Wharton Independent School

TECHNOLOGY

Faculty

ACCEPTABLE USE POLICY

2026-2027

TECHNOLOGY DEPARTMENT
2100 North Fulton • Wharton, Texas 77488
www.whartonisd.net

PRINCIPAL OFFICIALS &
ADVISORS BOARD OF TRUSTEES

Phillip Henderson, President
Garland Novosad, Vice President
Lisa Perez, Secretary
Alicia Carter, Board Member
Curtis Evans, Board Member
Millard Stains, Board Member
Robert Vandagriff, Board Member

Cabinet Administrators

Mr. Oduwole, Superintendent
Molli Bodungen, Executive Director of C&I
Heath Roddy, Executive Director of Technology
Sonya Sonia, Executive Director of Special Populations/Human Resources
Landy Williams, Chief of Police
Cheryl Hooper, Business Manager

Campus Principals

Donna Grissom-Sivells Elementary
Dana Gray- Wharton Elementary
Dr. Denise Ware -Wharton Junior High
Diana Bell - Wharton High School

Faculty Acceptable Use Policy (AUP)

Alignment with Texas Education Agency (TEA) Expectations

This policy is designed to align with applicable Texas Education Agency (TEA) guidance, including requirements related to student data privacy, instructional technology use, cybersecurity awareness, and compliance with federal and state regulations such as FERPA, CIPA, and COPPA, as applicable to public school districts in Texas.

Purpose

This Faculty Acceptable Use Policy establishes standards for the responsible, secure, and ethical use of the School District's technology resources. Its purpose is to support instruction, protect district data, ensure compliance with applicable laws, and maintain a safe digital learning environment.

Scope

This policy applies to all district faculty, including:

- Teachers
- Instructional staff
- Campus-based staff with system access
- Substitute teachers and long-term contractors

It covers all district-owned or district-managed devices, networks, systems, accounts, and data.

General Use Expectations

Faculty members are expected to:

- Use district technology primarily for instructional and professional purposes
- Exercise professional judgment in all online communications
- Follow all applicable district policies, state laws, and federal regulations
- Model appropriate digital citizenship for students

Account and Access Management

- Faculty accounts are personal and must not be shared
- Passwords must remain confidential and meet district security requirements
- Multi-factor authentication (MFA) must be used where required
- Access to systems will be role-based and limited to job responsibilities
- Accounts must not be used by unauthorized individuals, including students or family members

Acceptable Use of Technology

Faculty may use district systems for:

- Instructional planning and delivery
- Student learning management systems
- Professional communication with staff, students, and parents/guardians
- Approved research and curriculum development

Prohibited Use

Faculty are strictly prohibited from:

- Accessing, creating, or distributing illegal, harmful, or inappropriate content
- Using district systems for personal commercial gain or political campaigning
- Installing unauthorized software or bypassing security controls
- Circumventing content filters or network security systems such as VPNs
- Using district accounts for personal social media or non-educational public posting

Student Data Privacy

Faculty must:

- Protect all student educational records in accordance with FERPA and state law
- Use only district-approved platforms for storing or sharing student data
- Avoid transmitting sensitive student information through unsecured channels (personal email, messaging apps, etc.)
- Ensure student data is only shared with authorized individuals for educational purposes

Internet and Communication Use

- Professional communication standards must be maintained at all times
- District email and communication systems should be used for official school business
- Faculty must exercise caution when communicating with students digitally, ensuring transparency and appropriateness

A certified or licensed employee, or any other employee designated in writing by the superintendent or a campus principal, may communicate through electronic media with students who are currently enrolled in the district. The employee must comply with the provisions outlined below.

Employees are not required to provide students with their personal phone numbers or email address.

Texting should not occur between 10:00 p.m. and 7:00 a.m. unless extenuating circumstances exist and it is imperative to communicate the message. All other employees are prohibited from using electronic media to communicate directly with students who are currently enrolled in the District.

An employee is not subject to these provisions to the extent the employee has a social or family relationship with a student. For example, an employee may have a relationship with a niece or nephew, a student who is the child of an adult friend, a student who is a friend of the employee's child, or a member or participant in the same civic, social, recreational, or religious organization.

An employee who claims an exception based on a social relationship shall provide written consent from the student's parent. The written consent shall include an acknowledgement by the parent that:

- **The employee has provided the parent with a copy of this protocol**
- **The employee and the student have a social relationship outside of school**

    - **The parent understands that the employee's communications with the student are accepted from district regulation; and**
    - **The parent is solely responsible for monitoring electronic communications between the employee and the student.**
- All communication may be subject to monitoring and review

Device Use and Security

Faculty are responsible for:

- Securing district-issued devices at all times
- Locking devices when unattended
- Applying software updates as directed by the IT department
- Reporting lost, stolen, or compromised devices immediately

Personal devices are NOT allowed on the WISD network

Software and Applications

- Only district-approved software, applications, and services may be used for instructional or administrative purposes
- Faculty must not download or install unapproved software on district devices
- Cloud-based tools must be approved prior to storing student or district data

Artificial Intelligence and Emerging Technologies

If AI tools are permitted by the district:

- Faculty must use approved AI tools only
- AI-generated content must be reviewed for accuracy and appropriateness
- Student data must not be entered into unauthorized AI platforms
- AI tools must be used transparently and ethically in instructional settings

Monitoring and Privacy

Faculty should have no expectation of personal privacy when using district technology resources. The district reserves the right to:

- Monitor network activity, email, and system usage
- Review files and communications stored on district systems
- Investigate suspected policy violations

Security Reporting

Faculty must immediately report:

- Suspected phishing or cyberattacks
- Unauthorized access or account compromise
- Lost or stolen devices
- Any accidental exposure of sensitive data

Reports should be made to campus administration and/or the IT department.

Violations and Consequences

Violations of this policy may result in disciplinary action, which may include:

- Loss of technology privileges
- Written reprimand
- Mandatory retraining
- Suspension or termination of employment
- Legal action where applicable

Policy Review

This Acceptable Use Policy will be reviewed annually and updated as needed to reflect changes in technology, law, and district practices.

NOTICE:

Notice: The Technology Department reserves the right to remote in on any district device to perform maintenance at any time. If the Technology Department deems a device is unsafe due to a virus, they will come take the device immediately to maintain the integrity of our network.

Notice: If a faculty member has been issued a district laptop, this device is filtered while at home and on any another network. Faculty should understand that while not on campus, all filtering still applies for CIPA purposes. The Executive Director of Technology actively monitors all devices and any inappropriate activity will be reported.

Wharton Independent School District
AUP Signature Page for 2026-2027 School Year:

I understand that my use of the District's technology resources is not private and that the District will monitor my activity. I have read the District's technology resources policy, associated administrative regulations, and this is your agreement and agree to abide by the provisions of Wharton ISD. In consideration for the privilege of using the District's technology resources, I hereby release the District, its operators, and any institution with which they are affiliated from any and all claims and damages of any nature arising from my use of, or inability to use, these resources, including, without limitation, the type of damages identified in the District's policy and administrative regulations.

I understand that this user agreement must be renewed each school year. If you have any questions concerning this document, please contact Heath Roddy, WISD Executive Director of Technology, at 979-488-2595.

Signature: _____

Campus: _____

Date: _____