempt to break these rules, whether it succeeds or not, may result in loss of privileges, school discipline, and legal action. The District may also seek payment for damage, loss, or replacement of equipment or services. The District's decision about misuse is final.

Liability

Only the student a device is issued to may use it. Even though students are responsible for caring for the device, it remains District property. The District owns the licenses for software on the device, and that software may not be copied or moved to any other device.

Daily Use

Middle and high school students must arrive each day with a fully charged device and its charger. Students who repeatedly come unprepared may face appropriate consequences. Elementary students return their device to the classroom cart and plug it in to charge at the end of the day.

Network Access

Use of the District network follows the District's **Internet Acceptable Use Policy (#815)**. A current copy is available on the District website.

Digital Communication

Students use email, messaging in Schoology, and other approved tools to communicate with teachers and staff. All communication should follow the rules in the student handbook and be respectful and appropriate.

Care of the Device

Keep devices away from extreme temperatures. Do not leave them in places colder than about 35°F or hotter than about 90°F. Keep food, drinks, and pets away from the device and charger. Avoid rain, wet hands, and high humidity. Never leave a device in a vehicle; this invites theft and exposes it to harmful temperatures, and is considered negligence.

Do not decorate or personalize the device or its accessories in any way. This is treated as vandalism and may lead to consequences and, where appropriate, payment for repairs.

Security

Middle and high school students should keep the device with them, locked in their locker, or in a charging station while at school. Always guard your device closely and never leave it on a car seat, a bench, or anywhere tempting to others. You are responsible for any loss or theft. Elementary students should keep their device in the classroom or classroom cart unless a teacher says otherwise.

Loaner Devices

If your device stops working, Technology Services will give you a loaner to use while yours is repaired. All the same rules and responsibilities apply to a loaner device.

Backing Up Your Work

Students are responsible for backing up their own files. Save your work in Microsoft OneDrive so you can reach it anytime, anywhere, on any device. If a device fails or gets a virus, it will be erased and re-imaged, and Technology Services will not be able to recover files stored only on the device.

Troubleshooting

Report any device problem, software glitches, syncing issues, and the like, to your teacher or Technology Services right away. Students may not try to fix hardware problems themselves, and no District device may ever be taken to an outside party for repair. Failing to follow this rule may be treated as vandalism or negligence, no matter the outcome.

Damage or Theft

Report any physical damage to Technology Services immediately, and no later than the next school day. Technology Services will arrange a repair and a loaner if needed. The student and family are responsible for damage to District devices and may owe the cost of repair or

replacement under the District's device insurance policy. Students are responsible for full expense of any loss or theft, so please take care to keep the device secure.

Damage, Loss, and Repair Costs

Students and their family are responsible for any damage to, or loss of, the District-issued device, charger, and accessories. Because the device belongs to the District and is loaned to the student, caring for it well is an important responsibility for the whole family.

What families pay for

- If a device is damaged or lost and must be repaired or replaced, families are charged only for the full cost of the parts.
- The District does not charge for labor. All repairs are completed by District technicians at no labor cost to families.

Payment plans

We understand that repair or replacement costs can be difficult to manage all at once. The District is glad to work with parents and guardians to set up a payment plan that fits the family's budget. If you have a question or concern about a cost, please contact Technology Services or your school office so we can find a solution together.

As always, report any damage, loss, or theft to Technology Services right away, no later than the next school day, so the device can be repaired or replaced quickly.

Optional Device Insurance

To help families manage the cost of accidental damage, the District offers optional device insurance. Insurance is not required, but it can lower what a family pays if a device is accidentally damaged.

Cost

The annual premium is **\$25 per student**, which provides coverage for the school year.

What it covers

Insurance covers **accidental damage**. With insurance, a family pays only **10% of the actual cost of the parts** for a covered repair. As always, the District does not charge for labor.

What it does not cover

Insurance does not cover intentional damage, loss or theft, or lost chargers. For these, the family is responsible for the full cost of the parts (still with no labor charge), as described in the Damage, Loss, and Repair Costs section. Payment plans are available to help.

How to enroll

To enroll, complete the insurance form and pay the \$25 premium by check made out to Cornwall-Lebanon School District. If you have any questions about insurance, please contact Technology Services or your school office.

Artificial Intelligence (AI)

Artificial intelligence (AI) tools are programs that can write text, answer questions, solve problems, create images, or hold a conversation. Common examples include chatbots and writing or homework “helpers.” These tools can be useful, but they can also be wrong, and using them in place of your own thinking can get in the way of real learning.

For that reason, students may **not** use artificial intelligence for any schoolwork or on a District device unless a teacher specifically instructs them to. When a teacher does allow AI for a particular assignment, students must use it only in the way the teacher describes.

In short:

- **Do not use AI tools unless a teacher tells you to.** This includes writing, homework, projects, quizzes, tests, and any other assignment.
- When a teacher allows AI, follow their directions exactly to use only the tool and the steps they approve.
- Turning in AI-generated work as your own, without a teacher’s permission, is a form of cheating and will be handled like other academic dishonesty.
- Always do your own thinking first. AI can be confidently wrong, so anything it produces must be checked and is your responsibility.
- Never share personal information about yourself or others with an AI tool.

Using AI in a way that is not allowed is a violation of this handbook and the District’s Responsible Use Policy, and may result in loss of device privileges and other consequences. If you are unsure whether AI is allowed for an assignment, ask your teacher first.

How the District Keeps Students Safe Online

Keeping students safe is one of the District’s highest priorities. To help protect students whether they are at school or at home, the District uses safety technology on its devices and accounts. These tools work alongside, not instead of, the supervision and support that families and staff provide.

Web Content Filtering (Securly)

The District uses **Securly**, a web content filter, on student devices and District accounts. Securly blocks pornography, violent or harmful websites, and other content that is not appropriate for school. Because it follows students on their District laptop, the filter helps keep them safe both at school and when the device is used at home.

Using a filter like this also helps the District meet the **Children's Internet Protection Act (CIPA)**, a federal law that requires schools to filter or block harmful online content in order to receive certain federal funding. No filter is perfect, so families should still help supervise online activity at home. Students must never try to bypass, disable, or work around the filter, doing so violates the Internet Acceptable Use Policy (#815).

Student Safety Monitoring (Bark for Schools)

The District also uses **Bark for Schools**, a student-safety tool that watches for warning signs that a student may be in danger. Bark reviews activity in District accounts such as email, documents, and other District tools and looks for content that may point to bullying, threats of violence, self-harm, or other serious safety concerns.

When Bark detects something that may be serious, it alerts District staff so they can check in, offer support, and involve families or other help when needed. The goal of this monitoring is student safety and wellbeing, not to get students in trouble. It is also a reminder that District accounts and devices are not private and may be reviewed at any time, as explained in the Responsible Use Policy. If you or someone you know is struggling or in danger, please tell a trusted adult right away.

Requesting Stricter Filtering (Education-Only Access)

Parents and guardians may ask the District to place an even stricter filter on their child's device that limits Internet access to educational sites only. This is an optional setting that families can request.

Please note: this stricter setting also locks down search and video features. Because some assignments rely on searching the web or watching videos, your child may not be able to complete certain assignments as they are given while this lock-down is in place.

If an assignment cannot be completed because of the requested filtering, the student should work with the teacher on an alternative assignment. To request education-only access, please contact Technology Services or your school office.

Guidelines for Cyber Safety

Technology opens up amazing learning opportunities, but the Internet is not an all-access pass. Students of every age need guidance and supervision online. Here are tips to help families keep children safe:

- Spend time online together. Ask your child to show you their favorite sites, and talk openly about online dangers. Make sure passwords stay private from everyone except a parent or guardian, even close friends have been known to misuse them.
- Keep devices in a common, shared space at home rather than behind a closed bedroom door. It is much harder for someone to take advantage of a child when the screen is in view.
- If you can, add content filtering at your home modem or router. Remember that the District filter, like all filters, is not perfect, do not rely on it alone.

- Stay aware of your child’s online accounts and check in regularly. Be open about why: keeping them safe is part of your job as a parent or guardian.
- Teach responsible habits. Remind your child never to meet in person with someone they only know online; never share personal details like full name, home address, school, or phone number; never open files or pictures from unknown sources; and never reply to messages that are mean, obscene, or harassing. Remind them that not everything or everyone online is what it seems.
- Set clear expectations. Decide together which sites are okay for research and for fun, and write the rules down so they are easy to remember.
- Stay connected with your child’s school. Staying in touch with teachers and counselors makes it more likely you will hear about anything happening online that could affect school.
- Remember that people online are not always who they claim to be. Show your child how easily someone can pretend to be someone else.
- Watch streaming and social apps together. Video and social platforms are hugely popular and mostly rely on users to report bad content, so a child can stumble onto something upsetting. Guide their choices, and tell them to come to you if they ever see something that bothers them.
- Encourage your child to pause before posting. A good test: “Would I be okay with my parents, teacher, principal, and grandparents seeing this?” If not, don’t send it.
- Learn the privacy settings on the apps, games, and sites your child uses. Look for sections labeled “parents,” “privacy,” or “safety.”

Cyberbullying

Cornwall-Lebanon School District is committed to a safe, healthy, and respectful environment for every student. Bullying creates fear, gets in the way of learning, and can lead to more serious harm, so the School Board does not tolerate it. For full details, see **School Board Policy #249 – Bullying/Cyberbullying**.

What is a cyberbully?

A cyberbully is someone who uses technology repeatedly to be cruel to another person. Online attacks can hurt even more than face-to-face bullying because people can hide behind a screen and act in ways they never would in person. A rumor or cruel post can spread fast and follow someone everywhere there is an Internet connection even at home, where they should feel safe.

A cyberbully might:

- Send repeated unwanted calls, texts, or messages.
- Post repeated cruel comments or send unkind messages to a victim.
- Create a fake profile to embarrass someone.
- Break into someone’s account to change settings, lock them out, or pretend to be them.
- Forward private messages or photos, sometimes after tricking the victim into sharing them.

- Post embarrassing photos or videos of the victim.
- Spread rumors through messages, social apps, or other public spaces.
- Gang up on or humiliate someone in online games or virtual spaces.

Five ways to protect your child:

1. Remind your child never to share passwords, even with good friends.
2. Ask your child to tell you right away about any bad experience online, and save the evidence in case it is needed.
3. Encourage your child not to respond to a bully, reacting often makes it worse. Block the bully using privacy settings instead.
4. Remind your child to treat others kindly, to not strike back, and to stand up for friends who are being bullied.
5. Set healthy limits on social time online. The more time spent online, the more likely problems become.

Is your child a victim?

Many children don't tell their parents they are being bullied, they may fear losing Internet access or feel ashamed and blame themselves. Reassure your child that no one deserves to be mistreated, that people sometimes hurt others because they are hurting too, and that you need to know what's going on so you can help.

Warning signs can be hard to spot, but may include:

- Seeming nervous or unusually quiet, especially after being online.
- Wanting much more or much less time online than usual.
- Not wanting to go outside or to school.
- Trouble sleeping or eating.
- Headaches or stomachaches.
- Trouble focusing on schoolwork.

If you suspect cyberbullying:

Talk with your child and work out a plan together. You might:

- Contact the school. Let teachers, the counselor, or the principal know so they can watch for signs and share strategies or programs already in place.
- File a complaint if the behavior continues. Most apps, websites, and phone companies have anti-harassment policies and may shut down the bully's account.
- Contact the police if you fear for your child's safety. Cyberbullying can become criminal when it involves threats, extortion, stalking, obscenity, child pornography, extreme harassment, or hate crimes.

If you learn your child has been cruel to someone online, find out why. Help them, but make it clear that bullying, online or off, is never okay. If your child sees someone else being targeted,

encourage them to support that person and report the abuse. Talking openly is the best way to give your child the tools to handle cyberbullying.

Device Use and Classroom Routines

Lockers

- Store your device in your locker or a charging station whenever it is not with you.
- Never pile other things on top of your device.
- Never leave your device loose at the bottom of the locker.

Hallways

- Carry a laptop securely with both hands.
- Never leave your device unattended for any reason.
- Close the laptop lid before changing classes to put it to sleep. Do not shut it down.

Classroom Habits

- Keep the device centered on your desk.
- Close the laptop lid before standing up.
- Lock the screen before walking away.
- Never place objects like pencils on the keyboard. Closing the lid on them can crack the screen.
- Follow all directions and rules from your teacher.

Care of the Device at Home

- Fully charge the device every 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 charger from extreme heat or cold, food and drinks, small children, and pets.