to a child's mental, emotional, or physical welfare as well as a failure to make a reasonable effort to prevent sexual conduct with a child. Maltreatment is defined as abuse or neglect. Anyone who has reasonable cause to believe that a child has been or may be abused or neglected has a legal responsibility under state law for reporting the suspected abuse or neglect following the procedures described above in *Reporting Suspected Child Abuse*.

Reporting Crime

Policy DG

The Texas Whistleblower Act protects district employees who make good faith reports of violations of law by the district to an appropriate law enforcement authority. The district is prohibited from suspending, terminating the employment of, or taking other adverse personnel action against, an employee who makes a report under the Act. State law also provides employees with the right to report a crime witnessed at the school to any peace officer with authority to investigate the crime.

Scope and Sequence

Policy DG

If a teacher determines that students need more or less time in a specific area to demonstrate proficiency in the Texas Essential Knowledge and Skills (TEKS) for that subject and grade level, the district will not penalize the teacher for not following the district's scope and sequence.

The district may take appropriate action if a teacher does not follow the district's scope and sequence based on documented evidence of a deficiency in classroom instruction. This documentation can be obtained through observation or substantiated and documented third-party information.

Technology Resources

Policy CQ

Goose Creek CISD allows certain employees to utilize different District-owned technology resources (computers, laptops, tablets, cell phones, networks, e-mail accounts, cloud storage, devices connected to GCCISD networks, all district-owned devices used on or off school property, etc.). Use of a District-owned technology resources is a privilege, not a right and are primarily for administrative and instructional purposes. With this privilege comes responsibility. Participating employees are responsible at all times for the proper use of the technology resources and are required to abide by the provisions of the acceptable use agreement and administrative procedures. Failure to comply with the guidelines set forth may result in suspension of access, termination of privileges, and may lead to disciplinary and/or legal action. Limited personal use is permitted if the use:

- Imposes no tangible cost to the district.
- Does not unduly burden the district's technology resources.
- Has no adverse effect on job performance or on a student's academic performance.
- Has no commercial purpose; and
- Is limited in the same manner as Personal Use of Electronic Communications. An employee shall not use technology resources for personal use while assigned to other duties.

Any user identified as a security risk, as having improperly used District technology resources, or as having violated District and/or campus acceptable use policies or administrative regulations may be denied access to District technology resources.

The Superintendent or designee shall develop and implement administrative regulations, guidelines, and user agreements consistent with the purposes and mission of the District and with law and policy.

Networked communication systems such as ParentSquare, Instant Messaging, Online Chat, Video Conferencing and Web-exing, are real-time network communication systems and are primarily available for instructional and administrative purposes. Information shared using these systems should be transitory in nature, as documented under Email Retention Transitory Information 1.1.057.

Use of any Districts technology resources shall not be considered confidential or private (including but not limited to e-mails, direct messaging, text messages, locally stored files, cloud stored files, etc). Designated District staff shall be authorized to monitor the District's technology resources at any time to ensure appropriate use.

1. Employees are responsible for the content stored on the technology device. Users may download personal content to the device as long as it meets the expectations set forth in Board Policy, Employee Handbook, Administrative Guidelines and other legal or district requirements. Any personal content on District technology resources shall not be considered private and may be monitored or accessed to ensure appropriate use of the device(s).

2. The technology device must be secured with a passcode/password at all times. Incidents or suspected incidents of unauthorized access and/or disclosure of confidential data are to be immediately reported to the campus principal or immediate supervisor and the Technology Department.

3. Goose Creek CISD reserves the right to remotely wipe, without notice, all data from the technology device if confidential data is suspected to be at risk of disclosure, the Operating System is suspected to have been breached, or a violation of Board Policy or the Employee Handbook. Costs incurred by an employee for personal content on the District device will not

be recoverable. For example: if an App is downloaded that is determined to contain inappropriate content (sexually explicit, obscene, etc.) and the device is wiped/reset, the employee will not be reimbursed for any personal purchased App.

4. Users will not change or remove (or attempt to change or remove) security features on the technology device. “Jailbreaking” is not allowed.

5. Users must take reasonable measures to safeguard the device from damage, loss or theft such as using the district provided protective case. Users must immediately report damage, loss, or theft of the technology device to the campus principal or immediate supervisor and file a police report where appropriate. Users are responsible for the cost of replacing lost or damaged technology resources and associated accessories, such as power cords.

6. When requested by the District, or upon separation of employment, the participating employee agrees to return the technology device, case, charger, and any other District- issued accessories to their campus principal or immediate supervisor in the same condition it was issued, less reasonable wear.

7. If a user fails to return the technology device, case, charger, and any other accessories upon request or upon separation from employment, the employee hereby consents to the District deducting from his or her final paycheck the cost of replacing the technology resource and related accessories. As a means of reference, as of June 2021, iPad cost is $319.00, power adaptor and cable are $35.00, and case is $57.55. This cost is subject to change as equipment costs change.

8. The assigned technology device remains the property of Goose Creek CISD at all times, including while being used or possessed by the participating employee. This includes any technology items that may have been purchased through grants, donations, sponsorships, gifts, or other District-related activities, such as Classwish.org, Donorpages.com, or Donorschoose.org.

9. If a user is issued a district cell phone, the phone must be turned on and kept with you at all times when on duty or on call. Otherwise, the device must be securely stored.

Employees are required to abide by the provisions of the district’s acceptable use agreement and administrative procedures. Failure to do so can result in suspension of access or termination of privileges and may lead to disciplinary and/or legal action. Employees with questions about computer use and data management can contact the Technology Department.

Staff Request for Approval of Technology Resources

Before use in the classroom, use with students, or administrative use, all instructional programs and applications requiring the user to accept terms of service, or a user agreement must be approved by the Technology Department. This includes online learning resources, online applications, digital subscription services, and other programs or technology applications.

To request to use an instructional program or application, staff must complete and submit the Instructional Program/App Request Form. Software applications must not conduct mental health assessments or other assessments unrelated to educational curricula that are intended to collect information about students without direct and informed parental (or person standing in parental relation) consent.

User Responsibility

The individual in whose name a system account is issued will be responsible at all times for its proper use. If inappropriate use or activity is witnessed, it should be reported to a supervisor. User accounts and passwords are not to be shared or disclosed to any other individual. Inappropriate use of personal computing and electronic communication may result in disciplinary action, up to and including termination of employment.

District computers will provide a best effort at filtering access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act and as determined by the Superintendent or designee.

Concerns and complaints regarding student use of technology resources, including cybersecurity and online safety concerns should be directed to the Campus Administration. Campus administrative staff must be notified of any activity that poses a risk to student safety. If it is deemed necessary to deactivate the student's technology resource as a result of this activity, campus administrative staff will contact the Technology Department for assistance.

Technology staff shall assist campus administration with reviewing and providing relevant data when an investigation is opened in regards to internet activity and student safety. Technology staff shall deactivate a student's technology resource if campus administration has contacted the Technology Department and deemed the deactivation necessary for student safety. The technology resource shall stay deactivated until campus administration approves it to be reactivated.

Staff should consider necessary adjustments, by age level, to the use of electronic devices in the classroom to foster development of students' abilities regarding spending school time and completing assignments without the use of an electronic device.

Staff should consider appropriate restrictions on student access to social media websites or applications. ParentSquare should be utilized over other social media tools. Student interaction should be on ParentSquare instead of Facebook, Instagram, twitter, etc. Social media tools should be used for broad communication to the public as a whole and not for student educational purposes. Please see CIPA for further details.

Campus Administration is required to notify the student's parent or person standing in parental relation, if a student accesses inappropriate or concerning content, including, but not limited to, content related to: self-harm, suicide, violence to others, or illicit drugs. When a student accesses content involving harmful, threatening, or violent behavior, the school system must follow established suicide prevention programs, intervention policies and procedures, and make appropriate notifications to the Safe and Supportive Schools Program Team established under Texas Education Code, Section §37.115, as applicable.

Business Use of Electronic Media

If an employee adds a picture to District electronic media, the picture must be a professional photo of the employee.

Do not put anything in an e-mail or electronic communication that you would not want published in a public document.

E-mail or electronic communications pertaining to official business carried out on a home computer or personal device may be —public information.

Use the Family Educational Rights and Privacy Act (FERPA) guidelines in determining the definition of confidential records.

Social Media: Employees shall not use scheduled work time to engage in social media activity that is not job related. Employees may not use District resources to access personal social media platforms of students or other staff members.

When authorized to discuss GCCISD or GCCISD-related matters, employees are required to identify themselves, the campus or department they are representing, and state their job assignment. Employees may not publish confidential information on social media sites. Employees are personally responsible for the content they publish on blogs, wikis, or any other form of user-generated media.

Employees shall not use personal electronic communications devices to give the impression that they are representing, giving opinions, or otherwise making statements on behalf of GCCISD unless appropriately authorized to do so.

Personal Use of Electronic Communications

Policy CQ, DH

Electronic communications include all forms of social media, such as text messaging, instant messaging, electronic mail (email), web logs (blogs), wikis, electronic forums (chat rooms), video-sharing websites (e.g., YouTube), editorial comments posted on the Internet, and social network sites (e.g., Facebook, Twitter, LinkedIn, Instagram). Electronic communications also

include all forms of telecommunication such as landlines, cell phones, and web-based applications.

While operating District-owned vehicles or power equipment, employees may not use personal electronic communication devices.

As role models for the district's students, employees are responsible for their public conduct even when they are not acting as district employees. Employees will be held to the same professional standards in their public use of electronic communications as they are for any other public conduct. If an employee's use of electronic communications violates state or federal law or interferes with the employee's ability to effectively perform his or her job duties, the employee is subject to disciplinary action, up to and including termination of employment. If an employee wishes to use a social network site or similar media for personal purposes, the employee is responsible for the content on the employee's page, including content added by the employee, the employee's friends, or members of the public who can access the employee's page, and for web links on the employee's page. The employee is also responsible for maintaining privacy settings appropriate to the content.

An employee who uses electronic communications for personal purposes shall observe the following:

- The employee may not set up or update the employee's personal social network page(s) using the district's computers, network, or equipment.

- The employee shall limit use of personal electronic communication devices to send or receive calls, text messages, pictures, and videos to breaks, mealtimes, and before and after scheduled work hours, unless there is an emergency, or the use is authorized by a supervisor to conduct district business.

- The employee shall not use the district's logo or other copyrighted material of the district without express written consent.

- An employee may not share or post, in any format, information, videos, or pictures obtained while on duty or on district business unless the employee first obtains written approval from the employee's immediate supervisor. Employees should be cognizant that they have access to information and images that, if transmitted to the public, could violate privacy concerns.

- The employee continues to be subject to applicable state and federal laws, local policies, administrative regulations, and the Texas Educators' Code of Ethics, even when communicating regarding personal and private matters, regardless of whether the employee is using private or public equipment, on or off campus. These restrictions include:

    - Confidentiality of student records. [See Policy FL]

- Confidentiality of health or personnel information concerning colleagues, unless disclosure serves lawful professional purposes or is required by law. [See DH(EXHIBIT)]

- Confidentiality of district records, including educator evaluations and private email addresses. [See Policy GBA]

- Copyright law [See Policy CY]

- Prohibition against harming others by knowingly making false statements about a colleague or the school system. [See DH(EXHIBIT)]

See *Electronic Communications between Employees, Students, and Parents,* below, for regulations on employee communication with students through electronic media.

Personal Devices on District Networks

Connecting to the District's wireless network with personal technology devices, such as laptops and tablets is allowed only for educational purposes and with the Principal and or Supervisor's approval. The district's technology staff will not be allowed to work on personal equipment. Using broadband Internet service or any other ability to connect to the Internet outside of the district's internet filtering or wide area network is prohibited. Teachers and staff must use the district's visitor wireless network and abide by all guidelines included in this handbook.

Data Privacy and Information Security

Employees play an important role in keeping Goose Creek CISD's sensitive information secure. Many employees may come into contact with sensitive information on a daily basis. Examples of "sensitive information" at Goose Creek CISD include:

- addresses;
- dates of birth;
- bank account/routing numbers;
- phone numbers;
- social security numbers;
- driver's license numbers;
- medical records and personnel records of employees/students;
- student grades/work;
- student discipline information and;
- any financial information.

The Family Educational Rights and Privacy Act, or FERPA, permits the district to disclose appropriately designated "directory information" from a student's education records without written consent.

"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.)

GCCISD adheres to standards outlined in Texas Education Code Chapter §32 and will minimize data collected on students through all means available.

Employees have a duty to protect the district and keep sensitive information safe. Failure to do so could result in disclosure of student data (whether intentional or unintentional) or a data breach. In reference to FERPA, privacy and data security:

- Users will not disclose or transmit GCCISD confidential or sensitive data on social media, personal email, personal instant messaging, etc.
- Users will not attempt to access or alter any information that they are not authorized to access.
- All users will report to the Technology Helpdesk, unnecessary access to GCCISD Information Systems if the access is not required for their duties (e.g., inadvertent access that has been provisioned but is not necessary).
- Users will not disclose GCCISD information to others without a valid need to know.
- Users will not disclose GCCISD information to Artificial Intelligence sites or other similar websites, as that data could potentially be stored, sold or used without the consent of GCCISD, students, or parents.
- Users will not post on social media examples of student work, grades or other confidential information as designated by the Family Educational Rights and Privacy act (FERPA) unless prior consent has been given by the parent/guardian in the Release of Student Directory Information during online registration.
- For documented and approved transfer/storage of confidential or sensitive information:
- Users will ensure that any GCCISD confidential or sensitive information stored in any location uses approved disk encryption.
- Users will utilize approved encryption for transmitting GCCISD confidential or sensitive data via email or other file transfer methods including (SFTP, secure copying, API integrations, etc.)

Vetting Third-Party Services and Applications

Goose Creek CISD uses online services and integrations with third-party systems as part of its daily operations. Each of these systems must be vetted for data privacy and security prior to being utilized. It is the responsibility of every district employee to ensure that a system is vetted prior to being utilized and complies with Texas Education Code Chapter 32, Subchapter D. This includes mobile apps, computer programs, online services, etc. that may have access to district data. Before utilizing a third-party service or application, a third-party risk rating must be

conducted, and a Data Privacy Agreement signed. Any concerns that arise from the risk rating or DPA will then be addressed with the third-party to try and resolve them. Any remaining risk or concerns that cannot be resolved must be approved by the Superintendent before use. For more information on getting a third party vetted, contact the Technology Department.

Guidelines for keeping this information secure are:

Make sure sensitive information is physically secure.

- Lock up or password protect documents containing sensitive information when not using them. This includes employee information and any student information.
- Shield information from view when others (non-authorized people) are near.
- Lock cabinets or computer screens before walking away.
- Don't leave sensitive items like employee records or student information on desks or in unlocked cabinets.
- Keep mobile devices (laptops, smartphones, tablets, USB drives, etc.) either within your sight or locked up at all times. Use password protection and auto lock screens to further protect these devices.

Manage your passwords.

- Use strong passwords on systems that contain sensitive information: mix 8 or more (12 is recommended) upper and lower case letters, numbers, and special characters, longer is better and is harder for others to guess.
- Do not reuse passwords on different accounts. Note: Goose Creek CISD does use Single-Sign On integrations between many systems. This is not password re-use as it is still using a single authentication credential.
- Do not use your district password on ANY non-district account.
- Do not share passwords with others.

Understand data privacy security to protect student and employee data.

- FERPA – The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy of student education records. FERPA requires staff to take reasonable steps to protect student records and information. Under FERPA, parents and eligible students may inspect, review, and request to amend education records. Some best practices include verbally discussing student information rather than sending student data via email and checking with the Technology Department to ensure software and websites are properly vetted before allowing students to use them. More information can be found at https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html or by calling 1-800-USA-LEARN

- COPPA – Children's Online Privacy Protection ACT (COPPA) imposes certain requirements on operators of websites or online services directed to children under 13

years of age. Employees can help ensure compliance with COPPA by understanding what data is collected by a website or application, and ensuring the websites or applications are properly vetted by the Technology Department before allowing students to use them. More information can be found at: http://www.coppa.org/coppa.htm.

- CIPA – The Children's Internet Protection Act (CIPA) was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the internet. CIPA requires that districts have an internet safety policy that includes technology protection measures which block or filter internet access (on computers used by minors) to pictures that are (a) obscene; (b) child pornography; or (c) harmful to minors. Internet safety policies must include monitoring the online activities of minors, and as required by the Protecting Children in the 21st Century Act.1), must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms; and cyberbullying awareness and response. More information can be found at: https://www.fcc.gov/consumers/guides/childrens-internet-protection-act.

- PPRA - The Protection of Pupil Rights Amendment (PPRA) is a federal law that requires schools to obtain written consent from parents before minor students are required to participate in any U.S. Dept. of Education funded survey, analysis, or evaluation that reveals information concerning the following areas: political affiliations; mental and psychological problems potentially embarrassing to the student and his/her family; sex behavior and attitudes; illegal, anti-social, self-incriminating and demeaning behavior; critical appraisals of other individuals with whom respondents have close family relationships; legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers; religious practices, affiliations, or beliefs of the student or student's parent; or income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program.) More information can be found at: https://studentprivacy.ed.gov/content/ppra

Guard against social engineering attacks (such as phishing).

- Carefully review links and attachments in emails before clicking or opening.
- Use bookmarks to safely return to sites visited frequently. Use browser functions that warn of sites with poor reputations.
- Be careful of all requests for sensitive information, whether by e-mail, phone, text message, or in person.
- Independently verify the identity and authority of any requester with your supervisor or a Technology staff member before disclosing sensitive information.

Avoid unsecure networks outside the office.

- Don't connect to the office emails or systems from public Wi-Fi.

- If connecting while traveling or working from home, have the Technology Department set you up properly with secure remote access.

Securely destroy sensitive information when no longer needed.

- Secure shredding is the preferred disposal method of hard copy documents with sensitive information.
- Destruction of electronic data should be done according to the Technology Department's Data Destruction Guidelines.

Immediately report suspected information security events to the Technology Helpdesk at 281-420-4633 or helpdesk@gccisd.net.

Questions regarding Information Security and Data Privacy may be addressed to the Technology Helpdesk.

Data Incident Reporting (Privacy or Security)

Policy CQB

Any user that becomes aware of a possible data breach/disclosure, indicators of data or technology resource(s) compromise, or any other cybersecurity concerns must notify the Technology Helpdesk so the issues can be documented and investigated according to the Technology Incident Response Plan.
Upon discovering or receiving notification of a breach of system security, the District cybersecurity coordinator shall disclose the breach to affected persons or entities in accordance with the timeframes established by law.
The District shall give notice by using one or more of the following methods:

- Written notice.
- Electronic mail, if the District has electronic mail addresses for the affected persons.
- Clear posting on the District's website.
- Publication through broadcast media.

Data Retention and Records Management

Policy CPC

A District employee must make provisions to retain documents and messages in accordance with the district's records retention policy, CPC Legal and Local. Each user is responsible for using the proper records retention practices.

Each individual employee who creates and maintains electronically stored information (ESI), is responsible for determining the retention of the ESI and maintaining it in compliance with District, state, and federal records retention requirements.

In the event the ESI was not created by a District employee, then the employee who received the ESI or responded to the ESI will be responsible for its retention and maintenance. The

Technology Department will consider e-mail as administrative correspondence and will, therefore, maintain retention according to the state control schedule.

The individual who creates and maintains ESI or who received or responded to ESI may delete or erase the ESI when it is no longer required to be maintained in connection with a claim or pursuant to District, state, or federal records retention requirements.

For more information, please visit Texas State Library and Archives Commission Records Control Schedules Administrative (GR Schedule): https://www.tsl.texas.gov/slrm/recordspubs/gr.html

The district's email system is a communication system and is not intended to be the primary records retention repository.

- The retention requirement associated with any document is determined by its content, not the method of delivery.
- The responsibility of retaining an internally created and distributed document (or message) most often falls on the author – not the recipients.
- Employees who receive messages from outside the district are responsible for proper records retention of those messages.
- Email that has been requested in a subpoena or public information request must be retained until the request has been addressed, even if the retention period has expired.

The content and function of an email message determines the retention period for that message. All emails sent or received by an agency is considered a state record. Therefore, all email messages must be retained or disposed of according to the agency's retention schedule. Email systems must meet the retention requirements found in Texas Administrative Code 6.94(e).
Email generally falls into several common record series categories. These are:

1. Administrative Correspondence. 1.1.007 – Incoming/outgoing and internal correspondence, in any format pertaining to the formulation, planning, implementation, interpretation, modification, or redefinition of the programs, services, or projects of any agency and the administrative regulations, policies and standards that govern them. Subject to archival review. Retention: 3 years.

2. General Correspondence. 1.1.008 – Non-administrative incoming/outgoing and internal correspondence, in any media, pertaining to or arising from the routine operations of the policies, programs, services, or projects of an agency. Retention: 1 year.

3. Transitory Information. 1.1.057 – Records of temporary usefulness that are not as integral part of a records series of an agency, that are not regularly filed within as agency's recordkeeping system, and that are required only for a limited period of time for the completion of an action by an official or employee of the agency or in the preparation of an on-

going records series. Transitory records are not essential to the fulfillment of statutory obligations or to the documentation of agency functions. Examples of transitory information are routine messages such as internal meeting notices, routine slips, incoming letters that add nothing of substance to enclosures; and similar routine information used for communication, but not for the documentation, of a specific agency transaction. Retention: After the purpose of record has been fulfilled.

Sensitive Information Storage on Devices

Employees will not download, save, copy (including Google Takeout), or export any sensitive information, PII (personally identifiable information) of staff/students, or other resources out of any GCCISD computer system unless it is completely necessary and with the Principal or immediate supervisors' approval. Sensitive information will not be emailed or saved to portable storage devices such as cd/dvd, portable flash drives, etc or copied to cloud service providers such as dropbox.com, box.com, etc. Sensitive information on a district laptop or tablet must be encrypted to prevent information theft. It is the user's responsibility to immediately notify the district's technology department if any sensitive information is lost or stolen.

As part of the District's Information Security Guidelines, data stored on district resources are subject to auditing and/or monitoring to ensure compliance. Employees found storing sensitive data without appropriate approval and without appropriate encryption/security controls may face disciplinary action, up to and including termination of employment.

Electronic Communications between Employees, Students, and Parents

Policy DH

A certified or licensed employee, or any other employee designated in writing by the superintendent or a campus principal, may use electronic communications with students who are currently enrolled in the district. The employee must comply with the provisions outlined below. Parent Square is the official communication tool that is permitted for staff when communicating with students and parents. ParentSquare should be utilized over other social media tools. Student interaction should be on ParentSquare instead of Facebook, Instagram, twitter, etc. Social media tools should be used for broad communication to the public as a whole and not for student educational purposes. Electronic communications between all other employees and students who are enrolled in the district are prohibited. Employees are not required to provide students with their personal phone number or email address. An employee shall notify his/her supervisor when a student engages in improper electronic communication with the employee.

An employee is not subject to the provisions regarding electronic communications with a student to the extent the employee has a social or family relationship with a student. For

example, an employee may have a relationship with a niece or nephew, a student who is the child of an adult friend, a student who is a friend of the employee's child, or a member or participant in the same civic, social, recreational, or religious organization. An employee who claims an exception based on a social relationship shall provide written consent from the student's parent. The written consent shall include an acknowledgement by the parent that:

- The employee has provided the parent with a copy of this protocol;
- The employee and the student have a social relationship outside of school;
- The parent understands that the employee's communications with the student are excepted from district regulation; and
- The parent is solely responsible for monitoring electronic communications between the employee and the student.

The following definitions apply for the use of electronic media with students:

- *Electronic communications* means any communication facilitated by the use of any electronic device, including a telephone, cellular telephone, computer, computer network, personal data assistant, or pager. The term includes email, text messages, instant messages, and any communication made through an Internet website, including a social media website or a social networking website.
- *Communicate* means to convey information and includes a one-way communication as well as a dialogue between two or more people. A public communication by an employee that is not targeted at students (e.g., a posting on the employee's personal social network page or a blog) is not a *communication*: however, the employee may be subject to district regulations on personal electronic communications. See *Personal Use of Electronic Media*, above. Unsolicited contact from a student through electronic means is not a *communication*.
- *Certified or licensed employee* means a person employed in a position requiring SBEC certification or a professional license, and whose job duties may require the employee to communicate electronically with students. The term includes classroom teachers, counselors, principals, librarians, paraprofessionals, nurses, educational diagnosticians, licensed therapists, and athletic trainers.

An employee who communicates electronically with students shall observe the following:

- The employee is prohibited from knowingly communicating with students using any form of electronic communications, including mobile and web applications, that are not provided or accessible by the district unless a specific exception is noted below.

- Only a teacher, trainer, or other employee who has an extracurricular duty may use text messaging, and then only to communicate with students who participate in the extracurricular activity over which the employee has responsibility. An employee who communicates with a student using text messaging shall comply with the following protocol:

    - The employee shall include at least one of the student's parents or guardians as a recipient on each text message to the student so that the student and parent receive the same message;

    - The employee shall include his or her immediate supervisor as a recipient on each text message to the student so that the student and supervisor receive the same message;

    - For each text message addressed to one or more students, the employee shall send a copy of the text message to the employee's district email address.

- The employee shall limit communications to matters within the scope of the employee's professional responsibilities (e.g., for classroom teachers, matters relating to class work, homework, and tests; for an employee with an extracurricular duty, matters relating to the extracurricular activity).

- The employee is prohibited from knowingly communicating with students through a personal social network page; the employee must create a separate social network page ("professional page") for the purpose of communicating with students. The employee must enable administration and parents to access the employee's professional page.

- The employee shall not communicate directly with any student between the hours of 9 p.m. and 5 a.m. An employee may, however, make public posts to a social network site, blog, or similar application at any time.

- The employee does not have a right to privacy with respect to communications with students and parents.

- The employee continues to be subject to applicable state and federal laws, local policies, administrative regulations, and the Texas Educators' Code of Ethics including:

    - Compliance with the Public Information Act and the Family Educational Rights and Privacy Act (FERPA), including retention and confidentiality of student records. [See Policies CPC and FL]

    - Copyright law [Policy CY]

    - Prohibitions against soliciting or engaging in sexual conduct or a romantic relationship with a student. [See Policy DH]

- Upon request from administration, an employee will provide the phone number(s), social network site(s), or other information regarding the method(s) of electronic media the employee uses to communicate with one or more currently-enrolled students.

- Upon written request from a parent or student, the employee shall discontinue communicating with the student through email, text messaging, instant messaging, or any other form of one-to-one communication.

- An employee may request an exception from one or more of the limitations above by submitting a written request to his or her immediate supervisor.

- All staff are required to use school email accounts for all electronic communications with parents. Communication about school issues through personal email accounts or text messages are not allowed as they cannot be preserved in accordance with the district's record retention policy.

- An employee shall notify his or her supervisor in writing within one business day if a student engages in an improper electronic communication with the employee. The employee should describe the form and content of the electronic communication.

Public Information on Private Devices

Policy DH, GB

Employees should not maintain district information on privately owned devices or cloud storage. Any district information must be forwarded or transferred to the district to be preserved. The district will take reasonable efforts to obtain public information in compliance with the Public Information Act. Reasonable efforts may include:

- Verbal or written directive

- Remote access to district-owned devices and services

Guidelines for Use of Artificial Intelligence

Artificial intelligence (AI) refers to computer applications or programs that are capable of reasoning, decision-making, and solving problems. These applications or programs mimic the way the human brain learns by processing massive amounts of training data, and then using what it "learns" to generate an output that best answers the prompt that it is given.

Goose Creek CISD commits to embracing the transformative potential of AI in education, aligning our approach with our vision and core values of integrity, inclusivity, innovation, and individuality. We are committed to empowering every student with knowledge and skills they need to succeed in a global community, including the use of advanced and evolving technology, such as AI.

As we navigate the evolving landscape of AI in education, Goose Creek CISD will continuously engage with the latest research, collaborate with stakeholders, and adapt our strategies to ensure that our integration of AI aligns with our mission to provide a comprehensive and inclusive educational experience for all. We endorse a human-centered strategy in employing AI, which fosters a learning environment where technology serves to enrich our human qualities, not diminish them.

Guiding Principles:

Professional Responsibility: All employees are expected to engage with AI technologies responsibly, ensuring their use enhances educational outcomes and adheres to our district's ethical standards. AI systems have the potential to produce biased or incorrect content. It’s crucial for employees to check for accuracy before sharing with others.

AI Literacy and Professional Development: We recognize the importance of equipping our students and staff with the necessary skills to understand, interact with, and ethically use AI technologies. This will include instructional lessons and professional development opportunities. Our commitment to AI literacy is integral to our mission of providing a high-quality, future-ready education.

Enhancing Teaching and Learning: Embracing our core value of inclusivity, we pledge to use AI as a tool to foster equitable educational opportunities. We will leverage AI to augment the educational experience, supporting teachers to enhance their instructional strategies and enabling students to achieve personalized learning outcomes. Our goal is to eliminate barriers and create learning experiences that cater to the diverse needs of every student, ensuring no one is left behind in the digital revolution.

Data Privacy: Employees must rigorously uphold our district's data privacy protocols when using AI technologies. The privacy and security of student and staff data are paramount, and any AI tools employed must comply with our stringent data protection policies. When using any AI language model (ChatGPT, MagicSchool, etc.), student work and student/parent/employee personal information (PI) such as the following should NOT be entered/uploaded:

Name, Address, Email address, Phone number, Social Security number, Date of birth, ID Number, Photos, videos, or audio recordings, or any other information that could be used to identify yourself or others.

Computer Software Policy

It is the practice of the district to respect all computer software copyrights and to adhere to the terms of all software licenses to which the district is a party. Technology Department is charged with the responsibility of enforcing these guidelines.

All computer software installed on district equipment must be vetted by, purchased, reported to and installed by Technology Department, or its designee. Software acquisition is restricted to ensure that the school district has a complete record of all software that has been purchased

for district computers and can register, support, and upgrade such software accordingly. Additionally, software used on district computers used for instructional purposes must also be vetted by a district curriculum coordinator.

Students, district employees, and volunteers may not duplicate any licensed software or related documentation for use either on the district's premises or elsewhere unless Technology Department is expressly authorized to do so by agreement with the licenser. Unauthorized duplication of software may subject the employee and/or the school district to both civil and criminal penalties under the United States Copyright Act.

Students, district employees, and volunteers may not give software to any third-party including relatives, clients, contractors, etc. District employees, students, and volunteers may use district approved software on local area networks or on multiple machines only in accordance with applicable license agreements.

For further information regarding the purchase and installation of computer software, please call the Technology Helpdesk at 281-420-4633 or helpdesk@gccisd.net.

Intellectual Property Rights

Policy CY

As agents of the District, employees shall have limited rights to work they create using the District's electronic communications system. The District shall retain the right to use any product created in the scope of a person's employment even when the author is no longer an employee of the District.

Recordings in the Workplace

School employees are prohibited from making video or audio recordings of students, unless they have the advance permission of the campus administrator to do so for a permissible reason.

While this is not illegal to secretly record workplace discussions or meetings with adults, the district prohibits this practice unless the employee has the advance consent of the other(s) who are present and/or being recorded. Because it is unprofessional and disruptive to district operations, the Texas Commissioner of Education has stated that secretly recording such conversations may be good cause for termination of employment.

Use of Security Cameras

Policy CK

The District utilizes security cameras and video recording devices at the school campuses and other District facilities. These are located in cafeterias, hallways, classrooms, designated areas, entryways, buses, and parking areas. Information provided by reviewing the videotapes will be utilized, as needed, to help maintain a safe and orderly environment. The District may view

recordings to aid in the investigation of employee misconduct and violations of Board Policy, Employee Handbook, Administrative Guidelines and other legal or district requirements.

Disclaimer of Liability

The District shall not be liable for user's inappropriate use of electronic communication resources or violations of copyright restrictions or other laws, users' mistakes or negligence, and costs incurred by users. The District shall not be responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the internet.

These guidelines apply to stand-alone computers as well as computers connected to the Network/Internet. The district makes no warranties of any kind, whether expressed or implied, for the services it is providing and is not responsible for any damages suffered by users. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its negligence or user errors or omissions. The district is not responsible for phone/credit card bills or any other charges incurred by users. Use of any information obtained via the Network/Internet is at the user's own risk. The district specifically denies any responsibility for the accuracy or quality of information obtained through its services. Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the providers and not the district. The district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the district's electronic communications system.

Criminal History Background Checks

Policy DBAA

Employees may be subject to a review of their criminal history record information at any time during employment. National criminal history checks based on an individual's fingerprints, photo, and other identification will be conducted on certain employees and entered into the Texas Department of Public Safety (DPS) Clearinghouse. This database provides the district and SBEC with access to an employee's current national criminal history and updates to the employee's subsequent criminal history.

Employee Arrests and Convictions

Policy DH, DHB, DHC

An employee must notify his or her principal or immediate supervisor within three calendar days of any arrest, indictment, conviction, no contest or guilty plea, or other adjudication of any felony, and any of the other offenses listed below:

- Crimes involving school property or funds.