STAFF
RESPONSIBLE USE POLICY

AISD is invested in using technology to support professionalism for AISD staff, enhance student learning, and improve learning outcomes. Using your device, the AISD network and systems is a privilege and any privilege comes with responsibility. Signing this Responsible Use Policy (RUP) will serve as an acknowledgment of this information for Austin ISD staff and contracted staff.

What is the purpose of the district's Responsible Use Policy (RUP)?

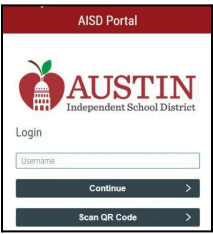The purpose of this responsible use policy for Austin ISD is to set:

- set clear expectations
- create conditions for effective and professional use of AISD systems, equipment, and tools for all AISD staff
- provide accountability for staff interactions with technology and AISD systems

STAFF
RESPONSIBLE USE POLICY

AUSTIN | Information Technology
Independent School District
Simple. Standard. Secure.

The following are expectations for Austin ISD staff when using AISD accounts and district systems.

As a representative of Austin ISD, I will:

BE RESPONSIBLE FOR MY AISD/GOOGLE ACCOUNT:

☐ I will keep my username and password secure.

☐ I will not share my password or security codes (multi-factor authentication) with other users internally or externally under any circumstances. This includes sharing a password with other district staff, substitutes, or students.

☐ I will be mindful of mixing personal and professional accounts. I will only use my Austin ISD account to access digital tools that have been vetted and approved for district use.

☐ I will use professional language in all work-related communications including email, social media posts, audio recordings, conferencing, and artistic works.

☐ I will treat others' digital content and digital spaces with respect.

☐ I will respect the content of others and not read, edit, share, download, or delete files without permission.

☐ I will do my best to recognize and report when someone attempts to unlawfully gain access to my Austin ISD account (through email phishing, etc.).

☐ I will forward any suspicious emails to junkmail@austinisd.org.

BE RESPONSIBLE FOR MY INTERNET USE:

☐ I will model and actively practice positive digital citizenship.

☐ I will be considerate of what I post online, and I will not disrupt school activities or compromise school safety and security.

☐ I will treat others with respect and dignity.

☐ I will not seek out, display, or circulate material that contains hate speech, sexually explicit, or violent content while at school or while identified as a district employee.

☐ I will be respectful of the district resources I have access to. Use of the district network for illegal, political, or commercial purpose is prohibited.

☐ I will be mindful of the files I send and share. I will not transmit large files that are unrelated to district business and disruptive to the district network.

☐ I will seek appropriate permission before transmitting a broadcast (email, instant message, announcement, etc.) to official or private distribution lists, regardless of content or recipients.

☐ I will practice honesty and integrity with my access to district resources. Forgery or attempted forgery of email, messages, or other electronic material is prohibited.

☐ I will respect the content of others and not read, modify, share, forward, download, or delete their emails without permission.

BE RESPONSIBLE FOR AISD DEVICES AND EQUIPMENT:

☐ I will take all reasonable precautions to protect district equipment from damage, theft, or loss.

☐ I will be mindful of equipment use agreements.

☐ I will only take assigned and approved devices and hardware off AISD property.

☐ I will engage in best practices with downloads on my AISD-issued device(s). I will use caution when downloading files or opening emails, as attachments or unverified downloads could contain viruses or malware.

☐ I will be a partner in protecting district resources. I will report vandalism in any form to the appropriate administrator and/or technical personnel.

☐ If I see something, I will say something. I will report system weaknesses or security events related to any protected district data or information systems housing protected data to the IT Security Office by submitting an AISD Help ticket.

STAFF
RESPONSIBLE USE POLICY

BE RESPONSIBLE FOR SAFETY AND CYBERSECURITY:

☐ I will be a protective agent of data. I will keep safe all personally identifiable information (PII) about students and employees. I understand PII includes, but is not limited to: names, home addresses, birth dates, telephone numbers, student ID numbers, employee numbers, educational records, and images.

☐ I will only use district-maintained email accounts to transmit PII from students' education records to other district email accounts of district employees who have a legitimate educational or business interest in the information.

☐ I understand that the transmission of student information to external parties by district email is strictly prohibited as is the forwarding of such district emails to non-district email providers (e.g. Gmail, Yahoo, etc.).

☐ I will refrain from forwarding messages from my district email account to any non-district account(s).

☐ I will maintain the confidentiality of health or personnel information concerning district employees and colleagues unless disclosure serves lawful professional purposes.

☐ If PII must be shared via a file-sharing or collaboration service, such as Google Drive, I will only use a service that the district has provided me an account for and has deemed appropriate for sharing such information.

☐ I will become aware of privacy settings on websites that I visit.

☐ I will abide by all laws, this Responsible Use Policy, and all district security policies, including the district's record management program, the Texas Open Meetings Act, the Public Information Act, the Family Educational Rights and Privacy Act (FERPA), and AISD security and privacy standards.

☐ I will report all cases of bullying to my site administrator or other authority. Bullying in any form, including cyberbullying, is unacceptable both in and out of school.

☐ Authorized employees who are not at their assigned workplace must ensure that all protected paper documents, as well as data storage media with protected data, must be removed from the desk or other places (e.g. printers, photocopiers) to prevent unauthorized access.

☐ Authorized employees who are not at their assigned workplace must ensure that all protected information is removed from their computer screen and access must be denied to all systems for which the employee is authorized to use by logging off the district network, locking the screen with a password, or turning off the computer.

Please see this resource on the last page with terms related to cybersecurity.
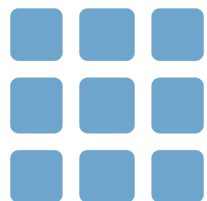
BE RESPONSIBLE WITH MY USE OF DIGITAL TOOLS:

☐ I will stay up to date in regards to which digital tools, software, and equipment have been approved and vetted by Austin ISD.

☐ I will abide by software licensing terms and cease using software when licenses expire.

☐ I understand that I will not share student data or information with digital tools/programs not approved by the district.

☐ I will endeavor to create digital content that is inclusive and can be accessed by learners of various languages, abilities and needs.

☐ I will teach students about positive digital citizenship, including responsible and ethical use of Generative Artificial Intelligence (AI) applications and tools (where applicable and age-appropriate). This should align with Technology TEKS and the student RUP. All users are responsible for respecting and maintaining the security of district electronic resources and networks.

☐ I will not use the district network or equipment to obtain unauthorized information, attempt to access information protected by privacy laws, or impersonate other users.

	☐ I will respect the district security settings and filters. I will not make attempts to bypass these filters, including through the use of proxy servers or VPN services, on any district-issued device, or while on district property.
	☐ I will not install or use illegal software or files, including unauthorized software or apps, on any district computers, tablets, smartphones, or new technologies.
	☐ I know that remote access to the district network must be authorized in writing by the district, and may take the form of district-provided Virtual Private Network (VPN) Services.
	☐ I am aware that improper use of the district's technology resources, including creating and distributing chain letters, sending spam, setting up equipment so that it can act as an "open relay" for third-party spammers, providing products or services for pay, or installing a non-approved Virtual Private Network (VPN) services, is prohibited.
	☐ I will only access information meant for my viewing. I will not attempt to gain unauthorized access to restricted information or resources.

	☐ I know that while there are copyright fair use exemptions (https://www.copyright.gov/fair-use/), all users must:
	  ☐ respect intellectual property.
	  ☐ follow all copyright guidelines (https://www.copyright.gov/title17/) when using the work of others.
	  ☐ not download illegally obtained music, software, apps, and other works.

BE RESPONSIBLE WITH THE USE OF ARTIFICIAL INTELLIGENCE (AI) TECHNOLOGY

☐ I will ensure that any AI systems used are age-appropriate and that do not violate the privacy of other individuals.

☐ I will ensure that AI systems do NOT share any personally identifiable information (PII) or other sensitive or protected data within the system that is not fully protected between the district and vendor of the AI platform.

☐ The use of AI for academic purposes should align with the district's curriculum and instructional goals.

☐ I will ensure AI tools are being used responsibly, including but not limited to, avoiding any form of plagiarism or cheating.

☐ I will not assign and require the use of AI tools outside of the list of district-approved tools and resources.

Frequently Asked Questions

What are some consequences of irresponsible use?

- Misuse of district devices and networks may result in suspension of access to district technology resources including revocation of account.
- Misuse may also result in disciplinary and/or legal action against employees, including suspension, expulsion, or criminal prosecution by government agencies. (See AISD Student Code of Conduct, Policy BBI, CQ, CQB, EIA, and DH - Employee Standards of Conduct and the Texas Educator's Code of Ethics).

How does the RUP comply with the law?

The RUP is also intended to:

- prevent unauthorized access and other unlawful activities by users online
- prevent unauthorized disclosure of sensitive information

- comply with federal and state legislation including, but not limited to:
  - the Children's Internet Protection Act (CIPA)
  - Children's Online Privacy Protection Act (COPPA)
  - the Family Educational Rights and Privacy Act (FERPA)
  - the Securing Children Online through Parental Empowerment SCOPE Act
  - Health Information Portability Accountability Act (HIPAA)

How does the RUP take into account copyright violations?
- Copyrighted software or data may not be placed on any system connected to AISD's system(s) without permission from the copyright holder and the AISD's Chief Technology Officer, or designee.
- Only the owner(s) or individuals the owner(s) specifically authorized may upload copyrighted material to the system(s).

Who does the RUP apply to?
- "User" includes anyone using computers, the internet, email, and all other forms of electronic communication, district accounts, district online systems, or equipment provided by the AISD (the "network") regardless of the physical location of the user.

When does the RUP apply?
- The RUP applies when AISD-provided equipment (laptops, tablets, etc.) is used on or off AISD property.
- The RUP applies when non-AISD devices access the AISD network or sensitive information.

Who has access to district technology?
- Access shall be made available to users for instructional and administrative purposes in accordance with administrative regulations, AISD policy, and state/federal law.
- Users understand that AISD may take back possession of AISD equipment at any time or remove access to the network or other district digital systems.
- Access to AISD's technology resources and network, including electronic communications and computer systems, is a privilege, not a right.

How does the district partner in and create conditions for the responsible use of technology?
- AISD uses technology protection measures to filter network access, as much as reasonably possible, to visual and written depictions that are obscene, pornographic, or harmful to minors.

- AISD can and will monitor users' online activities and access, review, copy, and store or delete any communications or files and share them with adults as necessary. Users should have no expectation of privacy regarding their use of AISD equipment, network, and/or Internet access or files, including email (students in grades 6-12 only).
- AISD will take all necessary measures to secure the network against potential cyber security threats. This may include blocking access to AISD applications, including, but not limited to, email, data management and reporting tools, and other web applications outside the United States and Canada.

When and how should I report violations of the RUP?
- Immediately report any known violation of the district's applicable policies or Responsible Use Policy to a supervisor or the district via Let's Talk (Technology Support), AISD Help, or Help Desk.
- You must report requests for personally identifying information or contact from unknown individuals as well as any content or communication that is abusive, obscene, pornographic, sexually-oriented, threatening, harassing, damaging to another's reputation, or illegal.

STAFF
RESPONSIBLE USE POLICY

What are some important terms and ideas to be familiar with in terms of safety and cybersecurity?

Cybersecurity Term	Description
Cookies	Small files which are stored on a user's computer. Cookies provide a way for the website to recognize you and track your preferences.
Data Breach	This is a confirmed incident where information has been stolen or taken from a system without the knowledge or authorization of the system's owner.
Denial of Service (DoS)	An attack floods a website with so much internet traffic that it crashes.
Firewall	A software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the internet.
Identity-Based Attack	A hacker pretends to be someone else to steal personal information or gain access to private systems.
Insider Threats	An employee misuses their access to harm the school's network or steal data.
IP Address	An identifying number for a piece of network hardware.
Malware	Malicious software designed to cause damage or steal data from a computer, server, or network without awareness.
Man in the Middle (MitM)	A hacker secretly intercepts and possibly changes the messages between two parties who believe they are directly communicating with each other.
Multi Factor Authentication (MFA)	A method to verify a user's identity by requiring them to provide more than one piece of identifying information.
Phishing	A hacker tricks someone into giving away their personal information by pretending to be a trustworthy source in an email or message.
Ransomware	Malicious software locks you out of your files or computer and asks you to pay money to get access back.
Spoofing	A hacker disguises themselves as a trusted source to trick you into giving them access to your personal information or computer.
VPN (Virtual Private Network)	Gives you online privacy and anonymity by creating a private network from a public internet connection. VPNs mask your internet protocol (IP) address so your online actions are virtually untraceable.

STAFF
RESPONSIBLE USE POLICY

AUSTIN
Independent School District

Information Technology

Simple. Standard. Secure.

DISCLAIMER: The Superintendent or designee will oversee AISD's electronic communication system(s). AISD's system(s) will be used only for administrative and instructional purposes consistent with AISD's mission and goals. AISD makes no guarantees about the quality of the services provided and is not liable for any claims, losses, damages, costs, or other obligations arising from the use of the network or AISD accounts. Users are responsible for any charges incurred while using AISD devices and/or network. AISD also denies any liability for the accuracy or quality of the information obtained through user access. Any statement accessible online is understood to be the author's individual point of view and not that of AISD, its affiliates, or its employees.

School/Department: _____

Employee Name: _____

Employee Number: _____

Employee Signature: _____ Date: _____

Please return this form to your supervisor or administrator to be kept on file. It is required for all employees who will be using our computer network and/or Internet access.