Employee Data Privacy Handbook

GOOSE CREEK CONSOLIDATED INDEPENDENT SCHOOL DISTRICT

DATA PRIVACY is important to GCCISD because there are legal and ethical limitations on the collection, use, sharing, and handling of student information. Several federal and state laws regulate information that we collect on students, regardless of if it is kept on paper, on a school server or on an online website. As schools continue to increase the use of online resources, the amount of student information kept outside of our school walls is rising. Each one of these outsourced or online resources come with a contract, regardless of if it's just a "free" website. Schools, and staff, are legally and ethically required to keep student information private, regardless of where and how the student data is created, used, or stored.

Almost weekly, we hear news about a new data breach from a major store chain, bank or online reseller. Just as our consumer data is valuable and at risk of a data breach, our students' and staff's information is also vulnerable and must be protected. Our parents and community depend on us to keep their children's data private and safe. We must be sensitive to parents who may believe that too much data is being collected about their children. Others fear that student data may be breached and used inappropriately by companies for commercial gain.

This privacy guide will explore the most frequently asked questions regarding federal and state regulations, the use of online resources and established best practices adopted by districts to keep our student data safe.

What does data privacy mean?

Although there is not a unified definition of data privacy, the term is often used to describe the data we collect, why we collect it, what we do with it, as well as each person's rights around their own data. Data privacy is part of a comprehensive data governance program. However, it is important to know that data privacy is different from data security, which deals more with how we protect data and our technology from unauthorized access. We cannot have sound data security without data privacy and vice versa. Data privacy requires us to stop before sharing data and evaluate if we really need to collect that data, if we trust the source we are using for the collection or whom we are sharing information, and how we will protect the student and parent's rights around that data.

What federal laws do I need to know about?

There are three (3) major federal laws that impact the use of resources in schools. These include FERPA, PPRA, and COPPA.

- Family Education Rights & Privacy Act (FERPA) – a federal law that addresses the privacy of students' educational records and safeguards student privacy by limiting who may access student records as well as appropriate purposes for access. FERPA ensures that parents have the right to know what information is in their child's education record and gives parents the right to review, and correct, their student's education record. FERPA also protects student records from unauthorized disclosure, either intentionally or unintentionally, and requires written parental consent for disclosure. FERPA was most recently updated in 2011, and regulates how schools may, or may not, share data with vendors and others.
    - There are three important definitions under FERPA
        - Personally Identifiable Information (PII) – includes the name of a student or family member, address, personal identifiers (e.g. social security number), indirect identifiers (e.g. date of birth), and other information, alone or in combination, whereby a "reasonable person in the school community" could identify the student.
        - Education Records – materials that are "maintained by an educational agency or institution or by a person acting for such an agency or institution" and contain information directly related to a student.
        - Directory Information – Includes information generally not considered harmful or an invasion of privacy if released. This information is defined by the school via policy. For more information on directory information at Goose Creek CISD, see https://schools.gccisd.net/page/tms.cybersecurity?tab=Directory%20Information.
- Protection of Pupil Rights Amendment (PPRA) – sets rules that require schools to obtain parental consent before administering a survey, analysis, or evaluation that requires students to share certain types of sensitive information (below). The law also requires schools to provide parents access to instructional materials that are used in connection with the survey, analysis, or evaluation.
    - political affiliations of the student or the student's parent;
    - mental and psychological problems of the student or the student's parent;
    - sex behaviors and attitudes;
    - illegal, anti-social, self-incriminating, or demeaning behavior;

  - critical appraisals of individuals that have a close family relationship with the student;
  - legally privileged information, such as conversations with doctors, lawyers, or clergy;
  - religious practices, affiliations, or beliefs of the student or the student's parent; or
  - income (other than information required by law to determine eligibility for financial aid).

- Children's Online Privacy & Protection Act (COPPA) – regulates how commercial entities may collect and use information from children under age 13, this includes rules around parental consent. Although COPPA does not regulate schools, it does have major implications that impact the resources available for students under the age of 13. COPPA requires that operators of websites obtain permission from the parent or legal guardian before collecting personal information from children under the age of 13, and that they verify that the person providing permission is the parent or legal guardian.
  - The website operator may rely on the school to provide consent in lieu of the parent. However, even when policy allows for schools to consent on behalf of the parent, the school system cannot provide consent for commercial uses of the data; only the use of data for educational purposes. It is important to note that Personally Identifiable Information has a different definition under COPPA, and includes a screen name or username, persistent identifier (used in a web browser to track a user), photo, video or audio of child's voice or image, IP address and geolocation, information about parent collected online. In addition, compliance with COPPA does not ensure compliance with FERPA. Therefore, you should consult with your school before using any resource that requires COPPA compliance.

What about HIPAA and our students with medical needs?

This one gets a little more complicated. The Health Insurance Portability and Accountability Act (HIPAA) governs privacy and security of health information in certain kinds of health records. It's important that student health information maintained by most K-12 School Systems is usually not subject to HIPAA. The U.S. Department of Health and Human Services and the U.S. Department of Education's released joint guidance on the application of FERPA and HIPAA in 2008 that stated "a student's health records, including immunization records…as well as records maintained by a school nurse, are education records subject to FERPA", not HIPAA.

This ruling is because these records are generally directly related to the student and are maintained by the school for educational purposes and not for healthcare. That said, if your

school hires a healthcare provider to treat kids, those records may be subject to HIPAA. Regardless, it is important to ensure that the health information of your students is secure.

What about state laws?

Since 2013, there have been over 100 state laws passed around data privacy. Visit https://studentprivacycompass.org/state-laws/ for information about state laws.

What do our policies say?

Goose Creek CISD has several policies and internal documents regarding student data privacy.

- CQ – Technology Resources
  - Internet Safety: implement an internet safety plan that includes restricting unauthorized disclosure, use, and dissemination of personally identifiable information regarding students; and educating students about cyberbullying awareness and response and about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms.
- CQB – Technology Resources: Cybersecurity
  - Data Breach: shall disclose a breach involving sensitive, protected, or confidential student information as required by law
- FL – Student Records
  - The principal is custodian of all records for currently enrolled students. The superintendent is the custodian of records for students who have withdrawn or graduated.
- Data Governance Manual
  - You must report any security incident that could or has affected GCCISD data or resources.
  - Do not release student records or identifiable information

What about FERPA exceptions, can't we just use those to share information?

FERPA provides several exceptions to gaining parental consent prior to sharing student records. These exceptions include:

- to authorized School Officials with a legitimate educational interest

- to officials of another school system where a student is transferring
- to specified officials for audit or evaluation purposes
- to appropriate individuals for use in determining financial aid for a student
- to organizations conducting certain studies for or on behalf of the school
- to appropriate officials to comply with a judicial order or lawfully issued subpoena, perpetration of a crime, or disciplinary proceeding
- to appropriate officials in cases of emergency to protect the health and safety of the student or other individuals
- to state and local authorities, within a juvenile justice system, pursuant to specific state law
- to accrediting organizations

You may be surprised that these exceptions are very specific. When contracting with a service provider, schools typically use the School Officials exception. To accomplish this, the contract or agreement with the service provider must have specific language designating the provider as a School Official as well as detailing what data can be collected and how it will be used. The school must also ensure that they maintain control of all data, this is accomplished through the contract. It is important to note that directory information is not part of the FERPA exceptions as directory information is not considered a student record.

What if I only share directory information, is that allowed?

Technically, yes. However, it is important to really evaluate the service or website to ensure that directory information is the only information shared AND collected by the site. You may only share directory information, but the service provider may be collecting additional personally identifiable information or student data, such as progress towards mastery or student work. Once you evaluate a site/service, you will find that very few keep only directory information and do not create a student record.

"**Directory information**" is information that, if released, is generally not considered harmful or an invasion of privacy. Examples include:

- A student's photograph (for publication in the school yearbook);
- A student's name and grade level (for communicating class and teacher assignments);
- The name, weight, and height of an athlete (for publication in a school athletic program);
- A student's name and photograph (posted on a district-approved and managed social media platform); and
- The names and grade levels of students submitted by the district to a local newspaper or other community publication (to recognize the A/B honor roll for a specific grading period.)

The employee handbook dictates how and when directory information may be disclosed. In

addition, FERPA allows parents to opt out of schools sharing directory information. It is best practice to consult your supervisor prior to sharing directory information. For more information on GCCISD Directory Information please visit https://schools.gccisd.net/page/tms.cybersecurity?tab=Directory%20Information.

Don't we have the right to sign up for services on behalf of the parent?

Schools have certain authorities under the designation of "in locus parentis" (Latin for "in the place of a parent"), however this does not give a blanket right to sign up for any online services. When you click the "I accept" box on a website, that is considered a contract and is governed accordingly. Many schools have policies that govern who has the ability to sign a contract. At Goose Creek CISD, it is our practice that only the school board, superintendent, or superintendent's designee have this authority.

In addition, some terms of service and privacy policies have stipulations that prevent the use of the resource by students under the age of 13 or 18 or may require direct parental consent. Schools and/or teachers do not have the legal right to violate the stated contract terms. In addition, if a contract stipulates direct parental consent, then there are most likely data sharing conditions, such as commercial use of data, that require that consent. FERPA does not allow student data to be used for commercial purposes; therefore, when this condition is stated, the contract should be evaluated further.

Can I sign up for a site if I only share the students' initials or a number, not the students' names?

In short, NO. Many teachers may have the false belief that you only create a FERPA protected records when you use a student's full name; however, that is not the case. Any record that can be tied to a student and is maintained is protected. This includes records that may be assigned a random number (or any other identifier: word, color, etc.), use initials or a nickname, or uses any single sign on method such as signing in with their Google, Microsoft, or Classlink account. Educational records are often created on many online sites, free or paid, even if the information collected may or may not be used for grading; if it is tied directly to a student and tracked (for progress, completion, comprehension, etc.), it is considered an educational record, even if the teacher is the only one who knows who's who.

Why do we have a software approval process?

When using an online service provider, schools/districts must accept responsibility for

transferring a large amount of student (and/or staff) information to the provider. Schools/Districts must carefully vet the online provider to ensure that proper privacy protections are met. If student privacy requirements are not met, the online service could cause the school/district to not comply with federal regulations and privacy standards. To ensure compliance, schools/districts enter into contracts with every online service provider.

Each online resource comes with a contract, regardless of if it's just a "free" website, app, or browser extension. To ensure the privacy and security of data, the district also mandates that signed Data Privacy Agreements must be in place with any third-party that receives student (or staff) data. These are included within district purchasing agreements and administrative guidelines. This is required even if the third-party only collects directory information.

In addition to state requirements, FERPA affords parents the right to inspect educational records upon request. Without a process to identify all systems that collect and maintain student records, schools would not be able to fulfill this legal requirement.

What about iPad applications?

Unfortunately, iPad applications are not that simple. Many applications collect data while the student is using them. Some even require access to the user's Google Drive, Docs, email or other files/folders. Others will store copies of the user's work on their servers. All the information collected is tied to the student account logged in, potentially making it an educational record. All iPad applications should follow the same evaluation process as any other online resources.

What about browser extensions, those just use the browser, right?

Unfortunately, browser extensions are not that simple. Many extensions collect data while the student is using them. Some even require access to the user's Google Drive, Docs, email or other files/folders. Others will store copies of the user's work on their servers. All the information collected is tied to the student account logged in, potentially making it an educational record. Browser extensions should follow the same evaluation process as any other online resources.

I'm doing a research project for my continuing education; can I use the FERPA studies/research exception?

The FERRPA studies exception is often misrepresented. It is important to note that there is not a research exception. FERPA does allow an exception for studies that are "for, or on behalf of" educational agencies or institutions. These studies can only be for the purpose of developing, validating, or administering predictive tests; administering student aid programs; or improving

instruction. There are no other allowed studies under the exception. There is also a requirement for a written agreement that must have several provisions to protect the student data used for the study. It is important to reiterate that the study must be "for, or on behalf" of the school/district; this does not allow for independent researchers, including post-graduate students, that are not conducting research directly for the school. If an independent researcher requests information, that information can only be shared with direct parental consent, the directory information exception or if all student identifiers are removed and the data is de-identified.

Since FERPA applies to all student data, does all this mean that I can't even post student work on my wall?

It depends, if your school/district lists student work on display as part of directory information and the work does not have a score/grade, you can put it on display.

Parents do have the right to opt out of having their student's directory information shared. It is important to check to see if any of your students have been opted out. In order to verify this information, check the directory information resource page for directions on running this report at https://schools.gccisd.net/page/tms.cybersecurity?tab=Directory%20Information.

Can I post photos of my classroom and students on social media?

Most schools have policies that allow for the use of student photos; typically, this is through directory information. It is also important to distinguish between district and personal social media accounts. School/district staff should never post identifiable photos of students or student work on a personal account.

Goose Creek CISD's directory release covers the use of photos on district approved social media. Therefore, a teacher cannot post student photos on their personal social media account. Please ask your building administration if your school has an approved social media account to post student photos.