Student Responsible Use Guidelines for Technology
Pflugerville Independent School District

Vision

In the Pflugerville Independent School District, technology is an integral part of the teaching and learning process. It is a tool to enhance the delivery of curricula, increase teacher and student productivity and efficiency, promote creative expression, increase communication and access to information. Our vision is to transform the use of technology to an integrated role that supports appropriate teaching strategies and makes instruction more relevant to students at all levels. The infusion of appropriate technologies into the instructional program will help ensure that students are prepared to be skillful and productive users of information in the future.

Mission

Our mission is to ensure the use of appropriate technologies to develop digital skills, process and present information, enhance the delivery of curricula, meet the academic needs of a diverse student population, and promote optimal growth and learning through critical thinking and problem solving.

Philosophy

Technology encompasses tools that encourage students to think creatively, communicate effectively, solve problems wisely, and manage information skillfully. Technology in this context includes computers, mobile devices, data and video systems designed and networked, when feasible, to enhance communication and instruction. In order to accomplish this goal, the Pflugerville Independent School District has made technology a priority. It is our belief that technology is more than just hardware. It can transform the District's culture by providing a way to explore possibilities and opportunities while developing a 21st century learner.

These technologies, when properly used, promote educational excellence in the District by facilitating resource sharing, innovation, and communication. Illegal, unethical or inappropriate use of these technologies can have dramatic consequences, harming the District, its students and its staff. These Responsible Use Guidelines are intended to minimize the likelihood of such harm by educating District students and their parent(s) or adult guardians and setting standards, which will serve to protect the District and promote technology integration.

Compliance Education

To educate District students on proper technology use and conduct, users are required to review these guidelines at the beginning of each school year. The parent(s) or legal guardian of a student user is required to acknowledge receipt and understanding of the District's Student Responsible Use Guidelines for Technology (hereinafter referred to as the RUG) as part of their review of the District's Discipline Management Plan, Student Code of Conduct and Student Handbook. District instructional staff supervising students who use the District's system will also provide ongoing education for proper technology use and conduct annual reviews of the Student RUG and CyberSafety and CyberBullying lessons.

Definition of District Technology System

The District's computer systems and networks (system) are any configuration of hardware and software. These systems include but are not limited to the following:

- District-provided Internet access via hardwired computers or wireless access
- District provided hardware including but not limited to phones, chromebook, and laptops
- Email accounts
- District approved software including operating system software, application software and Online Subscription Resources
- District Data and Information stored internally or externally via servers, databases, and applications
- New technologies as they become available and as defined by local administrative regulation.

Availability of Access

Computer/Mobile Devices/Network/Internet access will be used to enhance, engage and extend student learning consistent with the District's Mission and Goals. Computer/Mobile Device/Network/Internet access is provided to all students unless parents or guardians request in writing that access be denied.(Opt Out through Student Handbook form). Student Internet access will be under the direction and guidance of a District staff member.

Each District computer, mobile devices and Guest Wi-Fi (available for students who bring their own personal technological devices) has Filtered Internet access provided to students as defined by the federal Children's Internet Protection Act (CIPA) Filtering software, as defined by CIPA), blocks access to visual depictions that are obscene, pornographic, inappropriate for students and/or harmful to minors.

A student who gains access to any inappropriate or harmful material is expected to report the incident to the supervising District staff member.

A student who knowingly violates any portion of the Responsible Use Guidelines (RUG) will be subject to suspension of access and/or revocation of privileges on the District's Computer/Network/Internet systems and will be subject to disciplinary action in accordance with the Board-approved *Discipline Management Plan and Student Code of Conduct*.

Use of Personal Technological Devices (BYOD/BYOT)

The District believes technology is a powerful tool that enhances learning and enables students to access a vast amount of academic resources. The District's goal is to increase student access to digital tools and facilitate immediate access to technology-based information, much the way that students utilize pen and paper. To this end, the District will open a filtered, wireless network through which students in specific age groups will be able to connect privately owned (personal) technological devices. Students using personal technological devices must follow the guidelines stated in this document while on school property, attending any school-sponsored activity, or while using the Pflugerville ISD network.

BYOD

Limited use of personal devices on campus will be allowed only if authorized by campus administrators.

Students are allowed to bring personal technological devices that can access the Internet **INTO THE CLASSROOM** for educational purposes **ONLY** as determined by the classroom teacher through campus guidelines and expectations. Students will be allowed to use the device for personal use between classes and in the cafeteria setting in a digitally responsible manner.

The following guidelines must be adhered to by students using a personally-owned technological device on campus:

Personal Device Internet Access. Internet access is filtered by the District on personal technological devices in the same manner as District-owned equipment. If Internet access is needed, connection to the filtered Internet through the wireless network provided by the District is required. Students must connect to a District Wireless Access Point. Students may not be connected to the Internet provided by a device carrier's Data Plan.

Personal Student Technological Devices. Student devices are the sole responsibility of the student and the parent(s) / adult guardian owner. The campus, campus personnel and the District assumes no responsibility for personal technological devices if they are lost, loaned, damaged or stolen.

Student Device Setup, Maintenance, Storage and Security. Each student and their parent(s) / adult guardian owner is responsible for his/her own technological device, including the: set-up, maintenance, charging, storage and security.

Students who do not have access to personal technological devices will be provided with comparable District-owned equipment or given similar assignments that do not require access to electronic devices.

Technological devices are only to be used for educational purposes at the direction of a classroom teacher or as stated for specific age groups.

Campus administrators and staff members have the right to prohibit use of devices at certain times or during designated activities e.g., campus presentations, theatrical performances, guest speakers, campus based assessment, District based assessment, State mandated assessments) that occur during the school day.

Third-Party Supplied Information

Students and parents of students with access to the District's system should be aware that use of the system may provide access to other electronic communication systems in the global electronic network that may contain inaccurate and/or objectionable material.

A student who knowingly brings prohibited materials into the school's electronic environment or is identified as a security risk will be subject to loss of access and privileges on the District's Computer/Network/Internet and will be subject to disciplinary action in accordance with the Discipline Management Plan and Student Code of Conduct. Other consequences may also be imposed.

Monitoring

All District technology usage shall not be considered confidential and is subject to monitoring by any designated District staff member at any time to ensure appropriate use. Students should not use the computer/network/Internet systems to send, receive or store any information, including email messages, that they consider personal or confidential and wish to keep private. All electronic files, including email or instant messages, transmitted through or stored in the computer system shall be treated no differently than any other electronic file. The District reserves the right to access, review, copy, modify, delete or disclose such files for any purpose. Students should treat the computer/network/Internet systems like a shared or common file system with the expectation that electronic files, sent, received or stored anywhere in the computer/network/Internet systems, will be available for review by any authorized representative of the District for any purpose. Personal technological devices connected to the district network/wireless access point/Internet are subject to examination in accordance with the Discipline Management Plan and the Student Code of Conduct.

Student Technology Usage Responsibilities

1. All Students are responsible for their own actions in accessing all District available resources.
2. Students are required to bring their district issued device to campus or virtual learning each day. The device must be fully charged and ready for instruction.
3. Student issued district devices that are damaged, lost, stolen or in any way not available for the instructional day must report these issues immediately to their campus administrator.
4. All students are bound by all portions of the District's Student Responsible Use Guidelines.
5. Students who knowingly violate any portion of the Student Responsible Use Guidelines will be subject to disciplinary action in accordance with District policies stated in the **Student Code of Conduct and Discipline Management Plan.**

Campus Level Responsibilities - **The principal or designee shall:**

1. Be responsible for disseminating and enforcing the District's Staff and Student Responsible Use Guidelines at the campus or departmental level.
2. Ensure that all staff and student users of the District's system complete and sign the agreement in the HR Compliance course to abide by District policies and administrative regulations regarding such use.
3. Ensure that campus staff, including EDP and Clubs or other programs that meet outside the school day, who supervise students who use the District's systems provide information emphasizing its appropriate, safe, and ethical use.
4. Ensure all users of the District's systems follow stated appropriate and ethical use.
5. Use the District's student management system to identify students who do not have permission to use the Internet and inform staff who are responsible for these students that they do not have permission to use the Internet, student email or Websites that provide 21st century collaboration and communication tools.
6. Students under the age of 13 may not use internet resources that prohibit use by students under the age of 13. This includes access via a teacher's account.
7. Provide training to staff that supervise students on digital responsibility, digital citizenship and appropriate use of technology resources.

Teacher Responsibilities - The teacher shall:

1. Deliver District prepared CIPA/COPA age-appropriate compliance lessons in Internet Safety, Digital Responsibility, Cyber Safety and Cyberbullying for all students during the 1st week of school, weekly during the month of October and monthly follow ups throughout the school year.
2. Review District technology usage responsibilities with students prior to gaining access to such systems. (Use the Condensed Rules For Students found in the PfISD Student RUG)
3. Verify the list of students whose parents have denied consent to access the Internet, email, and Educational digital content. (Opt-out box on student registration form)
4. Provide developmentally appropriate guidance to students as they use digital collaboration and communication tools to acquire 21st century skills and apply them to the learning goals and objectives.
5. Use technology resources in support of instructional goals and objectives.
6. Provide alternate activities for students who do not have access to electronic resources.
7. Address student violations of the District's Student Responsible Use Guidelines as defined in the Discipline Management Plan and Student Code of Conduct.

Pflugerville ISD Student Code of Conduct

Pflugerville ISD Students are expected to maintain appropriate conduct when accessing the communications and information technologies available through district technology systems access. All students must comply with the District's Student Responsible Use Guidelines at all times when accessing any part of the technology systems.

1. Students are required to maintain password confidentiality by not sharing their password with others. Students **may not** use a staff member or student's system account. Passwords must be guarded. They are the primary way in which student members are authenticated and allowed to use assigned District's computing resources. Supervising District staff members have access to student passwords to assist them in using the District Computer/Network/Internet. MS and HS students will reset/change their passwords from the assigned default under the direction of the supervising staff member.
2. Students will only access the District network resources using their User ID and Password. Other logins may allow students to gain access to resources to which they would otherwise be denied.
3. Students must not utilize any hardware or software in an attempt to compromise the security of any other system, whether internal or external to the District's systems and network. Examples of prohibited activities include (but are not limited to) Trojan horses, password crackers, port security probes, network snoopers, personal routers (wired or wireless), IP spoofing, and intentional transmission of viruses or worms.

Technology usage is subject to monitoring by designated staff at any time to ensure appropriate use. Electronic files sent, received or stored anywhere in the computer system are available for review by any authorized representative of the District for any purpose. Parents and Guardians that acknowledge the Student Code of Conduct and the Student Handbook affirm that at all times their student's actions while using the District's system will not violate the law or the rules of network etiquette, will conform to the guidelines set forth in the Student Responsible Use Guidelines, and will not violate or hamper the integrity or security of the District's technology system.

If a violation of the Student Responsible Use Guidelines occurs, a student may be subject to one or more of the following actions:

1. Revocation of access;
2. Disciplinary action in accordance with the Student Code of Conduct and the Discipline Management Plan

Use of Social Networking/Digital Tools

Students may participate in District recommended Internet based learning environments related to curricular projects or school activities. The use of blogs, wikis, podcasts, and other digital tools are considered an extension of the student's classroom environment. Verbal or written language that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, wikis, podcasts, and other District approved digital tools.

Use of System Resources

Students are asked to purge email or outdated files on a regular basis. Student email shall not be retained and will be removed 30 days from a student's graduation date or departure from the District.

Reporting Security Problem

If knowledge of inappropriate material or a security problem on the computer/network/Internet is identified, the student should immediately notify the supervising District staff member. The security problem should not be shared with others.

Inappropriate Use

Inappropriate use includes, but is not limited to, those uses that violate the law, that are specifically named as violations in this document, that violate the rules of network etiquette, or that hamper the integrity or security of this network system or any components that are connected to it. The following actions are considered inappropriate uses and are prohibited.

-Violations of Law

Transmission of any material in violation of any federal or state law is prohibited. This includes, but is not limited to:

1. threatening, harassing, defamatory or obscene material;
2. copyrighted material;
3. plagiarized material;
4. material protected by trade secret; or
5. blog posts, Web posts, or discussion forums/replies posted to the Internet which violate federal or state law.

Tampering with or theft of components from District systems may be regarded as criminal activity under applicable state and federal laws.

Any attempt to break the law through the use of a District computer/network/Internet account may result in prosecution against the offender by the proper authorities. If such an event should occur, the District will fully comply with the authorities to provide any information necessary for the litigation process.

- Modification of Computer

Modifying or changing computer settings and/or internal or external configurations without appropriate permission is prohibited.

- Transmitting Confidential Information

Students may not redistribute or forward confidential information (i.e. email address, phone number, home address, birthdate, student ID, parent's phone, etc.). Confidential information should never be transmitted, redistributed or forwarded to outside individuals who are not expressly authorized to receive the information. Revealing personal information about oneself such as, but not limited to, home addresses, phone numbers, email addresses, birthdates of others is prohibited.

-Commercial Use

Use of the District systems for any type of income-generating activity is prohibited. Advertising the sale of products, whether commercial or personal, is prohibited.

-Marketing by Non-PflSD Organizations

Use of the District systems for promoting activities or events for individuals or organizations not directly affiliated with or sanctioned by the District is prohibited.

-Vandalism / System Interference / Unauthorized Access

Any malicious attempt to harm or destroy District equipment and other networks to which the District has access; or the deleting, examining, copying, or modifying files and/or data belonging to other users, without their permission is prohibited.

Deliberate attempts to degrade or disrupt system performance are violations of District Student Code of Conduct and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses, attempts to exceed, evade or change resource quotas and causing network congestion through mass consumption of system resources.

Unauthorized access or attempted access of any portion of the District's computer systems, networks, or private databases to view, obtain, manipulate, or transmit information, programs, or codes is prohibited and will result in revocation of the student's access to computer/network/Internet.

Violations as defined above are prohibited and will result in the cancellation of system use privileges. Students committing defined violations will be required to provide restitution for costs associated with system restoration and may be subject to other appropriate consequences as defined by the **Student Code of Conduct and Discipline Policies.**

-Copyright
Students may not engage in the unauthorized copying, distributing, altering or translating of copyrighted materials, software, music or other media without the express permissions of the copyright holder.

Downloading or using copyrighted information without following approved District procedures is prohibited.

An original work created by a student that will be published on the Internet will require written parental consent.

Electronic Communication and Collaboration Tools / Email Retention

District email and other digital tools such as, but not limited to Google Apps for Education, SeeSaw and Canvas are tools used to support and extend classroom communication and learning. Student use of these communication tools should be limited to instructional, school-related activities. Internet access to personal email accounts and personal social media sites are not allowed.

Electronic communication and collaboration tools are important resources for acquiring 21st Century skills. By providing these tools, the District is equipping a student with the skills necessary for success. Parents wishing to deny access to District electronic communication and collaboration learning tools must return the Opt Out form located in the Student Handbook. Parents may also deny Internet access. Parents must submit this request in writing to the campus administrator. (Policy CQ)

Google Apps for Education - Student & Parent Notification

Pflugerville ISD believes that electronic communication and collaboration enables 21st Century learning, promotes positive digital citizens and equips students with skills necessary for success now and in the future. In August 2013, Pflugerville ISD established a Google Apps for Education tool set for all students. The Google Apps for Education tool set includes Drive (Docs, Presentation, Forms, Spreadsheet, and Drawing), Calendar, and Gmail.

1. A Google Apps for Education student account will be created for all students.
2. All students will receive access to Google Drive (online documents), Calendar and Gamil account (student email).
3. The District provides the opportunity for parent(s)/guardian(s) to restrict Google Apps access.

If you do not want your student to have access to Google Apps while at school, please submit a written request to your child's campus administration.

Students should keep the following points in mind:

-Perceived Representation. Using school-related email addresses, Google docs, Edmodo, and other communication tools might cause some recipients or other readers of the email to assume that the student's comments represent the District or school, whether or not that was the student's intention.

-Privacy. Email, Google Docs, Edmodo and other communication within these tools should not be considered a private, personal form of communication. Private information, such as home addresses, phone numbers, last names, pictures, or email addresses, should not be divulged. To avoid disclosing email addresses that are protected, all email communications to multiple recipients should be sent using the blind carbon copy (bcc) feature.

-Inappropriate Language. Using obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language in emails, Google Docs, Edmodo, blogs, wikis, or other communication tools is prohibited. Sending messages that could cause danger or disruption, personal attacks, including prejudicial or discriminatory attacks is prohibited.

-Email Retention. Student email shall not be retained and will be removed 30 days from a student's graduation date or departure from the District.

-Political Lobbying. Consistent with State ethics laws, District resources and equipment, including, but not limited to, emails, blogs, wikis, or other communication tools may not be used to conduct any political activities, including political advertising or lobbying. This includes using District email, Google Docs, Edmodo, blogs, wikis,

or other communication tools to create, distribute, forward, or reply to messages, from either internal or external sources, which expressly or implicitly support or oppose a candidate for nomination or election to either a public office or an office of a political party or support or oppose an officeholder, a political party, or a measure (a ballot proposition). These guidelines prohibit direct communications as well as the transmission or forwarding of emails, hyperlinks, or other external references within emails, blogs, or wikis regarding any political advertising.

-Forgery. Forgery or attempted forgery of email messages is prohibited. Attempts to read, delete, copy or modify the email of other system users, deliberate interference with the ability of other system users to send/receive email, or the use of another person's user ID and/or password is prohibited.

-Unsolicited Messages. Students shall refrain from forwarding emails which do not relate to the educational purposes of the District. Email intended for forwarding or distributing to others is prohibited. Creating, distributing or forwarding any annoying or unnecessary message (SPAM) to a large number of people is prohibited.

RUG Agreement Violations

Denial, Revocation, or Suspension of Access Privileges. Any attempt to violate the provisions of this agreement may result in revocation of the student's access to the computer/network/Internet, regardless of the success or failure of the attempt. In addition, school disciplinary action in accordance with the Discipline Management Plan and Student Code of Conduct and/or appropriate legal action may be taken. With just cause, the System Administrator and Campus administrator may deny, revoke, or suspend computer/network/Internet access contingent upon the results of an investigation.

Systems User Warning. Sites accessible via the computer/network/Internet may contain material that is illegal, defamatory, inaccurate or controversial. Each District computer with Internet access has filtering software that blocks access to sites that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act. The District makes every effort to limit access to objectionable material; however, controlling all such materials on the computer/network/Internet is impossible, even with filtering in place. With global access to computers and people, a risk exists that students may access material that may not be of educational value in the school setting.

Disclaimer

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not guarantee that the functions or services performed by, or that the information or software contained on the system will meet the staff member's requirements, or that the system will be uninterrupted or error free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not the District. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communication systems.

Student Responsible Use Guidelines

Condensed Rules for Students

In the Pflugerville Independent School District, technology is an integral part of the teaching and learning process. Pflugerville ISD will provide students with the opportunity to use District and Personal electronic devices for educational purposes only. Pflugerville ISD accepts no responsibility for lost, stolen, or damaged personal devices, or the maintenance or installation of applications or software on personal devices. Students must comply with the Pflugerville ISD Student Responsible Use Guidelines (RUG) at all times. The complete RUG is available on the Student Tab of the PfISD website and in the student handbook. The Condensed Rules for Students version is not a substitute document for the complete Student RUG. Students are accountable for all provisions in the complete PfISD Student RUG.

Students will:

- Connect to the assigned PFISD network while on campus.
- Students are required to bring their district issued device to campus or virtual learning each day. The device must be fully charged and ready for instruction.
- Student issued district devices that are damaged, lost, stolen or in any way not available for the instructional day must report these issues immediately to their campus administrator.

Responsible Use

- Use of technological devices and the internet appropriately is an expectation of PfISD. Understand that breaking the rules may mean that you lose the privilege to use the computers or internet at school, including personal technological devices.
- District technological devices must be connected to the District internet/network and will be used for educational purposes only.
- Personal technological devices must be connected to the assigned District wireless internet and will be used for educational purposes only.
- Never DELETE or damage another person's work on the District Share drive or Google Drive.
- Students will **ONLY** use their **own** Username and Password to login to the computer or other device.
- Students must report to the teacher/parent/guardian if they believe someone has used their username/password.
- Use appropriate and polite language online on campus and during virtual learning.
- Handling other students' devices is not allowed unless directed by the teacher.
- Students must include a citation when using text, images, audio, and video retrieved from the internet.
- Students will not forge, send, post, or possess materials that are inappropriate, illegal, obscene, pornographic, violent, threatening, abusive, harassing, or damaging to another's reputation (cyber bullying), while using the device, no matter the location.
- Students will not play **Games, Stream Music, or view Recorded Video Programs** on their district provided student device at school or in Virtual Learning unless it supports curriculum learning objectives and / or other educational purposes.
- Participating in internet auctions is prohibited at all times on any District device.

Internet Safety

- NEVER reveal any personal information on the internet – including last name, address, phone number, school address, password, birthdate, or any other information about yourself or your parents.
- NEVER meet anyone you have talked to while working on the internet at school or at home.

Staff and Student District Device Care

- Damage, removal or relocation of mobile devices, cables, mice, headphones or power bricks from a mobile cart is prohibited.
- Damage, removal or relocation of computers, mice, monitors, keyboards, cables or headphones from Computer Labs or Classrooms is prohibited.
- Students will report missing or damaged equipment to Campus Staff members.
- Campus Staff will enter a Technology ticket for District equipment that is missing or requires repair.
- Headphones are not District Technology equipment. Replacement is the campus responsibility or the individual students
- Sharing of earbuds or headphones is prohibited.
- District provided devices MUST be fully charged, on campus or in virtual learning each school day.