Note: For information regarding use of the District's technology resources and electronic communications by Board members, see BBI(LOCAL). For student use of personal electronic devices, see FNCE. For additional provisions governing employee use of electronic media, see DH(LOCAL) and the employee handbook. For information regarding District, campus, and classroom websites, see CQA. For information regarding intellectual property and copyright compliance, see CY.

Information Technology

The Superintendent of Schools or designee (normally the Chief Technology Officer) is charged with providing the technology environment to support the District's goals.

The Information Technology division (IT) is responsible for design, development, implementation, and support of reliable information technology services that promote digital learning for all students.

IT is also responsible for identifying and managing risks to the information systems and data assets by establishing and maintaining appropriate controls.

Technology Resources

The District will make technology resources available to staff, students, parents, and members of the public as appropriate. Available technology resources include onsite internet access, District-owned hardware and software, District-approved online educational applications for use at school and at home, and digital instructional materials.

Technology Governance

IT will establish a Technology Steering Committee to facilitate stakeholder input regarding policy development, major technology investment decisions, resource utilization, and risk management.

Copyright

The reproduction, forwarding, or republishing or redistributing of words, graphics, or other copyrighted materials must be done only with the permission of the author or owner. Users must assume that all materials on the internet are copyrighted unless specific notice states otherwise.

Making unauthorized copies of licensed and copyrighted software, even if for "evaluation" purposes, is forbidden. The District permits reproduction of copyrighted materials only to the extent legally considered fair use or with the permission of the author or owner.

Electronic Signatures

At the District's discretion, the District may make certain transactions available online, including student admissions documents, student grade and performance information, contracts for goods and services, and employment documents.

To the extent the District offers transactions electronically, the District may accept electronic signatures in accordance with CQ(LOCAL).

When accepting electronically signed documents or digital signatures, the District will comply with rules adopted by the Texas Department of Information Resources, to the extent practicable, to:

- Authenticate a digital signature for a written electronic communication sent to the District;
- Maintain all records as required by law;
- Ensure that records are created and maintained in a secure environment;
- Maintain appropriate internal controls on the use of electronic signatures;
- Implement means of confirming transactions; and
- Train staff on related procedures as necessary.

Note: For more information, see DIR Guidelines for the Management of Electronic Transactions and Signed Records[1].

Content Filtering

The Chief Technology Officer or designee will select, implement, and maintain appropriate technology for filtering material considered inappropriate or harmful to minors. All internet traffic on the District's network will be filtered. Off-network web filtering for students will be provided for District-issued technology equipment authorized for student use off-campus.

The categories of material considered inappropriate and to which access will be blocked will include, but not be limited to, nudity/pornography; images or descriptions of sexual acts; promotion of violence, illegal use of weapons, drug use, discrimination, or participation in hate groups; instructions for performing criminal acts (e.g., bomb-making); and online gambling.

Content Filtering Exceptions

The Chief Technology Officer or designee will consider requests from users who wish to use a blocked site for bona fide research, instruction, or other lawful purposes. Users who wish to use an individually blocked site for bona fide research, instruction, or other lawful purposes must follow technology guidelines and processes to unblock the site.

Authorized Use

All students, employees, and Board members will be required to sign or affirm the District's acceptable use policy annually for issuance or renewal of an account. [See CQ(EXHIBIT—A)]

All other authorized users will be required to affirm the District's acceptable use policy each time before being granted access to the District's technology resources.

District technology resources will be used for learning, teaching, and administrative purposes consistent with the District's mission and goals. Limited personal use is permittable, however, the District does not grant ownership, privacy, or an expectation of privacy in the contents of any electronic messaging, including email, voice mail, text, or other internet activities involving District technology resources or equipment. Electronic communications are considered public records and may be released pursuant to the requirements of the Texas Public Information Act (TPIA).

Unauthorized Use for Employees

The following represent examples of the unauthorized use of District technology resources.

Personal use must be kept to a minimum and should not interfere with or impair an employee's job performance. Personal use is prohibited if it:

1. Interferes with the use of technology resources by the District;
2. Burdens the District with additional costs;
3. Interferes with the staff member's job duties or other obligations to the District;
4. Includes any activity that is prohibited by District policy or state or federal law;
5. Infringing upon the intellectual property rights of others or violating copyright laws;
6. Using District technology resources to advance the employee's or a third party's business or to make a personal profit;
7. Distribution of propaganda, campaign, or marketing materials;
8. Uploading or downloading District data without explicit written authorization;
9. Unauthorized access to confidential or sensitive information, student data, or any other information covered by existing state or federal privacy or confidentiality laws, regulations, rules, policies, procedures, or contract terms;

10. Downloading and/or installing unlicensed software;
11. Bypassing or attempting to bypass the District's security or content filtering safeguards;
12. Accessing or attempting to access resources for which an employee does not have explicit authorization;
13. Allowing another person to use a restricted District system;
14. Modifying, repairing, removing, reconfiguring, or tampering with a District electronic device except as authorized by the Chief Technology Officer;
15. Allowing non-District individuals permission to use assigned District technology equipment;
16. Accessing pornographic material;
17. Using the device to commit a crime;
18. Using District technology resources as a bot to launch malicious activities;
19. Possessing or using any computer hacking tools, as defined in the Texas Computer Crime Act; or
20. Violating any federal, state, or local law or Board policies and administrative rules.

Unauthorized Use for Students

The following represent examples of the unauthorized use of District technology resources by students:

1. Use of technology resources for commercial purposes;
2. Use of obscene, bullying, profane, lewd, threatening, disrespectful, or gang-related language or symbols;
3. Bypassing or attempting to bypass the District's security or content filtering safeguards;
4. Sharing of District account information;
5. Modifying, repairing, reconfiguring, or otherwise tampering with technology resources except as authorized by the Chief Technology Officer;
6. Unauthorized access or attempted unauthorized access to District information systems;
7. Intentionally overloading District systems (i.e. Distributed Denial of Service or Denial of Service attack);

8. Destroying or tampering with any computer equipment or software;

9. Possessing or using computer hacking tools, as defined in the Texas Computer Crime Act;

10. The use of technology resources for illegal activities including, but not limited to, planting viruses, hacking, or attempted unauthorized access to any system; or

11. Violating any federal, state, or local law or Board policies and administrative rules.

Access

Access to District technology resources will be controlled and managed to ensure that only authorized individuals and computers have appropriate access in accordance with educational and business needs.

All computers that are permanently or intermittently connected to the District network will use an approved credentials-based access control system.

All systems containing Confidential or Regulated Data, as defined below, will employ credentials-based access control systems and encryption for data in transit and encryption for data at rest, in accordance with Federal Information Processing Standard (FIPS) Publication 140-2 standards.

General Guidelines

Access to District technology resources will be managed as follows:

1. Every user must have a user profile that defines roles and access privileges.

2. The District will conduct reviews of standard users' access annually.

3. The District will conduct reviews of system administrator user accounts semi-annually.

4. The District will revoke user access within 48 hours of termination of employment, student withdrawal, graduation, or other change in enrollment status.

5. Only authorized users will be granted access to District information systems, and the principle of least privilege will be enforced.

6. The District will assign user privileges based on an individual's role. Efforts will be made to prevent any user from having access not required for the role.

7. Default access for systems containing Confidential or Regulated data will be “deny-all.”

8. The District will not permit anonymous or guest logins, except as explicitly authorized by the Chief Technology Officer.

9. Any user identified as a security threat or as having violated District policies may be denied access to the District’s technology resources.

Passwords

Passwords for District technology resources will be managed as follows:

- The District promotes the use of strong passwords, as defined by National Institute of Standards and Technology (NIST) Document SP 800-63-3[2].
- All District passwords must remain confidential and will not be shared.
- Passwords must have a minimum of 8 characters.
- Passwords must be stored and transmitted in an encrypted manner.
- District-owned mobile devices and Employee-owned mobile devices that allow access to District e-mail or any Confidential or Regulated data must be password protected in accordance with District standards.

Student Access

Student access to technology resources will be managed as follows:

1. Students in prekindergarten–grade 5 will be granted access to the District’s technology resources. Password complexity standards may be relaxed or waived as determined by the campus principal and/or Chief Technology Officer as elementary students will have no access to Confidential or Regulated data. Students in grades prekindergarten–grade 5 will be provided access to authorized District online educational applications and digital instructional materials and should not create individual accounts using personally identifiable information. Students in grades prekindergarten–grade 5 may be assigned individual District-issued accounts, email accounts, and passwords as authorized by the campus principal and/or Chief Technology Officer. Email accounts for elementary students are restricted to limit communications within the Dallas ISD domain.

2. Students in grades 6–8 will be assigned individual District-issued accounts and passwords for use of District technology

resources, including individual email accounts. Email accounts for middle school students are restricted to limit communications within the Dallas ISD domain. Students in grades 6–8 will be provided access to authorized District online educational applications and digital instructional materials and should not create individual accounts using personally identifiable information.

3. Students in grades 9–12 will be assigned individual District-issued accounts and passwords for use of District technology resources, including individual email accounts. Email accounts for high school students are not restricted. Students in grades 9–12 will be provided access to authorized District online educational applications and digital instructional materials and should not create individual accounts using personally identifiable information.

4. When using social media in the classroom, staff should provide information to parents and guardians regarding the purpose of the selected media and a description of the information shared. Unless detrimental to the classroom objective, staff will use password-protected social media sites. Parents and guardians may opt out of participation in classroom social media projects that will use the student's photo or likeness by signing the District's Consent and Release of Liability Form[3].

5. Parent/Guardian approval is required before any student may be assigned District-owned technology equipment for use off-campus. Both Parent/Guardian and student must complete and sign the District form acknowledging the responsibilities of the student and Parent/Guardian when a device is assigned to a student. [See CQ(EXHIBIT—B)]

Parent Access

Parents/Guardians may be provided access to District technology resources, including student information and learning management systems or mobile applications, in accordance with guidelines established by the campus or the administrative department.

Access is strictly limited to information for the specific child and must be revoked upon withdrawal, change in enrollment status, or when the child turns eighteen.

District Employee Access

With written approval of the immediate supervisor or the Superintendent or designee, and upon acceptance of the District's acceptable use policy, District employees will be granted access to the District's technology resources as appropriate.

Public Access

Members of the public may be provided access to District technology resources, including computer and internet access, online job

applications, and access to the District's guest Wi-Fi services, in accordance with guidelines established by the campus or the administrative department.

Use of District technology resources by members of the public may not interrupt instructional activities or technology operations.

Participation in Social Media

Under appropriate system controls and supervision, participation in approved social media using the District's technology resources for educational and administrative purposes is permissible for students and staff.

Social media includes but is not limited to text messaging, instant messaging, email, web logs (blogs), electronic forums (chat rooms), video-sharing websites (e.g. YouTube), editorial comments posted on the internet, and social network sites (e.g., Facebook, Instagram, Twitter, LinkedIn).

Students participating in social media using the District's technology resources should assume that all content shared, including pictures, is public. No personally identifying information should be published. Students should not respond to requests for personally identifying information or contact from unknown individuals.

Student Training on Safety and Security

Students participating in social media and other public internet services using the District's technology resources must receive training on the following:

1. All content shared, including pictures, is presumed to be public;
2. Personally identifiable information about themselves or others should not be shared;
3. Requests for personally identifiable information or to respond to any contact from unknown individuals should not be answered;
4. Students may not sign up for unauthorized programs or applications using the District's technology resources;
5. Risks of disclosing personal information on websites and applications using the students' own personal technology resources;
6. Recognizing cyberbullying and appropriate responses; and
7. Using appropriate online etiquette and behavior when interacting using social media or other forms of online communication or collaboration.

Approval of Technology Resources

The District will ensure that all technology resources in use within the District meet state, federal, and District standards for safety and security of District data, including a student's education records and personally identifiable information. [See FL(LEGAL) and (LOCAL).]

District staff wanting to use an online instructional resource, mobile application, digital subscription service, or other program or technology application requiring the user to accept terms of service or a user agreement, other than a District-approved resource, must first submit a request for approval. [See Digital Instructional Resources Authorization Request form]

No student 13 years of age or younger will be asked to download or sign up for any application or online account using his or her personally identifiable information.

Reporting Violations

Students and employees must immediately report any known violation of the District's applicable policies, internet safety plan, or responsible use guidelines to the principal or Information Security Director.

Students and employees must report to a principal or the Information Security Director any requests for personally identifiable 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.

The Information Security Officer will promptly inform the Chief Technology Director, law enforcement, or other appropriate state agency of any suspected illegal activity relating to misuse of the District's technology resources and will cooperate fully with local, state, or federal officials in any investigation or valid subpoena.

Sanctions

Inappropriate use of the District's technology resources may result in revocation or suspension of the privilege to use these resources, as well as other disciplinary or legal action, in accordance with applicable laws, District policies, the Student Code of Conduct, and District administrative regulations.

Termination / Revocation of Use

The District may suspend or revoke a system user's access to the District's technology resources upon violation of District policy and/or administrative regulations regarding acceptable use.

Issuing Technology Equipment to Students

The following rules will apply to all campuses and departments loaning technology devices and equipment to students for off-campus use:

1. Proposed projects to distribute devices and equipment to students must be jointly approved by the appropriate Executive Director of School Leadership and the Chief Technology Officer.
2. Before loaning devices and equipment to a student, the IT quadrant supervisor and principal must have clearly outlined:
    a. An equitable process to determine eligibility;
    b. An agreement that identifies the responsibility of the student regarding home placement, use, and ownership of the device or equipment [See CQ(EXHIBIT–B)];
    c. A process to distribute and initially train students in the setup and care of the device or equipment;
    d. A process to provide ongoing technical assistance for students using the device or equipment;
    e. A process to measure utilization of the device or equipment;
    f. A process to measure impact on student achievement;
    g. A process for retrieval of the device or equipment from a student as necessary; and
    h. A process for reporting lost or stolen devices or equipment.

Student Use of Personal Electronic Devices for Instructional Purposes

The following rules will apply to student use of personal telecommunications or other electronic devices for on-campus instructional purposes:

1. Requests to use personal telecommunications or other personally owned electronic devices for on-campus instructional purposes must be submitted to the principal for approval.
2. Agreements for acceptable use of the District's technology resources and personal telecommunications or other electronic devices for on-campus instructional purposes must be signed annually by the student and parent. [See CQ(EXHIBIT–A)]
3. When using devices for instructional purposes while on campus, students must use the District's guest Wi-Fi. Any attempt to bypass the District's content filter will result in restrictions and/or disciplinary action as required by the Student Code of Conduct.
4. When not using devices for instructional purposes while on campus, students must follow the rules and guidelines for

noninstructional use as published in the student handbook and policy FNCE.

5. Students should bring devices from home fully charged, if possible.

6. The District is not responsible for damage to or loss of personally owned electronic devices brought from home. The District will not provide direct technical support for personal devices. The District may provide information to the students and parents as to how to configure approved personal devices for instructional use.

7. Campuses may impose additional rules and restrictions regarding use of personal electronic devices that do not conflict with District policies. Violation of these rules may result in suspension or revocation of system access and/or suspension or revocation of permission to use personal electronic devices for instructional purposes while on campus, as well as other disciplinary action, in accordance with the Student Code of Conduct.

Information Security

All data, regardless of the form or format, which is created or used in support of the District business activities is owned by the District. District-owned data is an asset and must be protected from its creation through its useful life, to its timely and authorized disposal. District data must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use.

Data Classification

The District uses the Texas Department of Information Resources guidelines to classify data. The District uses four data classifications: Public, Sensitive, Confidential and Regulated.

District-owned data is classified as follows:

1. Regulated Data is information that is controlled by a state or federal regulation or other third-party agreements. Examples of Regulated Data may include, but are not limited to:

   a. Health information;

   b. Credit card information; and

   c. Criminal justice information.

2. Confidential Data is information that typically is excepted from the Texas Public Information Act. Examples of Confidential Data may include, but are not limited to:

a. Personally Identifiable Information (PII), such as a name in combination with social security number (SSN) and/or financial account numbers;

b. Intellectual property, such as vendor copyrights, patents, and trade secrets;

c. Passwords used for authenticating individuals; and

d. Network architecture schematics.

3. Sensitive Data is information that could be subject to release under a public information request but should be controlled to protect third parties. Examples of Sensitive Data may include but are not limited to:

a. Operational information;

b. Personnel records;

c. Salary information; and

d. Internal communications.

4. Public Data is information that is freely and without reservation made available to the public. Examples of Public Data may include but are not limited to:

a. Press releases;

b. Public web postings; and

c. Publications.

Responsibilities

The following key roles and responsibilities apply to the District's information security practices.

Data Owner: The District executive responsible for specific information that must be protected. The Data Owner has the primary responsibility for data protection. For instance, financial data belongs to the Chief Financial Officer, employee data to the Chief Human Capital Management Officer, and student data to the Chief Academic Officer, Chief of School Leadership, and/or school principal in accordance with policy FL(LOCAL).

Systems Owner: The District administrator responsible for directing the operation of a computer system and the applications residing on that system. Systems Owners are those persons delegated the responsibility for protecting the information of the Data Owners. The Systems Owner may or may not be the Data Owner of any data maintained on the system for which they are responsible. The

Systems Owner may or may not be the Information Technology Division. Regardless of systems ownership, all applicable security controls must be documented and maintained.

Chief Technology Officer: The Chief Technology Officer has the authority to determine whether a new District computer system or service is launched in accordance with information security standards as well as the extent of required mitigation work for existing systems.

Data User: Individuals for whom the systems are designed. Data users may include District employees, students, parents/guardians, District vendors, and members of the public at large. Data users access system resources to achieve some benefit related to their education, job duties, or citizen participation in District governance. Depending on the nature of the system, data users may or may not be individually identifiable.

The Data Owner, in consultation with the IT Information Security Director and the Legal Department as needed, is responsible for determining the data classification level. Once a classification has been defined, the computer systems containing that information must be approved by the Data Owner and Chief Technology Officer, and must meet minimum standards for security controls, as described below.

If the system is deemed by the Data Owner, in consultation with the Information Security Director and General Counsel or designees, to contain a particular threat due to type or magnitude of the information, the marketability of the information, or the potential for fraud or other misuse, additional security controls may be required.

Security Controls

The Dallas ISD Information Security Control Standards Framework (Dallas ISD-ISCS) for information systems containing Public, Sensitive, Confidential, and Regulated Data are based on the NIST, Special Publication 800-53[4]. The District's information security control standards are also published on the District's public website [see Dallas ISD Information Security Control Framework (Dallas ISD-ISCF)[5]].

These information security controls are subject to change as data protection practices and technologies evolve.

Exceptions to the security control standards must be authorized in writing by the Chief Technology Officer and General Counsel.

Data Sharing

District data will only be shared with authorized third parties through an approved Data Sharing Agreement or as otherwise authorized by law [see Data Sharing Agreement template].

Each data sharing request is evaluated for appropriateness and compliance and must be authorized by the appropriate District signators. Vendors and partners authorized to receive district data are required to protect Dallas ISD data in accordance with all applicable laws, regulations, and standards.

Software Licensing

All software used in the District must be legally licensed and approved. All software should be installed by technology department staff or authorized agents.

Personal Software

The installation of personal software on District technology equipment is prohibited.

Mobile Device Usage For Employees

The use of mobile devices can increase employee productivity, promote employee and student safety, and provide economic efficiencies. This section outlines allowable business use for mobile devices, provides a framework for mobile device management and accountability, and defines allowance parameters.

A mobile device is defined as any portable electronic device with cellular communications capability, such as mobile phones, "smart" phones, tablets, or hotspots. There are three types of mobile devices:

1. District-owned mobile device: A mobile device owned by and with service plan paid by the District and used for conducting District business.
2. Reimbursed mobile device: A mobile device owned by the employee with a service plan paid in part by a District allowance and which is used in whole or in part for conducting District business.
3. Non-reimbursed mobile device: A mobile device owned by the employee with a service plan paid in whole by the employee, but which is used in part for conducting District business.

Department Responsibilities

Departments must actively manage mobile devices using the following standards:

- Departments may assign District-owned mobile devices as necessary for business needs and manage the purchasing, assignment, and use of District-owned mobile devices in compliance with law and applicable District policy [see Mobile Device and Hot Spot Authorization Agreement (Parts 1 & 2)];
- Departments will provide an appropriate District-owned mobile device and service plan when an employee’s job duties require use of a mobile device and the employee does not receive an allowance for a mobile device;

- Departments may approve an allowance for an employee who uses a personal mobile device for District business, and the Department must manage the authorization, administration, and use of reimbursed mobile devices in compliance with law, District policy, and information security standards;
- Departments will provide allowances for authorized use of reimbursed mobile devices at the following standard monthly levels:
  - Access to District Wi-Fi only - $0;
  - Voice/text services - $25/month;
  - Data services - $25/month; and
  - Voice/text and data services - $50/month.
- Departments may approve business use of non-reimbursed mobile devices as necessary for the conduct of District business. Approved use will comply with applicable laws and District policy and information security standards. [See Mobile Device and Hot Spot Authorization Agreement (Parts 1 & 2)];
- In determining which, if any, type of mobile device use is authorized for business needs, departments should consider whether:
  - Employee's job requires field work or travel where landline phones are inaccessible or inefficient;
  - Employee's job requires immediate or on-call availability;
  - Employee needs a mobile device for work-related safety, security, or other emergency reasons;
  - Employee's job requires real-time communication, including email, text messaging, or use of mobile applications;
  - When use of a mobile device increases productivity, enables business objectives, reduces costs, or improves employee satisfaction; and
  - Other requirements as defined and documented by department.
- Before allowing use of any mobile device to conduct District business, authorized department staff and the District employee receiving the authorization must complete and sign the applicable portions of the Mobile Device Authorization and Agreement. [See Mobile Device and Hot Spot Authorization

Agreement[6] in the District's Information Technology website. (Parts 1 & 2)];

- Periodically monitor the ongoing appropriateness of mobile device authorization, issuance, services, reimbursement, and adherence to security standards;
- A Mobile Device Authorization and Agreement terminates, and the Department will cease paying, when the first of the following events occurs:
  - Employee termination;
  - Department ceases to have a business need for employee mobile access;
  - Termination or suspension of the reimbursed or non-reimbursed mobile device service and/or service contract; and
  - A decision to terminate authorization for District paid mobile device or reimbursed personal device at the discretion of the department.
- Designate an individual who will coordinate District-Owned mobile device orders, service delivery, and billing for their respective department and users;
- Use the existing master contracts for District-owned mobile devices and services unless a waiver is authorized by the appropriate chief;
- Notify the Telecommunications Department of lost or stolen mobile devices immediately; and
- Preserve and retain, in accordance with records retention schedules, records including text messages and emails used to conduct District business.

Employee Responsibilities

Employees must:

- Obtain proper authorization before use of any mobile device to conduct District business;
- Sign the appropriate employee agreement [See Mobile Device and Hot Spot Authorization Agreement (Parts 1 & 2)];
- Upon notification of termination or revocation of the Mobile Device Authorization and Agreement, employees must immediately cease use of a mobile device to conduct District business and promptly return a District-owned mobile device to

the department coordinator or Telecommunications Department; and

- Upon termination of the Mobile Device and Hot Spot Authorization and Agreement, employees must consult with their department to appropriately preserve and retain public records, including text messages and emails, on the mobile device used to conduct District business.

Adoption or Last Amendment Date

This regulation was last amended on August 26, 2020.

---

[1] DIR Guidelines for the Management of Electronic Trans-actions and Signed Records: http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Texas%20Uniform%20Electronic%20Transactions%20Act%20(UETA)%20Guidelines.pdf
[2] NIST Special Publication 800-63 – Digital Identity Guidelines: https://pages.nist.gov/800-63-3/sp800-63-3.html
[3] District's Consent and Release of Liability Form: https://www.dallasisd.org/site/default.aspx?PageType=3&ModuleInstanceID=52530&ViewID=C9E0416E-F0E7-4626-AA7B-C14D59F72F85&RenderLoc=0&FlexDataID=62834&PageID=39025&Comments=true
[4] NIST, Special Publication 800-53: https://nvd.nist.gov/800-53/Rev4
[5] Dallas ISD Information Security Control Framework (Dallas ISD-ISCF): https://www.dallasisd.org/Page/61543
[6] Mobile Device and Hot Spot Authorization Agreement: https://www.dallasisd.org/Page/61537