General Sec ri Accep able U e Polic

Policy Title	Acceptable Use Policy
Policy Category	IT – Security Policy
Policy Owner	Information Technology
Policy Approver(s)	Chief Information Officer or Designee

Defini ion

Shadow IT: Th

5. Users will protect District IT assets, keeping them physically and logically secured and under the control of the user, including but not limited to:
    a) Locking down laptops with a locking cable or storing them in a locked drawer or cabinet when leaving them in the office.
    b) Ensuring the workstation is locked (screen/keyboard) whenever walking away from it.
6. Access to District systems and devices is controlled through individual accounts and passwords. Users are responsible for not sharing the password for that account with others.
7. As applicable, you must comply with the District's record management program, the Texas Open Meetings Act, the Public Information Act, the Family Educational Rights and Privacy Act (FERPA), including retention and confidentiality of student and District records, and campaign laws.

B. Electronic Communication and Internet Use

The use of District communication and internet systems and services (including email, instant messaging, voicemail, forums, social media, and more) is provided to perform regular daily tasks. The use is a privilege, not a right, and therefore must be used with respect, common sense, and in accordance with the following requirements:

1. The email systems and other messaging services used at the District are owned by the District and are therefore its property. This gives the District the right to monitor any and all email traffic passing through its email system. This monitoring may include, but is not limited to, inadvertent reading by IT staff during the normal course of managing the email system, review by the HR and legal team during the email discovery phase of litigation, and observation by management in cases of suspected abuse or employee inefficiency.

2. The District often delivers official communications via email. As a result, employees of the District with email accounts are expected to check their email in a consistent and timely manner so that they are aware of important District announcements and updates, as well as for fulfilling business and role-oriented tasks.

3. Electronic communication and the internet must not be used for illegal or unlawful purposes,

8. Any allegations of misuse should be promptly reported to the Service Desk. If you receive an offensive or suspicious email, do not forward, delete, or reply to the message. Instead, report it directly to Service Desk.

9. Email users are responsible for mailbox management, including organization and cleaning. If a user subscribes to a mailing list, he or she must be aware of how to unsubscribe from the list and is responsible for doing so if their current email address changes.

10. Archival and backup copies of email messages may exist, despite end-user deletion, in compliance with District's Records Retention Policy.

11. Email access will be terminated when the user terminates their association with the District, unless other arrangements are made. The District is under no obligation to store or forward the contents of an individual's email inbox/outbox after the term of their relationship has ceased.

12. Users shall not send sensitive information that is not appropriately protected (encrypted). (Appropriate means of protection include but are not limited to OneDrive or encrypted attachments through email.)

    a) Users shall take extra precautions when transmitting

a) Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a system or account that the user is not expressly authorized to access unless these actions are within the scope of regular duties. For the purposes of this section, “disruption”