Olean City School District Student Laptop, iPad, and MS Office 365 Account Guidelines and Procedures Summary

The laptop/iPad (referred to as "the device") is issued to you as an educational tool and should primarily be used in that capacity. The camera on the device may be enabled. The use of the camera is to be for educational purposes such as Teams or Zoom meetings with teachers. Any inappropriate use of the camera will result in the camera being disabled and disciplinary action. You may cover the camera lens (with tape or a sticky note) when not in use. Student use of the laptops/iPads falls under the guidelines of the District's Acceptable Use Policy for technology and the Student Code of Conduct Matrix. Access to the internet is monitored through our school's content filtering software and all rules and expectations are applied to the use of the device. Laptops may be selected at random for review. If it is found that the laptop has downloaded files or any executable files, or if the laptop is being used in an inappropriate manner the laptop will be returned to the Technology Department for removal of the files. USB ports are disabled on student laptops. The Student Code of Conduct Matrix will be used to determine the level of discipline. Your child will automatically be provided with a Microsoft Office 365 account, with a district email account (8-12 grade only) and Internet unless you submit written notification to the District that such access is not permitted. The notification must include the following: your child's name and student ID, building of enrollment, and be dated and signed by a parent/guardian. Please send the written notification to the building in which your child is enrolled. As a school district, which operates under the Family Educational Rights and Privacy Act (FERPA), the district is responsible for obtaining parental consent for the students' use of an Online Service for any student under 18 years of age. An annual AUP will be signed each school year. Students will be able to utilize the Microsoft Office 365 account while in school on the district laptop or on another device that has an Internet connection. Students will also be able to use some of the tools offline. Each student Microsoft Office 365 account that is created comes with the added benefit of five free licenses for Microsoft Office that can be downloaded and installed on any five devices the family owns.

Since this is a school owned device, users should have no expectation of privacy and the district may restrict or revoke privileges at any time. Activities that are never permitted include:

- Gaming, streaming, or media downloading
- Storage of personal photos or videos
- Installation of unauthorized software
- Accessing inappropriate or unfiltered content

Issued Equipment:

- Students will be given a Dell Latitude laptop, a slip-on case, and a power cord or iPad with case depending on what grade they are in.
- The camera may be enabled to allow for use in online classes and other educational purposes.
- The device must be returned to OCSD in appropriate working condition at the end of the school year or at the request of the Technology Office, Building Principal or District Superintendent.
- Students that leave the district or are suspended must return the district laptop by the date of withdrawal, suspension or termination.
- Continued use of a district device by students on out of school suspension will be determined by the building administrator and/or the district superintendent on a case by case basis.
- Failure to return district owned property prior to leaving the district may result in prosecution, civil liability, or paying the replacement cost of the laptop.

- Inappropriate background photos/ images, music, audio files or video may not be used or saved to the laptop.

Students will be responsible for:

- bringing the device to school every day.
- The device assigned to them
- keeping the device with you or in a secured (locked) area at all times.
- reporting the loss or theft of the device immediately.
- only using the camera, if enabled on the device, for educational purposes.
- remembering that the device is for educational purposes. Only district software will be installed on the device.
- following the OCSD Student Acceptable Use Guidelines at all times.
- being able to connect the device to their home wireless network, or public wi-fi network.
- being able to save files to their OneDrive account (cloud based).
- following the guidelines for Internet safety that you learned through the Internet Safety presentation.
- respecting the property rights and copyrights in data and computer programs and use the network for legal activities only. Questions regarding copyright should be directed to the building Library Media Specialist.
- leaving all screen settings, computer hardware, system software or district-prepared computer images as you found them.
- only using your personal password and access only your files unless you are granted permission by the account owner. Further, do not give out any personal information while online without a school employee's permission.
- only playing games, download or listen to music or view videos (for example: YouTube) on the computer network or the Internet when instructed to do so for educational reasons.
- Treating district equipment and resources with care and avoid intentional damage to any of the district equipment or network systems.

Acceptable Use of the Device:

All student use of district digital information systems must comply with district policies, standards, procedures, and regulations, as well as any applicable federal and state laws and regulations, including, but not limited to, copyright laws and licensing agreements. Acceptable student uses of the District's digital information systems include, but are not limited to:

- Protecting confidential information and student data, from unauthorized use or disclosure;
- Using digital information systems to support learning;
- Maintaining respectful conduct in their online communications and behavior;
- Reporting suspected cybersecurity incidents to appropriate district information technology personnel immediately; and
- Observing authorized levels of access and utilizing only approved digital information system devices and services.

In addition, students will ensure that their usage of the district digital information systems is aligned with the competencies of good digital citizenship. Students should be:

- Informed: evaluate the accuracy, perspective, and validity of digital media;

- Inclusive: open to hearing and recognizing multiple viewpoints and engaging others online with respect and empathy;
- Balanced: participate in a healthy variety of online activities and prioritize their time between virtual and physical activities;
- Engaged: use technology and digital channels to solve problems and be a force for good in their community; and
- Alert: aware of their digital actions and know how to be safe online.

Unacceptable Use:
The following list is not intended to be exhaustive but provides a framework for determining activities that constitute unacceptable use of district digital information systems. Unacceptable student uses of the district digital information systems include, but are not limited to:

- Attempt to modify/change/jailbreak or circumvent the device settings in any way. Doing so will result in the return of the device and disciplinary action as per the Student Code of Conduct Matrix.
- Download and/or attempt to install or run from a USB ANY executable software.
- Exchange devices with another student.
- Allow the device to be removed from their presence.
- Apply any permanent marks, decorations, or modifications to the device or the laptop case.
- Allow others to use the device assigned to them.
- Download any games on the device.
- Use slanderous, abusive, harassing or otherwise offensive images or messages.
- Use the network to view or send pornography and will report anything inappropriate to an adult.
- Participate in any spamming, pranks, threats, bullying, harassing, or other forms of unacceptable communication.
- Use network facilities for commercial or political use or for personal or private gain.
- Participate in chat rooms, instant messaging or other interactive recreational activities, not endorsed by the district, using the school's devices.
- Post or email inappropriate material on the Internet or through Outlook (district email services) that directly or indirectly affects the safety or welfare of students or staff.
- Distributing, transmitting, posting, or storing any electronic communications, materials, or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate;
- Engaging in unauthorized use or disclosure of personal, private, sensitive, and/or confidential information, including entering this information into generative artificial intelligence (AI) or other AI systems;
- Connecting unapproved devices to the district digital information systems;
- Installing, downloading, or running software that has not been approved in accordance with district policies;
- Using district digital information systems for commercial or personal purposes, including solicitation or advertisement, in support of religious, political, not-for-profit organizations, or for-profit business activities;
- Providing unauthorized third parties access to the district digital information systems;

- Tampering with, disengaging, or otherwise circumventing district-implemented IT security;
- Plagiarizing or engaging in copyright infringement; and
- Using district digital information systems to access personal social media platforms, email, or other personal account-based platforms.

Failure to comply with these guidelines will be treated as failure to comply with the District's Acceptable Use Guidelines and Student Code of Conduct Matrix and may be subject to disciplinary action.

Using the device:
Use of the device will require a few necessary tasks to keep the device performing well.

- Clean the screen often with only a soft, dry cloth.
- Keep food and drink away from the device.
- Charge the device nightly with the supplied charger, using a standard wall outlet for your power source.
- Document any software/ hardware issues to the Technology Department as soon as possible.
- Keep the device in a temperature controlled, dust free, smoke free environment.

Software Applications:

- There are key software applications which will be preinstalled on each device.
- Additional software applications may be installed by the IT Dept. to facilitate classroom instruction.
- Students may be asked to turn on the device when in school to install critical updates and then restart the device to have updates take effect. Failure to do so may cause some applications to not function properly.
- CIPA (Child Internet Protection Act) Compliant Internet Filtering and monitoring is available within our school network and installed on the device when it is connected to home wifi and public wifi networks. It remains the sole responsibility of the parents/guardians to monitor their student's use of the laptop and internet on their home wireless network.

Reporting Technical Issues & Damage:

- Any errors or problems with the device should be reported to the Technology Office.
- Any physical damage, intentional or not, to the device will be reported to the Technology Office immediately.
- Damage due to student negligence, such as leaving the device in a hot environment (*for example leaving it in a car during the summer) or using the laptop near water may result in the student/family assuming the financial responsibility of replacement of the laptop.
- The current replacement cost of a broken screen is: $180.00.
- A second incident of physical damage to a laptop may result in the loss of privilege to take a laptop home. This includes the loaner laptop.

*This list is not inclusive of what may be determined to be negligence on the user's part.