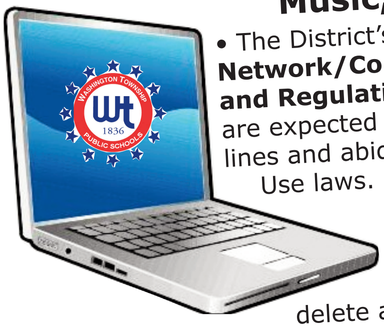
Washington Township School District
One-to-One Laptop Initiative

• Expectations of Digital Citizenship•

Student Responsibility in the One-to-One Initiative



Downloading Software

- All laptops will be distributed with pre-loaded software for coursework. Students may not download or install software or apps to their computers unless permission has been granted from the Information Technology Department. Any software or apps must be installed by members of the IT Department.

Loaning Equipment

- Students are not permitted to lend laptops or laptop components to others, including family members, for any reason.

- Parents/legal guardians may use the laptops to assist their child, who is assigned the laptop, with homework and school assignments.

File Management

- Laptops come with a standard pre-loaded image. This image may not be altered or changed in any way.

- Students are not permitted to remove or add any software/apps or change the computer settings, unless directed.

- Students are not permitted to change the computer name or to remove or change operating system extensions.

- The District does not accept responsibility for the loss of any data deleted due to re-imaging laptops or mechanical failure. It is the student's responsibility to regularly backup important files.

Music, Games or Programs

- The District's **Acceptable Use of Computer Network/Computers and Resources (Policy and Regulations #2361)** states that students are expected to comply with ethical-use guidelines and abide by all federal copyright and Fair Use laws.

Deleting Files

- Students are not permitted to delete any folders or files that they did not create or that they do not recognize. Deletion of files could interfere with the functionality of the laptop.

Storing/Saving Files

- Students should save their files in the cloud, using their District-provided OneDrive for Business Account.

Screensavers/Wallpapers

- Student laptops come equipped with standard screensavers and wallpapers. Students may modify or change their screensaver/wallpaper as long as it is appropriate and in compliance with Acceptable Use Policy #2361.

Passwords

- Students should login under their assigned usernames and passwords. It is recommended that students change their passwords within Office 365. Students should not share their passwords with other students and should log off of the computer and lock the screen when they are not at their laptop.

!

The District cannot guarantee that access to all inappropriate sites will be blocked. NO FILTER IS AS RELIABLE AS ADULT SUPERVISION. Students, as well as their parents/guardians, are not to TEST the laptop's capabilities regarding blocked sites by typing inappropriate sites into the computer, as web histories are logged. Should a student inadvertently access an inappropriate website, the site should be reported to a teacher, administrator and/or I.T. technician as soon as possible.

Student Email

- Student email accounts are provided by the school. Students must follow the requirement for email usage as set forth in Acceptable Use Policy #2361. Electronic communications coming from, and going to, the school-issued laptops can and will be monitored to make sure the terms of the agreement are being followed.

Digital Citizenship

- Digital communication etiquette is expected by all students using all school-provided communication accounts, sites or applications including, but not limited to, wikis, blogs, forums, interactive video conferencing, podcasts, online training, online courses, and online collaboration sites.

- As required by the Children's Internet Protection Act (CIPA), the District maintains an internet filter for use on the laptops. Students are required to notify a teacher or administrator if they access information or messages that are inappropriate, dangerous, threatening, or that make them feel uncomfortable.

- Students never should arrange to meet an unknown person utilizing social networks from the Internet.

- Students never should read someone else's email, or open their folders or files, without their permission.

- Students never should access or transmit anything with racist, abusive, threatening, demeaning, slanderous, objectionable, sexually explicit, or inflammatory content.

- Students should observe all copyright laws and should not claim authorship of work copied from a web site or from any other sources.

Off-Site Internet Use

- The District will not serve as a home Internet service provider. It is the responsibility of the parent/guardian to monitor student laptop use, especially Internet access, in the home.

Privacy

- There is no expectation of privacy regarding contents of computer files or communication using any school-owned computer or network. The District reserves the right to investigate, review, monitor, and restrict information stored on or transmitted via the District's equipment. Parents, guardians, and students do not have the right to or expectation of privacy for any use of school-owned laptops, computers, or other equipment.

- All laptops have a GPS tracking system. The GPS system will be used to help District staff and/or law enforcement should a laptop become lost or stolen. The District does not have remote access to the web camera installed on each computer when not connected to the District network.

- **Capturing video, audio, or photography without the consent of a classroom teacher is strictly forbidden.**

!

Internet Safety: Students are urged to keep their passwords secure and to protect their personal information. Students should not share their full name, address, phone numbers, password, or social security number.

Please note: All email, network, and Internet activity is the responsibility of the individual whose account is logged into the computer at the time of the activity.