NORTHERN LEBANON
SCHOOL DISTRICT

STUDENT DEVICE HANDBOOK

Overview

The Northern Lebanon School District provides a dedicated electronic device to all students in grades K through 12. As a key component of the district's technology initiatives, these devices serve as digital textbooks and communications tools for students. The mobile devices provide the anytime-anywhere access to learning that is needed for our students to become proficient, life-long learners. The devices have all the necessary software needed for students' learning goals, as well as an internet filter that is always active.

Students in all grades will be assigned a device – either a tablet or laptop depending on their grade and other student needs. All students except those in kindergarten are expected to take their devices home after school to complete their assignments.

The district will replace student devices every 3-4 school years as part of the program – typically, the devices will be replaced in the summer between grades 3 and 4, and again during the summer between grades 8 and 9. Graduating students will turn in their devices during the final week of their senior year, after they have completed their graduation requirements. The district will contact families 2-3 weeks before the end of the school year notifying them of the date(s) when device collection will occur. When requested, students must return their device, charging cable and protective case to their school for collection.

Student devices remain the property of the district; there is no option for students or families to purchase devices. Returned devices will be used for spare parts or sold to authorized vendors by the district.

Lost, damaged, or unreturned devices will result in fees for student's families as outlined in this Student Device Handbook. The district has eliminated its device insurance program, but we have applied a cost structure similar to the insurance program for all families with no upfront costs. In general, repair fees will equal 50% of the cost of parts or materials required to complete the repair, to a maximum of $100 per incident. A lost device will result in a flat fee of $120, which is approximately 30% of the replacement cost of any device. If the lost device is later found and in good working condition, then the replacement fee will be reimbursed. The costs for all device repairs may be revised and published annually in this handbook:

iPad Repair Fees

iPad Damage	Repair Cost
Broken Screen	$25
Broken Charging Port	$25
Broken Headphone Jack	$25
Broken Protective Case	FREE
Replacement Charger	$10
Replacement Device (if lost or destroyed)	$120*

Chromebook Repair Fees

Chromebook Damage	Repair Cost
Broken Screen	$25
Broken Top Lid	$25
Broken Bottom Lid	$25
Broken System Board	$25
Broken Keyboard	$25
Broken Protective Case	FREE
Replacement Charger	$10
Replacement Device (if lost or destroyed)	$120*

** Replacement Device fee will be canceled or reimbursed if the original device is later found and is still in good working order.*

Questions and Answers

When will I receive the district-issued device?

Students will receive their devices within their first week of school, barring any manufacturing or delivery delays from the district's equipment providers. The devices will be given to students while at school during the school day. V3 Virtual students will need to schedule a date and time to pick up their devices

Can I use my own protective case?

Students must use the protective case that the district has provided. Students and parents are not permitted to remove the case. Removing the case may result in a disciplinary referral. Replacement cases will be provided free of charge.

Can I decorate the district provided case or device?

No - you may not decorate the case or device. The device and the case remain the property of the district and decorating it will result in disciplinary referral. There may be an associated cost to replace parts or restore the device to its original condition if the decorations cannot be removed.

Who owns the district device?

The devices are the property of the Northern Lebanon School District. Students are expected to take good care of them, and must leave all labels and asset tags in place.

May I take the district device home?

Kindergarten students will leave their devices in their classroom, unless otherwise instructed by their teachers. Students in grades 1 through 12 are expected to take the device home after school. Students should use the provided charger to recharge the batteries each night, to prepare for the next school day. In some special circumstances, parents may request that a student's device remain at school. Such requests must be discussed with your student's principal/assistant principal.

May I access the Internet at home with the district device?

You may use the device at home and access your home internet in support of academics. There is an Internet filter installed, however; parents should not rely on this filter alone. Parents should be aware of their student's Internet use at home and should talk with them about how to stay safe online.

Can I bypass the Internet filter?

No one should ever try to tamper with the Internet filter. Any attempts to remove or bypass the filter will be considered a violation of the district' acceptable use policy. Trying to bypass the Internet filter will result in a disciplinary referral.

Can I set up a printer on my district device?

Printing from iPad devices is not supported. Students can add a personal printer to Chromebooks, but we cannot provide support for home printers. The steps to do so are outlined here: https://support.google.com/chromebook/answer/7225252?hl=en.

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

Only District personnel are permitted to fix broken devices; do not try to fix the device yourself or allow anyone else to try to fix it. District-provided devices are property of the School District.

Please report any problems to the school as soon as possible. Students in grades 7-12 should bring their device to the High School Library during the 1st period of any school day, where the Technology team will assist them. A technician will provide tech support, repair a broken device, or issue a loaner device for that school day, while repairs are completed. Nearly all repairs are completed on the same day they are reported. Loaner devices must be returned to the library by the end of that school day - they should not be taken home unless instructed by the Tech Services team.

Can I install my own software on the district device?

No - any software must be installed or authorized by the District.

How do I carry my device?

Be sure to remove any objects (like pens or pencils) from the keyboard area, then carefully close the lid of the Chromebook. Pick up the Chromebook by the hinge, like the spine of a textbook. Keep a firm grip on the hinge but do not press on the top lid because you can break the LCD screen. The hinge on a Chromebook can become damaged if you carry it with the screen open

For an iPad, the cover should always be placed over the screen when carrying it. Be sure to keep a firm grip on the iPad while carrying it.

Is there anything special I should do with my District device at home?

Just be sure you plug it in overnight so you come to school with a fully charged battery. 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 morning.

How long will I have the District device?

New students are issued devices when they enroll in the district. Students will use the same device for more than one school year. During the final week of school each year, devices will be collected from students in 3rd, 8th, and 12th grade. Students who return to the district in the fall will be issued a device during the first week of school. All other students will take their devices home over the summer to be brought back for use during the next school year.

Responsible Use Policy

As the Northern Lebanon School District embarks on the journey to enrich learning experiences, students are encouraged to use District resources such as computers, software, e-mail, 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
- E-mail 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, those uses; that violate the law or the Acceptable Use Policy (Board Policy 815), the rules of network etiquette, and that would disrupt the educational environment or hamper the integrity or security of school network. Some unacceptable practices include:

- The use of Instant Messaging or screen-sharing programs with other students during school hours without teacher consent.
- 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, e-mail 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 Northern 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 school 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 e-mail 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 user account to use another's name, e-mail, or computer address or workstation to send e-mail 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 e-mail 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 e-mail 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 Northern 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.

Guidelines for Usage

Liability

When a device is issued to a particular student, then that student, along with his or her parents or legal guardians, are the only authorized user of that device. While each student accepts responsibility for the care and use of the device, the device remains the property of the District. Only district personnel may disassemble the device, remove the protective case, or modify any software on the device. The District retains all licenses for the software installed on the device, and no software may be copied or transferred to another device. In the event of damage to the laptop caused by vandalism or negligence, parents will be charged for the required repair in accordance with the fees stated in this handbook.

Daily Use

Students are expected to arrive at school every day with their device battery fully charged. Students that repeatedly fail to have their battery fully charged may be subject to appropriate disciplinary action.

Network Access

Use of the District network is governed by the District Acceptable Use Policy. Students have a personal folder in the cloud accessible only to them and District personnel. They may also have access to group folders, shared by other students and teachers.

Web Access and Email Access

Students will utilize their school issued email account to communicate to teachers and administrators. Under no circumstances shall students use their own personal email to communicate with District employees.

Power Adapters

On a case-by-case basis, loaner power adapters are available in the library. A student may borrow a charger during the day by signing it out. It must be returned at the end of the day.

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 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 (please refer to the section titled Liability).

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

Loaner Devices

Should the 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 any personal photos or files to their district-provided online storage, such as Google Drive. The district is not responsible for lost photos or files stored on devices. If a student's device malfunctions, it may be factory reset by technicians to correct it. The Technology Department will not take preventive measures to save or recover data stored on the student device.

Troubleshooting

Students should report any device problems (i.e. printing, software issues, syncing, etc.) to the classroom teacher or to the Technology Department as soon as possible. Students are prohibited from trying to disassemble the device or remove any parts of the device. District-owned devices should not be taken to a third party for repair or troubleshooting. All issues related to student devices must be reported to the Technology Services team and will be repaired by district-authorized personnel. Failure to follow this policy, regardless of the resolution, will be considered vandalism and or negligence. (Please refer to the section titled Liability.)

Damage / Theft

All physical damage to the device must be reported immediately to a responsible adult-either at home or at school. It must be reported to the Technology Department no later than the next school day. The Technology Department will arrange for repair and a loaner as needed. Accidental or intentional damage is not covered by our warranty. The parent/student is responsible for all damages to District issued devices and subject to a cost of repair or replacement.

Guidelines for Safe and Responsible Use

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 online 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 & 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.

Speak to your Internet Service Provider about options like limiting time usage for certain devices.

Always maintain access to your child's social networking and other online accounts and randomly check his/her e -mail. Be upfront with your child about your access and reasons why. Tell him or her that protecting them is your job as a parent.

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 on-line
- 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 stick with 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. Children log on to see the funny homemade video the other children are talking about; to watch their favorite soccer player score a winning goal; even to learn how to tie a slip knot. 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. He should ask himself, "Would I want my parents, my principal/assistant 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."

Cyber-Bullying

The Northern 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 School 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 Board Policy 249.

What Is a Cyberbully?

A cyberbully is someone who uses Internet 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.

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.

Here are five suggestions to protect your child:

- Remind your child never to share his/her passwords, even with good friends.
- 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.
- 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.
- 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.
- 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.

Is Your Child a Victim of Cyberbullying?

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.

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 stomach aches.
- Trouble focusing on schoolwork.

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/assistant 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. Cyberbullying can cross into criminal behavior if it includes threats of violence, extortion, child pornography, obscenity, stalking, extreme harassment, or hate crimes.

If you learn that your child is being cruel to someone online, find out why. Often, cyberbullies 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.

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.

Cyberbullying 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

Protect the Device from:

- Extreme heat or cold
- Food and drinks
- Small children
- Pets

Care of Device at Home:

- Charge the device fully each night
- Use the device in a common room of the home
- Store the device on a desk or table - never on the floor

Traveling To and From School:

- Do not leave the device in a vehicle
- If someone is threatening you to steal your device, give it to them. Then tell a staff member as soon as you arrive at school
- Stolen devices are to be reported to the local police department as soon as possible

Lockers:

- Your device should be with you at all times, unless instructed otherwise. If it is not with you, make sure it is secured
- Never pile things on top of your device
- Never leave your device on the bottom of the locker
- Never leave the locker set to open without entering the combination

Hallways:

- Keep your device in the protective case at all times
- Always use two hands to carry the device
- Never leave the device unattended for any reason
- Close the lid of your Chromebook before you change classes to put the computer asleep

Classroom Habits:

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