

Universal Access to Technology

Student Device Handbook



Languages	2
Introduction	2
Why provide a device for every student?	2
Device Types	2
Receiving your Technology	2
Technology Basics	3
Caring for your MPS iPad or Chromebook	3
Transporting and Storing	3
Logging in and Passwords	4
Privacy, Security & District Monitoring	4
Expectations for Use	4
Responsible Uses	4
At Home Use	5
Unacceptable Behavior and Activities	5
Incident Levels for Damaged or Inappropriate Use of Technology	6
Pictures, Content, Data	7
Sound, Music, Games	7
Apps/Extensions	7
Other Resources	8
District policies of importance	8
Internet Access	8
Technical Support	8
Links	8
Technology Use Pledge	9

Languages

This is the **ENGLISH** version of the Student Device Handbook. To view a translated digital version, please visit [MPS Technology Student Handbook](#)¹ on The Source.

Introduction

The Universal Access to Technology program at MPS is in place to provide all students with an appropriate learning-level device, which they are able to use both at home and at school. Students in most grade levels will take these devices to and from school each day. This program is essential in ensuring learning-level appropriate access to technology is available for all students.

Why provide a device for every student?

Technology can be a powerful tool, especially when students are provided equal access to devices that are appropriate for their learning-levels. Technology transforms learning experiences, because it allows instruction to be personalized to meet students' individual needs and interests, as well as having the ability to support and expand classroom learning activities.

Device Types



Grades **PreK-2** receive iPads.



Grades **3-12** receive Chromebooks.

Note: Some students receiving Special Education services might need an iPad instead of a Chromebook, or vice versa based on their IEP. Families should contact their student's case manager, if they need something different than what they've received.

Receiving your Technology

Technology will be distributed to students by their school. Student technology should be assigned to students and tracked in the district student technology asset management system.

If your iPad or Chromebook requires set-up, use the getting started guides included with your technology package. These can also be found on [The Source](#).²

Technology Basics



Caring for your MPS iPad or Chromebook

It is your responsibility to take good care of the iPad or Chromebook that your school is lending you for instructional use. Here's what you can do to care for that device and keep your technology safe.

- Charge your device every night.
- Keep it safe when you're going to school and when you're in class.
- Be careful with your device.
- Be responsible and respectful when using it in school and at home.
- No food or drink should be near the technology.
- Carefully place cords/cables into the technology.
- You cannot decorate the exterior of the iPad/Chromebook. This includes stickers, decals, or other personalized items .
- Heavy objects should never be placed on top of technology.
- Be sure to pick up and carry your Chromebook using the keyboard, not the screen (This is the most common cause of damage).
- Make sure there is nothing on the keyboard before closing the lid of the Chromebook.
- Every device contains an MPS barcode decal. Do NOT remove, damage, or alter the decal in any way.



Transporting and Storing

Weather and Environment

Protect your technology from the weather. Avoid exposing your iPad/Chromebook to extreme temperatures by keeping it in its case at all times. Always carry it in a backpack or bookbag when outside. Keep in mind the following information:

- Do not leave your technology in the heat in temperatures above 95° F.
- Do not leave your technology in cold temperatures below 32° F.
- Keep your technology away from water and extreme humidity.

General Transportation and Storage

1. To prevent theft, never leave a device in an unsupervised area at school. Unsupervised areas include unlocked classrooms, locker rooms, computer labs, the library/media center, the lunchroom, restrooms, hallways, or anywhere on the school grounds, including athletic fields and playgrounds.
2. Do not leave a device on the floor or ground, even if the device is in a bag or backpack. It could be stepped on and damaged.
3. Students in grades 6–12: if you don't need your device for a class, or if your teacher has told you not to bring the device to class, store and lock it in your locker. Do not leave the device unattended in a bag or backpack. Anytime your device is away from you and not at home or in a secured locker, you run the risk of it being stolen.



Logging in and Passwords

MPS iPads and Chromebooks have a standard configuration and are ready to use. Students will need their MPS issued email address and password to access the technology and learning tools. Teachers can reset passwords for students who do not remember their password.

Students should [enroll in Password Self-Service](#)³ after receiving their email address and password. By enrolling in this service, you will be able to [change your password](#)⁴ in the future, in case it is forgotten.



Privacy, Security & District Monitoring

A digital environment opens up opportunities for both positive and negative aspects of data collection and sharing. To protect children, there are three federal laws that govern the collection, use, and sharing of personal information. In order to remain compliant with these federal laws and additional state laws, MPS reviews data privacy and security policies for all software and applications that are available in our self-service/app stores. The district also maintains a list of vetted websites, which require access to student information and/or require a student to log-in. MPS also uses a variety of different software programs and applications that help to manage student safety, as well as content-filtering that detects and blocks harmful or dangerous material while on district provided technology.

All MPS devices are scanned remotely on a regular basis to ensure that security settings have not been changed or deleted. If a student has accessed the internal parts of the device, installed an app that changes the device settings, or manually changed the settings, they will be subject to behavioral consequences, in accordance with the incident levels outlined in this document.

Expectations for Use



Responsible Uses

Students will have a Chromebook or iPad assigned to them. If they are transporting their Chromebook or iPad between school and home each day, they must be sure to bring their technology back to school each day with a fully charged battery.

Students must bring their device to all classes, unless a teacher specifically instructs them not to do so. Students are responsible for completing all course work, even if they leave their assigned technology at home.

District-issued technology is intended to be used for school activities. Only Minneapolis Public School students can login to district-issued Chromebooks and iPads.

Students should log in to their Chromebook/iPad using their school-issued email account. You should always be a good digital citizen by following these guidelines:

- **Respect and Protect Yourself** – Show respect with your actions. Be careful sharing information, images, and other media that you post online. Do not share personal information, contact details, or your activity schedules. Protect your password; do not share your password with anyone.
- **Respect Yourself and Others** – Show respect to others. Do not use technology to antagonize, bully, harass, or stalk people. You must follow the [Minneapolis Public School District's Bullying and Hazing Prohibition Policy 5201](#).⁵ Immediately report any inappropriate behavior directed at you when you are online to your teacher.

Students may receive a replacement iPad or Chromebook when their assigned device is being repaired. If there is a delay in assigning a replacement, the teacher will allow the student to complete required coursework without a device.



At Home Use

If a student brings their technology home for learning purposes, they must comply with all MPS Policies and Regulations (Refer to Policy 6415 for internet and educational network use). Students can connect to wireless networks using their district devices, but all users of the device must comply with district policies.



Unacceptable Behavior and Activities

Students may not use district technology resources to:

- Find, create, or send information to spread lies or misinformation, harass, harm, or bully others.
- Gain unauthorized or inappropriate access to district technology resources.
- Use, retrieve, store, or send inappropriate language, pictures, or other digital content.
- Engage in cheating, including getting or giving answers to tests; searching for and/or copying answers or information on the internet or other electronic resources; copying and submitting someone else's information, work, or assignment as their own; or participating in other similar forms of electronic cheating.
- Violate copyright or licensing agreements.
- Access inappropriate or blocked resources.
- Share or post any personally-identifiable information about yourself or others that might help someone locate or contact you or someone else. This includes such things as email addresses, full names, home or school addresses, phone numbers, parent or guardian names, or school name.
- Modify the operating system, add restrictions, remove security profiles, or vandalize district technology resources.
- Install any apps other than those authorized by Minneapolis Public Schools.



Incident Levels for Damaged or Inappropriate Use of Technology

Level 1 incidents

Level 1 behavioral missteps are minor and are addressed within the classroom community. Interventions aim to correct and teach alternative behavior, so students can learn and demonstrate safe and respectful behavior.

Examples of Level 1 device incidents may include:

- Using apps or the internet to access content not required for the learning activity;
- Treating the technology carelessly (such as removing its case, not keeping it in a backpack during transport, eating or drinking while using the device).

Level 2 incidents

Level 2 behavioral incidents are also classroom-managed and may include additional interventions from administrators or other support staff, who push into the classroom to provide support or facilitate brief out-of-class conversations or reflection time.

Examples of Level 2 device incidents may include:

- Intentional damage to a device or accessory (such as a broken screen caused by intentionally throwing or dropping the device; swinging a bag or backpack with a device inside; stepping on the device; intentionally spilling a liquid on the device; damage caused to a device that was not in the district-issued case).
- Sharing material without permission, cheating or plagiarizing, by using the work of others that is accessed digitally.
- Tampering with the internal components of the device or making unauthorized modifications to the device operating system, known as hacking the device.
- Using the camera to take someone else's picture without their permission.
- Loss of a device or accessories.

Level 3-5 incidents

Level 3-5 incidents are more significant in nature and may present a safety concern for the student and/or others. These incidents may result in a temporary loss of privilege to take a device home, or require supervision while the device is in use.

Note: Some of these violations may also result in the **removal or suspension of a student** from school, along with a plan for additional interventions and supports.

Examples of Level 3-5 incidents may include:

- Repeated intentional damage or loss of technology or accessories.
- Using a device for cyberbullying, bullying, or harassment.
- Sending or posting inappropriate or harmful messages or images.
- Other actions which violate the guidelines in this handbook.

NOTE



Schools may place a limit on the number of Chromebooks/iPads that may be replaced. If a student has repeated incidents, especially intentional damage or extreme misuse, they may **lose privileges** to have a Chromebook/iPad that is checked out to them **for the remainder of the academic year.**



Pictures, Content, Data

All recordings and pictures created with the device are subject to MPS policies as well as state and federal laws. Students may only take photographs, video, or record audio during the school day, if a teacher or administrator assigns it as schoolwork. Never photograph, record video, or create an audio recording of another person without that person's knowledge or permission.

- Use of electronic devices and cameras are strictly prohibited in locker rooms and bathrooms.
- Do not use the camera to take inappropriate or sexually explicit photos or videos.
- Do not use the camera to take pictures or share the personal information of yourself or another individual.
- Do not use the camera or microphones to embarrass, bully, or harass anyone in any way, including students, staff or other individuals.
- Do not email, post to the internet, or electronically send images, video, or audio recordings of other individuals without their written permission.



Sound, Music, Games

The sound on your Chromebook/Ipad must be muted at all times unless your teacher approves turning on the sound or turning up the volume for a class activity. Your teacher may also give you permission to use earbuds or earphones. If this happens, be sure the volume is low enough that the device cannot be heard by anyone nearby.



Apps/Extensions

Students cannot install any applications or extensions to their technology that are not approved by their school or the district. Students should not download applications or install extensions unless they are directed to do so by their teacher.

Other Resources



District Policies of Importance

- [Policy 6415: Internet And Educational Network Use](#)⁶
- [Regulation 6415B: Internet, E-Mail And Network Rules For Student Use](#)⁷



Internet Access

MPS will provide hotspots for those students who need them most. However, families should be aware that hotspot signals can drop out for a variety of reasons. High-speed internet access from a service provider will have the best connectivity. [Visit the city of Minneapolis wireless page](#)⁸ to learn about free and low-cost internet access. Families who qualify for public assistance programs can get internet access for as low as \$10/month. Families can also apply for the [Emergency Broadband Benefit](#)⁹. Due to limited availability and reliability of hotspots, we encourage families to apply for the Emergency Broadband Benefit (or other available options through the city) for low-cost internet access before requesting a hotspot.



Technical Support

IT Services Desk

If you have technical issues on a district-issued Chromebook/iPad, call the MPS IT Services Desk at ☎ (612) 668-0088. Service desk hours are 🕒 Monday-Friday from 7:30 AM-4:00 PM.

Technology Replacement

Please report technology issues to your teacher or school immediately. This includes technology that stops working, becomes damaged, or is lost or stolen.

Software and Operating System Updates

Occasionally software, apps, and operating systems require updates to keep technology functioning properly and securely. Students are expected to follow district directions for installing or updating software, apps, and operating system updates.



Links

1. bit.ly/MPStechhandbook
2. bit.ly/GetStartedGuides
3. bit.ly/enrollpassword
4. bit.ly/changepasswordMPS
5. bit.ly/policy5201
6. bit.ly/policy6415
7. bit.ly/policy6415B
8. bit.ly/MPLSwireless
9. bit.ly/emergencybroadband



Technology Use Pledge

Student Name: _____

School Site: _____

Grade: _____ Teacher: _____

Device: iPad Chromebook Hotspot

I acknowledge receiving the technology referenced above for use while I remain a student at MPS. I have read this, Universal Access Student Handbook. In order to maintain the privilege of using this technology, I agree to the following:

_____ I agree to follow the guidelines in this handbook, and will not use MPS technology, in or out of school, for inappropriate or unlawful purposes.

_____ I agree to keep my technology in my possession at all times and will not give or lend it to anyone.

_____ I agree to keep my technology in the provided case.

_____ I agree to keep my technology stored safely in my backpack when I'm not using it to lessen the chances that it will be damaged or destroyed.

_____ I agree to keep this technology charged so it's ready to use for school.

_____ I agree to return this technology to the school at the end of the year or if I leave the school.

I understand that failure to comply with any of these rules and/or district policies may result in losing my privileges to use District technology. In addition, loss, damage, or misuse of technology may incur service hours in order to restore privileges. Replacements needed due to typical wear and tear or technical issues to your device will not incur service hours or loss of privilege. The district reserves the right to limit the number of replacement technology devices it provides to a student in an academic year or to revoke privileges to technology altogether if a student misuses technology. Students must work with their building administration to determine what they need to do to obtain replacement technology in the event it is lost, stolen or damaged.

Student Signature: _____

Date: _____

Parent Signature: _____

Date: _____

Site Device Coordinator: _____

Date: _____