Goose Creek CISD
Data Governance Guidelines

Introduction

Protecting our students' and staffs' privacy is an important priority and Goose Creek CISD is committed to maintaining strong and meaningful privacy and security protections. 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 is 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 they are compliance with all laws, regulations, district polices, Admin guidelines, Employee Handbook, and Responsible Use Policies.

The Data Governance Guidelines are reviewed and updated at least 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 not only a necessary part of every staff person's job, it 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 then discard them in the correct and legal manner.

Every GCCISD staff person is responsible for one or more types of school district records. These records might involve student information, employee information, purchasing, training, phone messages, meeting agendas, webpages… the list seems endless. Read on to learn about proper handling, storage, and destruction of districtrecords.

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. So, students under 13 can't make their own accounts, teachers must make the accounts for them. In making the accounts, teachers need to be aware of their responsibility under FERPA.
http://www.coppa.org/

(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

Gives parents and minor students' rights regarding surveys, collection and use of information for marketing purposes, and certain physical exams.
http://www2.ed.gov/policy/gen/guid/fpco/ppra/index.html

(HIPPA) 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/

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 is important for the following reasons:

- 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 considered safe storage practices:

- 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 network drive such as S:, or on a GCCISD database system. These files are securely stored and are safe for records 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 of 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. BUT - Please make this decision with care!

Email Retention

- GCCISD retains all incoming and outgoing email in either your Outlook account. A program is in place to permanently delete district email after 5 years.
- Most email does not have a long retention requirement.
- You may or may not have direct access to all 5 years of your email.
- If you receive or send email that contains the RECORD COPY of items that have a long retention requirement (more than 5 years), it will be necessary for you to store that email in another way.
- Printing the email and filing the paper copy OR scanning the copy or otherwise creating a pdf for filing on a network drive are the two options we suggest for keeping email long term.

Much of our school district business is conducted through email correspondence, and these emails are considered School District records. In order to adequately comply with most retention requirements, GCCISD maintains our email database for a period of 5 years. During that period, any email that you have created or received through the district's Microsoft Outlook system is retrievable.

Securing Electronic Data at Rest

- GCCISD servers offer end to end fault tolerance, ensuring all backups, updates, patches, are completed. Any sensitive information is stored with appropriate 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 computer systems or USB devices.

Securing Electronic Data in Transit

- Sensitive information can only be gathered from within our district or 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.

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:

1. Are record copies of an item listed on the District's retention schedule.

OR

2. Have personal identifiable information (PII).

Why dispose of records?

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

When to Destroy Records

Maintain a regular schedule. Don't wait until you run out of room but 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

The District is dedicated to preserving one of GCCISD's most valuable resource - records and information. Properly managed records can result in considerable cost-savings and operational efficiency. Campus Principals will maintain records for current students and the District Superintendent will maintain all other records.