Goose Creek CISD
Data Governance Guidelines

Introduction

Protecting the privacy of our students and staff is Goose Creek CISD's priority. We are committed to maintaining strong, meaningful privacy and security practices. The privacy and security of this information is a significant responsibility and we value the trust of our students, parents, and staff.

The purpose of the Data Governance Guidelines are to institute effective data governance by establishing accountability, ensuring that the district's data is accurate, accessible and protected, and by establishing responsibility along with procedures to be used for the management and protection of information.

District employees are subject to regular audits to ensure compliance with laws and regulations, district polices, Admin guidelines, the Employee Handbook and Responsible Use Policies.

The Data Governance Guidelines are reviewed and updated annually or as needed per evolving laws and regulations.

Scope and Regulations

Proper management of school district records, whether in paper or electronic form, is a necessity of all staff, which is also a legal requirement. The Texas Local Government Records Act, Chapter 201, states that as a public school district employee, you have an obligation to correctly and efficiently maintain the records in your possession to comply with standards for public access, parent/student access, and for legal or audit purposes.

All employees must know the records for which they are responsible, the length of time they must be retained, and how to maintain and discard them in a correct and legal manner.

Every GCCISD staff person is responsible multiple types of school district records. These records may include student or employee information, purchasing, training records, phone messages, meeting agendas, webpages, etc.

Goose Creek CISD will abide by any applicable regulatory acts including, but not limited to:

(CIPA) Children's Internet Protection Act

CIPA requires districts to put measures in place to filter Internet access and other measures to protect students.
http://www.fcc.gov/guides/childrens-internet-protection-act

(COPPA) Children's Online Privacy Protection Act

COPPA puts special restrictions on software companies about the information they can collect about students under 13. Since students under 13 can't make their own accounts, district staff must make the accounts for them. In making the accounts, staff need to be aware of their responsibility under FERPA.
https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

(FERPA) Family Educational Rights and Privacy Act

FERPA requires that schools have written permission from the parent or guardian in order to release any information from a student's education record. Applications and third-party systems should be properly vetted to ensure they comply. http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

(PPRA) Protection of Pupil Rights Amendment

The Protection of Pupil Rights Amendment, or PPRA, is a federal law that provides certain rights for parents of students regarding, among other things, student participation in surveys; the inspection of instructional material; certain physical exams; and the collection, disclosure, and use of personal information for marketing purposes. http://www2.ed.gov/policy/gen/guid/fpco/ppra/index.html

(HIPAA) Health Insurance Portability and Accountability Act

Used to measure and improve the security of health information.
http://www.hhs.gov/ocr/privacy/hipaa/understanding/

(PCI DSS) Payment Card Industry Data Security Standard This covers the management of payment card data.
http://www.pcisecuritystandards.org/

(SCOPE Act) Texas House Bill No. 18, the Securing Children Online through Parental Empowerment Act, also known as the SCOPE Act, requires covered digital service providers to provide minors with certain data protections, prevent minors from accessing harmful content, and give parents tools to manage their child's use of the service.

Relevant to Texas school districts, the bill specifically relates to the protection of minors from harmful, deceptive, or unfair trade practices in connection with the use of certain digital services and electronic devices, including the use and transfer of electronic devices to students by a public school.

https://capitol.texas.gov/tlodocs/88R/billtext/pdf/HB00018H.pdf

The Texas State Library and Archives Commission (TSLAC) sets the required minimum standards for records management in local governments. The commission has created RETENTION SCHEDULES which GCCISD must follow in order to comply with the law. These schedules list the types of records that a school district is required to keep, and specifies the amount of time we are required to maintain that type of record. This requirement is addressed in our Board Policy CPC (Legal) and CPC (Local).

Data Retention Periods

GCCISD follows the Texas State Library and Archives Commission recommendation for record retention periods.

What is a record and why do we care?

According to Texas Local Government Code Section 201.003, a School District record:

- Documents the transaction of district activity and business.
- Is created or received by a school district staff person or board member.
- Is a record whether open (available for public access) or closed.
- May exist in any medium – paper, electronic, photo, film, etc.

Types of Storage

- Paper / Hard Copy
- On-Site Campus / Department
- Off-Site
- Electronic (District Network Drive or District-wide System)

School records DO NOT include extra copies of the original document, blank forms, or stocks of publications. The process of managing records:

- Improves access to information.
- Controls the amount of materials taking up valuable office, server or cloud space.
- Reduces operating costs.
- Minimizes litigation risks.
- Safeguards vital information.

Retention Terms and Guidelines

"Retention" - The minimum amount of time we are legally required to keep a record.

"Texas State Library and Archives Commission" - Agency responsible for setting and maintaining state standards for records retention.

"Retention Schedule" - A document that lists the record series of an organization, with mandatory minimum retention periods for each records series.

"Records Series" - A group of records, all with the same function, regardless of format
Examples of record series:

- Construction Records
- Correspondence
- Academic Records

Safe Storage of District Records

Whether the records you hold are in paper or electronic form, it is important to use safe storage practices. The following are best practices for safely storing records:

- Use a filing system (usually by year) which allows for easy access, and for removal of records when the time comes for destruction, deletion, or off-site storage.
- At least one other staff person should be aware of the location and filing system for your records, whether or not they have direct access.
- Electronic records must always be stored on a GCCISD network drive such as G:, S:, or on a GCCISD database system. These locations are secure and safe for record storage. Your Desktop, C: drive, or "My Documents" folders are susceptible to loss if your desktop or laptop computer fails.
- Be sure that the records you use, view or store are never accessible to unauthorized persons.
- Make sure paper records are stored at least a few inches off the floor, and are generally secure from flood, theft, accidental destruction, and other potential damage or loss.
- When scanning items into network electronic storage, the original paper copy may be destroyed per district or state guidelines. Please make this decision with care!

Email Retention

Much of our school district business is conducted through email correspondence, and these emails are considered School District records. To adequately comply with most retention requirements, GCCISD maintains our email database for a period of 7 years. During that period, any email that you have created or received through the district's Microsoft Outlook system is retrievable.

- GCCISD retains all incoming and outgoing for a period of 7 years.
- Most emails do not have a long retention requirement.
- You may or may not have direct access to all 7 years of your emails.
- If you receive or send emails that contain the RECORD COPY of items that have a long retention requirement (more than 7 years), it will be necessary for you to store that email in another way.
- Two options we suggest for keeping email long term are:
    - Printing the email and filing the paper copy;
    - scanning the copy or otherwise creating a pdf for storing on a network drive.

Securing Electronic Data at Rest

- GCCISD servers offer end to end fault tolerance, ensuring all backups, updates and patches are completed. Any sensitive information is stored with appropriate security access and encryption.
- GCCISD data servers are stored in a data center and can only be accessed by authorized personnel.
- Sensitive data should not be stored on any unencrypted end user computer systems or USB devices.

Securing Electronic Data in Transit

- GCCISD utilizes HTTPS protocols and certificates with modern encryption to ensure data is properly secured in transit.
- Sensitive information can only be gathered from within our district by using authorized credentials with our login portal or VPN access.
- Conditional access blocks users from logging into any accounts from outside of the United States.
- All network closets remain locked and can only be accessed by authorized personnel.
- Sensitive information should not be sent through unencrypted email.

Controls to Safeguard Data

Goose Creek CISD utilizes many controls to ensure that only authorized individuals that have a business or educational need to access data can do so. By utilizing role-based access to the network as well as most, if not all, applications and systems, the principle of least privilege is enforced. For more information on these safeguards and student data privacy please refer to the Student Data Collection and Security Fact Sheet.

Records Destruction

When your records have met their required retention period, it is important to destroy or delete them in a timely manner. District removal and destruction procedures are required when destroying paper records and other items if they:

- Are record copies of an item listed on the District's retention schedule; or
- Have personal identifiable information (PII).

Why dispose of records?

- Frees up physical space.
- Reduces operating equipment, storage supply, and personnel costs.
- Speeds up retrieval.
- Provides legal protection when done properly.

When to Destroy Records

Follow the retention schedule. It is illegal to destroy any record that is involved in ongoing litigation, public information request, or audit.

Contacts and Information

Goose Creek CISD is dedicated to preserving our most valuable resources - records and information. Properly managed records can result in considerable cost-savings and operational efficiency. Campus Principals or designee will maintain records for current students and the District Superintendent or designee will maintain all other records.

Updates to this Document

This document is reviewed annually to provide updates that align with changes in laws/regulations and the constantly changing technology landscape. Due to the effective date of some laws, this document may be updated more frequently as needed.