# Wills Point Independent School District
# Student Guidelines for Responsible Use of Technology

The purpose of Wills Point Independent School District (WPISD) technology, network, internet access, and communication services are to support education and district administration. The student use of innovative classroom tools will be aligned with the WPISD curriculum and under the direct supervision of campus faculty. The use of WPISD technology is a privilege, not a guaranteed right, and inappropriate use will result in the cancellation of that privilege. Neither is it private. Technical staff has the ability and mandate to remotely observe, record and review the actions of all users. Findings of inappropriate use of technology shall be sent to campus administrators for disciplinary action. Each student will be instructed by a WPISD faculty member pertaining to its proper use. Based upon the acceptable use guidelines outlined in this document, district administrators will deem what is inappropriate use.

## Governances:

The provision of this policy and associated guidelines and agreements are subordinate to school, local, state, and federal law. WPISD has the duty to investigate any suspected violations of this policy.

***Technology use in Wills Point Independent School District is governed by federal laws including:***

**Child Protection Law Internet (CIPA)**

CIPA requires that the school has implemented measures and regulations to help protect students from harmful materials, even those that are obscene and pornographic. This means that the student email is filtered. The email containing harmful content and inappropriate sites will be blocked.

**Act Privacy Protection of Children Online (COPPA)**

COPPA applies to commercial companies and limits their ability to collect personal information from children under thirteen years of age. Google's advertising is turned off automatically for users of Apps for Education. We do not collect personal information from students for commercial purposes. This consent form allows the school to serve as an agent for parent in the collection for information within the school context. The school's use student information is solely for educational purposes only.

**Federal Educational Rights and Privacy Act (FERPA)**

FERPA protects the privacy of student education records and gives parents rights to examine their student's transcript. Under FERPA, schools may release directory information (name, phone, address, education level, etc ...) but parents can request that the school not disclose this information.

## Inappropriate use of technology includes but is not limited to the following:

1. Any illegal activities including transmission or use of material in violation of any U.S. or state law. This includes, but is not limited to copyrighted material, obscene material, or material protected by trade secret.
2. Intentional damage to or unauthorized tampering with any district computer systems, network infrastructure, peripheral technology or data.
3. The deliberate erasure, renaming, or altering of another user's data or application files.
4. Deliberately using technology to annoy, bully or harass others with language, images or recordings.
5. Deliberately exploring or accessing any violent, objectionable, risqué or obscene language, text or images.
6. Plagiarism and forgery of data in any form.
7. Causing congestion of network resources through excessive streaming, downloading, copying or transmitting files for the purpose of entertainment.
8. Authorizing others to use their name, login ID, or password.

9. Attempting to discover another user's login ID or password for any computer system, be it local to WPISD or through a remotely hosted service.
10. Commercial activities, including product advertisement.
11. Political lobbying.
12. Attempting to alter, destroy, or disable district technology resources including but not limited to computers and related equipment, district data, the data of others, or other networks connected to the district's system.
13. Use of the Internet or other electronic communications to threaten district students, employees, or volunteers.

### Google Apps for Education:

WPISD has created a Google Apps for Education account for each student in the district. Google Apps for Education accounts allow students to communicate and collaborate using a set of online tools such as Google Docs, Google Drive, Google Classroom, and other Google services that meet our students' educational needs. These online tools and services play an important tole in preparing students for our increasingly digital world.

Google Apps for Education is SSAE 16 / ISAE 3402 Type II SOC 2audited and have achieved ISO 27001 certification. Google complies with applicable US privacy law and FERPA (Family Educational Rights and Privacy Act) regulations. For more information, visit: https://www.google.com/edu/trust

### Education Record and Personal Information

By participating in Google Apps for Education, information about students will be collected and stored electronically. Under state and federal law, a student's education records are protected from disclosure to third parties unless the third party is providing a contracted service for the WPISD. Through a contract with the WPISD, Google Apps for Education provides students with storage and creation tools that are cloud based. The collected student information is used to create each WPISD Google Apps for Education account. The WPISD's use of student information is solely for educational purposes. Permission for students to access the Internet is deemed to be granted unless a parent or guardian gives a written letter to the campus principal denying said access. If parents have questions or concerns about how Google Apps for Education will be used, they are urged to call the campus.

### Students 13 or younger:

For students under the age of 13, the Children's Online Privacy Protection Act (COPPA) requires additional parental permission for educational software tools. Parents wishing to deny access to these educational tools and the Internet must do so in writing to the campus principal indicating their child should be denied access to these tools. Examples of these tools are Discovery Education, Google Apps, wikis, and blogs.

## The following policies are to be followed by all WPISD student computer users:

1. Data Storage

All data files must be saved to the user's Google Drive are considered to be secure. Files stored on a workstation only should be considered at risk and will be unrecoverable in the event of system failure.

2. Student Email

The District will provide a student email account through the Wills Point ISD Google Apps for Education. Only High School students will have the ability to email outside the District.

Inappropriate use of email includes but is not limited to the following:

a. Writing an electronic message masquerading as another user.

b. Sending, posting, or possessing electronic messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal, including cyber bullying and "sexting," either on or off school property.

c. Using e-mail or Web sites to engage in or encourage illegal behavior or threaten school safety.

3. User IDs and Passwords

a. Users shall change account passwords according to all published schedules.

b. Users may not leave computers unattended while they are logged in to an active account.

4. Rights to Intellectual Property

Rights to intellectual property such as written material, photographs and artwork, created with technology provided by Wills Point ISD are not the exclusive concession of the student who created them. The right to use such properties will be shared by both the student and the district.

5. Malware Protection

a. It is the responsibility of each user to be aware of and follow all measures aimed at preventing the introduction or propagation of malware in our computer systems. Personal devices should have up to-date anti-virus protection.

b. Users shall not intentionally write, produce, copy, propagate, or attempt to introduce any computer code or command designed to self-replicate, damage, or otherwise hinder the performance of any computer system, software application or network appliance.

c. All external files must be scanned for viruses prior to use in any district computer system. External files include all files coming to district computers via removable media, email or internet download.

6. Personal Technology & BYOD

Student use of personal technology devices are for educational purposes when the teacher deems appropriate. Use of personal technology devices during the school day is a privilege. Students and parents/guardians participating in BYOD agree to the following conditions:

- Under no circumstance will Wills Point ISD accept responsibility for loss or damage to personal technology devices used within the district or during participation in school activities.
- The student takes full responsibility for his or her personal technology device.
- The student complies with teachers' request to shut down the computer or close the screen.
- If a student does not comply with a teacher's request to power down the device, the device can be confiscated and turned into the office. Parents can pick up the device from the office according to student code of conduct.
- The technology must be in silent mode while on school campuses and while riding school buses.
- The technology may not be used to cheat on assignments or tests.
- Student accesses to technology during class time should generally be limited to files, applications and internet sites which are relevant to the classroom curriculum. Exceptions to this guideline are at the discretion of the classroom teacher only.
- The student acknowledges that the school's network filters will be applied to the district's Wi-Fi network and will not attempt to bypass them.
- The student understands that bringing on premises or infecting the network with a Virus, Trojan, or program designed to damage, alter, destroy, or provide access to unauthorized data or information is in violation of the AUP policy and will result in disciplinary actions.
- The student realizes that processing or accessing information on school property related to "hacking", altering, or bypassing network security policies is in violation of the AUP policy and will result in disciplinary actions and possible monetary fines.
- The school district has the right to collect and examine any device that is suspected of inappropriate activity, causing problems or was the source of an attack or virus infection.
- The student realizes that printing from personal technology devices will not be possible at school.

7. Software Licenses for WPISD devices

a. Users may not install, change, or remove any software provided by WPISD without permission from the WPISD technology department. Non-approved software will be removed from district computer systems immediately and without prior notification of the user.

b. Users may not illegally copy software provided by WPISD or any other source. The use of illegally copied software is considered a criminal offense and is subject to criminal prosecution.

8. Web Presence

Publishing student work online promotes learning and collaboration and provides an opportunity to share the achievement of students. This work may be posted provided:

a. No objectionable, defamatory, risqué or obscene language, text or images are used.

b. Any picture containing an image of one or more students is presented in such a way as to maximize the anonymity of those students. The links are to other educational websites, and not to personal sites or sites of personal interest.

## Consequences

Violation of WPISD's policies and procedures concerning the acceptable use of technology will result in the same disciplinary actions that would result from similar violations under the Student Code of Conduct. Any or all of the following consequences may be employed:

1. Immediate removal of relevant data, files and/or communications.
2. Loss of computer privileges/Internet access, with length of time to be determined by the administration.
3. Liability for cost to trace, diagnose or repair the cause and results of any violation. This expense will be charged at a rate of $50.00 per hour plus material and contracted costs.
4. Any campus-based disciplinary consequences, including suspension and the placement in the Wills Point ISD DAEP as deemed appropriate by the administration.
5. Expulsion may be considered in flagrant violations that blatantly corrupt the educational value of computers or the Internet, in instances when students have used WPISD technology to violate the law or instances when students have used WPISD technology to compromise another computer network.
6. Referral to enforcement authorities for prosecution under the law.

*All the above policies and procedures for acceptable use of computers and networks are intended to make the computers and networks more reliable and consistent for the users who depend upon them daily. They are also intended to minimize the burden of administering the networks, so that more time can be spent enhancing services. If there is any doubt concerning the acceptable use of computers and networks contact the WPISD Director of Technology at 903-873-5100. If there are genuine needs that cannot be met by following these rules, please let a WPISD administrator know.*