Plattsburgh City School District

Technology Handbook

Updated 3/26/2025

We are excited to share with you the **Plattsburgh City School District Technology Handbook**, your go-to resource for navigating the digital landscape within our schools. As technology continues to shape our world, we believe that fostering digital literacy and responsible use of technology is essential for success in today's interconnected society.

What You'll Find in This Handbook:

1. **Digital Citizenship**:
    - Learn about responsible online behavior, digital etiquette, and how to be a respectful and ethical digital citizen. We'll cover topics such as cyberbullying, privacy, and netiquette.
2. **Device Usage Guidelines**:
    - Understand the rules and expectations for using district-provided devices. From laptops to tablets, we'll outline proper care, security measures, and appropriate use both in and out of the classroom.
3. **Online Safety and Security**:
    - Discover tips for protecting personal information, recognizing phishing scams, and staying safe while browsing the internet. We'll empower you to be savvy digital users.
4. **Educational Apps and Platforms**:
    - Explore the tools and platforms we use for learning here at the PCSD.
5. **Parental Involvement**:
    - Parents, find out how you can support your child's digital learning journey. We'll share strategies for monitoring screen time, engaging in conversations about technology, and collaborating with teachers.
6. **Troubleshooting and Support**:
    - Need technical assistance? Our troubleshooting section covers common issues and provides contact information for our tech support team.
7. **Acceptable Use Policy**

1. DIGITAL CITIZENSHIP:

Positive online behavior is essential for creating a respectful and supportive digital community.

Kindness and Empathy: Responding to others with kindness and empathy fosters a positive online environment. Encourage uplifting comments, compliments, and words of encouragement. For instance, leaving a supportive message to someone shows empathy and goodwill.

C*onstructive Criticism*: When providing feedback or engaging in discussions, focus on constructive criticism. Instead of simply criticizing, offer suggestions for improvement. For example, if reviewing a peer's project, highlight both its strengths and areas for growth.

Citing Sources and Giving Credit: In academic or creative work, always give credit where it's due. When sharing information, link to the original source or mention the author. Acknowledging others' contributions demonstrates integrity and respect.

Respecting Privacy: Avoid sharing personal information about others without their consent. Respect their privacy by refraining from posting sensitive details, photos, or videos without permission. For instance, don't share someone else's address or phone number online.

Being Inclusive and Open-Minded: Embrace diversity and different perspectives. Engage in respectful conversations even when opinions differ. Avoid derogatory language or offensive remarks. For instance, participate in online forums or groups with an open mind, appreciating the richness of diverse viewpoints.

- Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude.
- Use appropriate language: vulgarity, ethnic or racial slurs, or any other inflammatory language are prohibited.
- Pretending to be someone else when sending/receiving messages is considered inappropriate.
- Transmitting obscene messages or pictures is prohibited.
- Revealing personal addresses or phone numbers of the user or others is prohibited.
- Using the network in such a way that would disrupt the use of the network by other users is prohibited.

2. DEVICE USAGE GUIDELINES:

Students will:	**Students will not:**
Follow the guidelines in the District's Acceptable Use Policy, and any relevant state and/or federal laws.	Change any settings on the device without permission from the Technology Department or District Technology Integrationist.
ENSURE that devices are charged before the beginning of each school day.	Install software without permission from the Technology Department.
Use school computers for educational purposes in a safe, ethical, and responsible manner.	Make any changes that will damage the district device.
Avoid doing anything on the school device that impacts anyone else's happiness, safety, or privacy. THINK before you post!	Transport devices with the charger plugged into it.
Play only educational games on the district device.	Trade devices, chargers, or stylus with anyone else.
Students and parents should be mindful of the district's standards around violence, harassment, bullying, and other antisocial behavior.	Share passwords, personal information such as birthday, student ID, password, social security number, address, or phone number.
Handle the device with care, keeping it clean, dry, away from food and drink, and avoiding extreme hot or cold temperatures.	Remove the silver asset tag on the device.

Use the district device on a stable platform such as a desk or table and not on a soft surface like a bed, which will block the cooling vents and cause it to overheat.	Repair a district device or replace any items that go with it.
Always have the device in their own personal possession, in the care of a teacher or another responsible adult, or in a secure location.	Attempt to circumvent (go around) or violate copyright laws, or to steal software movies, music, or any other type of protected media using a school device.
Notify a teacher or technology staff member immediately if their device is not working properly.	Use tools that prevent the web browser from logging into their browsing history.
Return the device at the end of the school year, or any other time as requested.	Delete the browsing history.

USING YOUR LAPTOP AT SCHOOL

Laptops are intended for use at school each day. Students must be responsible for bringing their laptop to all classes. This is a mandatory classroom supply to have daily for instructional purposes. Students are only permitted to use district issued devices.

Music & Games

Music and games are not allowed on the laptop during school hours in the classroom without permission from the teacher. These expectations will be set by teachers and buildings to best meet the needs of the students and staff in the respective buildings/classes. Teachers will provide written digital expectations for students and families.

3. ONLINE SAFETY AND SECURITY

Passwords: Students should keep **secure passwords**. Emphasize the importance of not sharing passwords.

Private Information: Students should understand **private information** (e.g., address, phone number, email). Remind students how to protect these details and avoid sharing them publicly.

Photographs and Geotagging: Discuss the implications of posting **photographs online**. Remind students that seemingly innocent images may reveal private details (such as license plates or street signs).

- Students and families should not take pictures in school without the person's consent.
- Students and families should not take any pictures, videos, or screenshots of live class meetings for students. No student or parent should capture, retain, or share any picture or video of a live educational lesson in Microsoft Teams.

Respecting Intellectual Property: Help students understand **copyright** and **Creative Commons** licenses. Encourage them to respect the rights of creators by properly citing sources and seeking permission when using others' work.

Online Safety and Threats: Equip students with knowledge about **viruses**, **malware**, **phishing**, **ransomware**, and **identity theft**. Teach them how to recognize and protect themselves from these digital threats.

- We have a software product, Lightspeed, which is designed to help monitor all Internet sites that students attempt to access. This software blocks inappropriate sites and logs a history of every site that each user opens. All students who attempt to find inappropriate sites may be directed to the building principal or the District Technology Office.

Student Emailing: Grades K-8: Students have school email addresses and can email only within the district. This ensures a controlled and secure environment for younger students.

Grades 9-12: Students have school email addresses and can email outside of the district. This change for older students supports college and career readiness by allowing necessary external communication.

4. EDUCATIONAL APPS AND PLATFORMS

Plattsburgh City School District Public Portal (classlink.com)

MANAGING YOUR FILES & SAVING YOUR WORK

Saving to the Cloud - One Drive Microsoft School Account

All student work will be saved on the PLATTSBURGH CITY SCHOOL DISTRICT student One Drive account. The student is responsible for managing and not sharing usernames and passwords for any school-related accounts. The student is responsible for ALL actions that occur on his/her account. If a student suspects wrongdoing or harmful content, they should notify a staff member immediately. Student accounts and material may be reviewed at any time by district officials to ensure the safety of district networks and members. It is important that students are signed into the district device with their school account and not a personal account. This will allow for access to all necessary materials. Students should NOT use personal Microsoft accounts on their district device.

5. PARENTAL INVOLVEMENT

Parents will be responsible for monitoring students' use of the laptop at home and away from school. District security is in place on the laptop, however parental supervision and review is always essential.

Parents will be responsible for reviewing the Technology Handbook with their child(ren).

Parents are asked to monitor their student's activities on the internet and in Microsoft Teams regularly.

The parent/guardian must collaborate with the school to provide monitoring and supervision of district devices during non-school hours. Below are some suggestions in assist you in carrying out your parental responsibilities:

- Investigate and apply parental controls through your internet/Wi-Fi.
- Develop a set of rules/expectations for device use at home.

- Discuss with your child to never create an account.
- Contact your child's teacher with account access questions or concerns.
- Students are encouraged to use ClassLink Launchpad for a collection of district approved applications.
- Demonstrate a genuine interest in what your child is doing with the device and ask questions and request they show you their work often.
- Encourage and assist with charging routines.
- Only allow device use in common rooms of the home (ex. living room and kitchen) and not in bedrooms.

6. TROUBLE SHOOTING AND SUPPORT

- When in doubt, restart.
- Check for updates.
- Submit a Help Desk ticket explaining the issue.

The Plattsburgh City School District Technology Help Desk can be found at:
1to1plus.com/login/Plattsburgh_NY
The link can also be found in the top left corner of The Plattsburgh City School District website.

DEVICE UNDERGOING REPAIRS- Replacement Devices (iPads/laptops)

Loaner devices will be available for use during the school day in each building. Each building will share a plan with students that contains details of the loaner device process for their building.

LOST/DAMAGED DISTRICT DEVICES

Students should notify a teacher immediately. When a device needs repair, students should follow their building device reporting process.

The following steps will be taken for lost equipment:

• A bill will be generated to the individual/family for the replacement cost of the device or other equipment such as a charger or stylus.

Upon a student exiting the district, building Principals or Administrative Assistants will request the return of the district issued device along with any auxiliary equipment (charger, stylus, etc...). Equipment can be returned to the building or The District Technology Office.

If a student fails to return their district issued device upon termination of enrollment at PLATTSBURGH CITY SCHOOL DISTRICT, that student will be responsible for the replacement cost of the device and auxiliary equipment. This may delay the release of records.

7. ACCEPTABLE USE POLICY

4526

COMPUTER/INTERNET ACCEPTABLE USE
PLATTSBURGH CITY SCHOOL DISTRICT
POLICY

Educational Purpose

The Plattsburgh City School District recognizes that student instruction and learning will change as new technologies alter the ways in which information is accessed, communicated, and transferred. The district also recognizes that electronic information skills are now required as essential knowledge for critical thinkers, effective communicators, healthy and responsible citizens, and lifelong learners.

In responding to these changes, the Plattsburgh City School District actively supports student access to the widest variety of electronic information resources together with the development of appropriate skills to analyze and evaluate such resources.

All users of the district's computer network and the Internet must understand that use is a privilege, not a right, and that use entails responsibility. The district reserves the right to control access to the Internet for all users of its computers and network. The district will prohibit certain kinds of online activity, or access to specific websites.

All users of the district's computer network and equipment shall comply with this policy and regulation. Failure to comply may result in disciplinary proceedings and/or suspension/revocation of computer access privileges.

ACCEPTABLE USE

Users of district technology agree to abide by the following:

- Use of the district's computer network must be in support of education and research consistent with the district's mission and goals
- Each individual in whose name an access account is issued is responsible at all times for its proper use.
- All network users will be issued a login name and password. Passwords must be changed periodically.
- All network users are expected to abide by the generally accepted rules of network etiquette. This includes being polite and using only appropriate language. Abusive or sexual language or images, vulgarities and swear words are all inappropriate.
- Network users identifying a security problem on the district's network must notify the appropriate teacher, administrator or computer network coordinator. Under no circumstance should the user demonstrate the problem to anyone other than to the district official or employee being notified.
- Any network user identified as a security risk or having a history of violations of district computer use guidelines may be denied access to the district's network.

Prohibited Activity and Uses

The following is a list of prohibited activity concerning use of the district's computer network. Violation of any of these prohibitions may result in discipline or other appropriate penalties, including suspension or revocation of a user's access to the network.

- Using district computing resources for commercial or financial gain or fraud.
- Users will not reveal their personal information or that of others (i.e. complete names, addresses, telephone numbers).
- District network accounts are to be used only by the authorized owner of each account. Users shall not seek to learn, change or share other users' passwords, modify other users' files or data, or misrepresent other users on the network or Internet.
- Users shall not intentionally disrupt the use of the district's network or devices attached to the network.
- Using the network to send anonymous messages or files
- Steaking data, equipment or intellectual property
- Users agree that hardware or software shall not be destroyed, modified, damaged, or abused in any way.
- Malicious use of the district's network to develop programs or computer viruses that harass other users, infiltrate a computer or computer system, or damage the software settings/components of a computer or computing system is prohibited.
- Users are prohibited from loading, transmitting, or intentionally receiving threatening, harassing, obscene, sexually explicit or other antisocial content on the district's network.
- The use of the district's network to receive or transmit messages or material that is racist, sexist, abusive or harassing including pornographic material, inappropriate web sites or files, illegal software, or files dangerous to the integrity of the local area network or any attached device is prohibited.
- . Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting or making available any copyrighted software on the district computer network
- Students will follow copyright and fair use guidelines when using information from the Internet. These guidelines include proper citation when referring to downloaded text, images, and other media.
- Using the network while access privileges are suspended or revoked
- Using the network to receive, transmit or make available to others a message that is inconsistent with the district's Code of Conduct.

THE PLATTSBURGH CITY SCHOOL DISTRICT RESERVES THE RIGHT TO:

- monitor network, Internet, computer, and fileserver activity by ~~students~~ those on the district network;

- limit or remove an account on the district's network to prevent further unauthorized or unacceptable activity.
- The district reserves the right to access and view any material stored on district equipment or any material used in conjunction with the district's computer network.

Disciplinary action regarding violations of the student acceptable use policy will be determined at the building level consistent with existing practices. Violators risk losing computer privileges on a temporary or permanent basis, suffering disciplinary action and/or financial penalties, and facing possible prosecution for violation of local, state, and federal laws.

DISTRICT RESPONSIBILITY The district will allocate resources to promote, to the extent possible, a safe Internet experience for all students.

- The district will use protective technology measures to help prevent users from accessing inappropriate information on the Internet in accordance with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].
- The school staff will supervise, within reason, usage of the computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act.

With increased concern about identity theft, unwarranted invasion of privacy and the need to protect personally identifiable information, prior to students being directed by staff to use any cloud-based educational software/application, staff follow the Software Acquisition Process or check the Software Approval Portal list. The D.P.O will determine if a formal contract is required or if the terms of service are sufficient to address privacy and security requirements.

Cross-Ref: 5300, Code of Conduct

Adoption date: March 23, 2006
Last Revised: September 12, 2024
Last Reviewed: August 22, 2024

PCSD District Technology Office
49 Broad Street
518-957-6024 Technology Integration Office
518-957-6011 Technical Support

Administration:
Ms. Carrie Zales Assistant Superintendent of Curriculum
Mrs. Sue Wilson Business Manager and Data Protection Officer (DPO)
District Technology Integrationist:
Abby Leonard 518-957-6024 aleonard@plattscsd.org
IT Office (Technical Support):
Lucas Wisniewski 518-957-6011 lucas@plattscsd.org