Computer/Network/Internet Acceptable Use Agreement

Galveston Independent School District makes a variety of communications and information technologies available to students and District employees through computer/network/Internet access. These technologies, when properly used, promote educational excellence in the District by facilitating resource sharing, innovation, and communication within the District. Illegal, unethical or inappropriate use of these technologies can have dramatic consequences, harming the District, its students and its employees. These Acceptable Use Guidelines are intended to minimize the likelihood of such harm by educating District students and employees and setting standards which will serve to protect the District. The District firmly believes that the valuable information and interaction available on the computer/network/Internet far outweighs the possibility that users may procure material that is not consistent with the District's educational goals.

Mandatory Review. To educate District employees and students on proper computer/network/ Internet use and conduct, users are required to review these guidelines at the beginning of each school year. All District employees shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines. The parent or legal guardian of a student user is required to acknowledge receipt and understanding of Acceptable Use Guidelines as part of their review of the *Discipline Management Plan and Student Code of Conduct* handbook. Employees supervising students who use the District's system must provide training emphasizing its appropriate use.

Definition of District Technology System. The District's computer systems and networks (system) are any configuration of hardware and software. The system includes but is not limited to the following:

- Telephones, cellular telephones, pagers and voicemail facilities;
- Electronic mail (e-mail) accounts;
- Fax machines;
- Servers;
- Computer hardware and peripherals;
- Software including operating system software and application software;
- Digitized information including stored text, data files, e-mail, digital images and audio files;
- Internally accessed databases or tools;
- Externally accessed databases (such as the Internet);
- iPads, iPods and similar tablet devices
- Web domains, hosting and content
- New technologies as they become available

Availability of Access

Acceptable Use. Computer/Network/Internet access will be used to improve learning and teaching consistent with the District's educational goals. The District requires legal, ethical and appropriate computer/network/Internet use.

Privilege. Access to the District's computer/network/Internet is a privilege, not a right. Should a system user violate any of these provisions, his or her account may be terminated, future access may be denied, and disciplinary actions may be taken under Board Policy, the Employee Handbook, the Student Handbook and/or the Student Code of Conduct. In addition, all system users are held responsible for understanding that the inappropriate use of the District Technology System may be a violation of state, federal, and local laws, including but not limited to the following: Section 1030 of Title 18 of the United States Code, Fraud and Related Activity in Connection with Computers; the Texas Computer Crimes Statute; Section 1, Chapter 33.02 of Title VII of the Texas Penal Code, Breach of Computer Security; and Section 16.04 of Title IV of the Texas Penal Code, Unlawful Access to Stored Communications. Violations can lead to investigation and prosecution by law enforcement agencies. Under State Statute Section 41.001, Parental Liability, parents can also be held responsible for damage caused by a minor child.

Access to Computer/Network/Internet. Computer/Network/Internet access is provided to all District teachers and staff. Students may be allowed to use the local network with campus permission, but may only use the Internet with parent permission. Student Internet access will be under the direction and guidance of a District teacher or staff member.

Access to the District's electronic communications system, including the Internet, shall be made available to students and employees primarily for instructional and administrative purposes and in accordance with administrative regulations including, but not limited to, Board Policy, the Employee Handbook, the Student Handbook, and the Student Code of Conduct. Limited personal use is permitted if the use imposes no tangible cost to the District, does not unduly burden the District's computer or network resources, and has no adverse affect on an employee's job performance or on a student's academic performance.

All nonemployee/nonstudent users must obtain approval from the principal or departmental supervisor or designee to gain individual access to the District's system.

All individual users of the District's system must complete and sign an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on file in the principal's or departmental supervisor's office.

System users are required to maintain password confidentiality. System users are prohibited from sharing personal passwords with others. System users may not use another person's system account. The system user in whose name a system account is issued will be responsible for its proper use at all times.

Any system user identified as a security risk or having violated District Acceptable Use Guidelines may be denied access to the District's system. Other consequences, including but not limited to those contained in Board Policy, the Employee Handbook, the Student Handbook and the Student Code of Conduct, may also be assigned.

Content/Third-Party Supplied Information. System users and parents of students with access to the District's system should be aware that use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate/objectionable material. GISD uses filtering technology to restrict such access; however, it is not possible to absolutely prevent such access.

A student who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to the supervising teacher.

A student who knowingly brings prohibited materials into the school's electronic environment will be subject to suspension of access/revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Board-approved *Discipline Management Plan and Student Code of Conduct.*
An employee who knowingly brings prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies. [See Board policy DH]

Subject to Monitoring. All District computer/network/Internet usage shall not be considered confidential and is subject to monitoring by designated staff at any time to ensure appropriate use with or without the employee or student's consent. System users should not use the computer system to send, receive or store any information, including e-mail messages, that they consider personal or confidential and wish to keep private. All electronic files, including e-mail messages, transmitted through or stored in the computer system will be treated no differently than any other electronic file. The District reserves the right to access, review, copy, modify, delete or disclose such files for any purpose. Users should treat the computer system like a shared or common file system with the expectation that electronic files, sent, received or stored anywhere in the computer system will be available for review by any authorized representative of the District for any purpose.

User Responsibilities

Computer/Network/Internet users are responsible for their actions in accessing available resources.

Campus- and Departmental-Level Responsibilities. The principal/departmental administrator or designee will:

1. Be responsible for disseminating and enforcing the District Acceptable Use Guidelines for the District's system at the campus or departmental level.

2. Ensure that all individual users of the District's system complete and sign an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on file in the principal's or departmental supervisor's office.

3. Ensure that employees supervising students who use the District's systems provide information emphasizing its appropriate and ethical use.

4. Monitor and examine all users of the District's systems to ensure appropriate and ethical use.

Employee Responsibilities. District employees are bound by all portions of the District's Computer/Network/Internet Acceptable Use Guidelines. An employee who knowingly violates any portion of the Acceptable Use Guidelines will be subject to disciplinary action in accordance with District policies. [See Board policy DH]

Galveston ISD Employee Code of Conduct. District employees are expected to maintain appropriate conduct when accessing the communications and information technologies available through computer/network/ Internet access. All employees must comply with the District's Computer/Network/Internet Acceptable Use Guidelines at all times when accessing any part of the technology system.
Employees will guard and protect access to secure systems by:

1. **Protecting passwords and similar authorization information**. Passwords are the primary way in which users are authenticated and allowed to use the District's computing resources. Employees will not disclose personal password(s) to any individual, including a faculty or staff member. Similarly, employees will not disclose other identifying information (e.g., PIN

numbers) used to access specific system information, recognizing that if they do so, they will be held accountable for their actions as well as those of other parties to whom they have given access.

2. **Guarding unauthorized use of resources**. Employees will not allow others to make use of their accounts or network access privileges to gain access to resources to which they would otherwise be denied.

3. **Not circumventing or compromising security.** Employees must not utilize any hardware or software in an attempt to compromise the security of any other system, whether internal or external to the District's systems and network. Examples of prohibited activities include (but are not limited to) Trojan horses, password crackers, port security probes, network snoopers, IP spoofing, and intentional transmission of viruses or worms.

Computer/Network/Internet usage is subject to monitoring by designated staff at any time to ensure appropriate use. Electronic files sent, received or stored anywhere in the computer system are available for review by any authorized representative of the District for any purpose. Employees will affirm, in writing that at all times their actions while using the District's system will not violate the law or the rules of network etiquette, will conform to the guidelines set forth in the Acceptable Use Guidelines, and will not violate or hamper the integrity or security of the District's technology system.

If a violation of the Acceptable Use Guidelines occurs, employees will be subject to one or more of the following actions:

1. Revocation of access**;**
2. Disciplinary action;
3. Loss of employment with the District;
4. Appropriate legal action.

Student Responsibilities. District students are bound by all portions of the District's Computer/Network/Internet Acceptable Use Guidelines.

A student who knowingly violates any portion of the Acceptable Use Guidelines will be subject to suspension of access/revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Board-approved *Discipline Management Plan and Student Code of Conduct.*

Use of System Resources. System users are required to purge e-mail or outdated files on a regular basis.

Participation in Social Media Learning Environments. Students and employees may participate in social media learning environments, including but not limited to, blogs, discussion forums, RSS feeds, wikis, and message boards within a District-approved safe, secure, curriculum-supported learning opportunity.

Inappropriate Use

Inappropriate use includes, but is not limited to, those uses that violate the law, that are specifically named as violations in this document, that violate the rules of network etiquette, or that hamper the integrity or security of this or any components that are connected to the computer/network/Internet. The following actions are considered inappropriate uses and are prohibited:

Accessing inappropriate web sites. District network or District provided equipment may not be used at any time to access any inappropriate web site whether on District property or when away from the District for any reason. Inappropriate sites include but are not limited to the following:

- Sites containing pornographic material
- Sites containing child abuse or child exploitation material
- Proxy servers
- Dating web sites
- Cam web sites not approved by District
- Gambling sites
- Chat sites not approved by District
- Social Media sites not approved by District

Violations of Law. Transmission of any material in violation of any federal or state law is prohibited. This includes, but is not limited to:

- copyrighted material;
- plagiarized material;
- threatening, harassing, defamatory or obscene material; or
- material protected by trade secret.
- Streaming content

Tampering with or theft of components from District systems may be regarded as criminal activity under applicable state and federal laws.

Any attempt to break the law through the use of a District computer/network/Internet account may result in litigation against the offender by the proper authorities. If such an event should occur, the District will fully comply with the authorities to provide any information necessary for the litigation process.

Intellectual Property. Teachers, staff and students must always respect copyrights and trademarks of third-parties and their ownership claims in images, text, video streaming content and audio material, software, information and inventions. The copy, use, or transfer of others' materials without appropriate authorization is not allowed. System users will be held personally liable for any action(s) that violate intellectual property laws.

Transmitting Confidential Information. Teachers, staff and students may not redistribute or forward confidential information (i.e. educational records, directory information, personnel records, etc.) without proper authorization. Confidential information should never be transmitted, redistributed or forwarded to outside individuals who are not expressly authorized to receive the information. Revealing such personal information as home addresses or phone numbers of users or others is prohibited.

Modification of Computer. Modifying or changing computer settings/internal or external configurations without appropriate permission is prohibited.

Registering Domains. Individual registration of domain names, web hosting, and/or security certificates is strictly prohibited. Requests for web sites or domains will be reviewed by the MIS Department in conjunction with the District Communication's office. No additions will be considered without approval from both Departments. No external domain may be linked to the district web site without the express prior written consent of the MIS Department and Communication's office. Any attempt to circumnavigate these restrictions will result in serious disciplinary action up to and including dismissal.

Commercial Use. Use of the system for any type of income-generating activity is prohibited. Advertising the sale of products, whether commercial or personal is prohibited.

Marketing by Non-GISD Organizations. Use of the system for promoting activities or events for individuals or organizations not directly affiliated with or sanctioned by the District is prohibited.

Vandalism/Mischief. Any malicious attempt to harm or destroy District equipment, materials or data, or the malicious attempt to harm or destroy data of another user of the District's system, or any of the agencies or other networks to which the District has access is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above is prohibited and will result in the cancellation of system use privileges. System users committing vandalism will be required to provide restitution for costs associated with system restoration and may be subject to other appropriate consequences. [See DH, FN series, and FO series in Board Policy and the Board-Approved *Discipline Management Plan and the Student Code of Conduct*]

Impersonation/Plagiarism. Fraudulently altering or copying documents or files authored by another individual or assuming the identity of another individual is prohibited.

Illegally Accessing or Hacking Violations. Illegally accessing or hacking and subsequent manipulation of information of private databases/systems is prohibited.

File/Data Violations. Deleting, examining, copying, or modifying files/data belonging to other users, without their permission is prohibited.

Copyright Violations. Downloading or streaming copyrighted information without following approved District procedures is prohibited.

System Interference/Alteration. Deliberate attempts to exceed, evade or change resource quotas are prohibited. The deliberate causing of network congestion through mass consumption of system resources is prohibited.

Electronic Mail

Electronic Mail (e-mail) is one of the most used communications tools in the District. It should be used primarily for instructional and administrative needs. All teachers and staff are issued e-mail accounts and should keep the following points in mind:

Perceived Representation. Using school-related e-mail addresses might cause some recipients or other readers of the e-mail to assume that the user's comments represent the District or school, whether or not that was the user's intention.

Privacy. E-mail communication should not be considered a private, personal form of communication. Private information, such as home addresses or phone numbers, should not be divulged in e-mail without the permission of the individual involved.

Inappropriate Language. Using obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language in e-mails distributed through District e-mail is prohibited. Sending messages that could cause danger or disruption, personal attacks, including prejudicial or discriminatory attacks are prohibited.

Political Lobbying. Consistent with State ethics laws, District resources and equipment, including, but not limited to, e-mail, must not be used to conduct any political activities, including political advertising or lobbying. This includes using District e-mail to create, distribute, forward, or reply to messages, from either internal or external sources, which expressly or implicitly support or oppose a candidate for nomination or election to either a public office or an office of a political party or support or oppose an officeholder, a political party, or a

measure (a ballot proposition). These guidelines prohibit direct communications as well as the transmission or forwarding of e-mails, hyperlinks, or other external references within e-mails regarding any political advertising.

Forgery. Forgery or attempted forgery of e-mail messages is prohibited. Attempts to read, delete, copy or modify the e-mail of other system users, deliberate interference with the ability of other system users to send/receive e-mail, or the use of another person's user ID/password is prohibited.

Junk Mail/Chain Letters. Generally users should refrain from forwarding e-mails which do not relate to the educational purposes of the District. Chain letters or other e-mails intended for forwarding or distributing to others is prohibited. Creating, distributing or forwarding any annoying or unnecessary message to a large number of people (spamming) is also prohibited.

Resource Limits. Users should limit e-mail messages to instructional and administrative functions. Users should check e-mail frequently, delete unwanted messages promptly, and stay within the e-mail server space allocations. E-mail attachments are limited to 10MB or smaller. Attachments such as EXE, COM and other unauthorized virus-prone attachments will be blocked.

Personal E-mail Accounts. Internet access to personal e-mail accounts is not allowed.

Student E-mail Accounts

The following will apply to student e-mail usage:

1. Students are prohibited from accessing personal e-mail accounts using the District's system.
2. As appropriate and with written approval of the appropriate District personnel in the MIS Department, project e-mail accounts will be granted for specific educational activities.
3. Student e-mail accounts may be provided directly by the District or through the content management system of an approved online course.
4. Students who are given access to an e-mail account are expected to abide by all Acceptable Use guidelines.

District Web Contributor Responsibilities

The purpose of District Web sites is to communicate campus, department, and District activities and information to District Web patrons and employees. All official school and District Web sites must be hosted on a District Web server. All individuals creating/editing content for display on District Web servers are considered District Web-content contributors.

In conjunction with the District's MIS Department, the District's Communications Department is responsible for ensuring that all Web site content, including but not limited to GISD.org, campus Webs,+ and teacher Webs, conforms to the guidelines described below, as well the District's overall communications objectives. As such, the Communications Department reserves the right to alter or delete any content contained on a District Web site in order to ensure that it conforms to both Web site guidelines and the District's communications objectives.

Content Issues

For the requirements below," content" is defined as text, graphics, media, or other information that is visible/audible on a District Web page.

- All content must be approved by principals/department heads or their designees before being posted to District Web servers.
- If any content/file that is saved on a District Web server or content on an external (non-District) Web site which uses a hyperlink from a District Web page exhibits any of the following conditions or presents any of the following problems, the individual responsible for that content will be asked to eliminate the offending condition within a reasonable amount of time. If the condition is not corrected after a reasonable amount of time, the District's MIS Department will take action to rectify the situation. An employee who knowingly violates (or promotes the violation of) any portion of these guidelines will be subject to disciplinary action in accordance with District policies. [See Board policy DH]
- Content shall not be displayed if it:
    - Contains questionable/inappropriate material/themes.
    - Is of a personal nature.
    - Includes commercial, trademarked,/copyrighted material without the express written consent of the "owner" of the content. If consent is obtained, the proper trademark/copyright symbol/owner's credits must be displayed.
    - Is out-of-date or inaccurate.
    - Contains hyperlinks that do not return an active Web page and displays a "Page Not Found".
    - Contains hyperlinks that do not return a document and displays a "Page Not Found".
- Teachers must use Web sites on District Web servers to post class information. A hyperlink from a teacher Web site to a teacher's external, personal Web site or of any other external (non-District) Web site maintained by District staff or volunteers is prohibited.
- Personal information about District employees/parent volunteers will not be disclosed without the approval of the individual and the principal/administrator and will be in accordance with District/campus procedures. Non-District e-mail addresses, non-District mailing addresses, and non-District phone numbers will not be disclosed on District/campus Web sites.
- Pictures and names of employees/parent volunteers are allowed with their written approval.

Display of Student Information on District Web Sites
The following conditions apply to the display of student information on District Web sites. A content contributor who knowingly violates (or promotes the violation of) any portion of these guidelines will be subject to disciplinary action in accordance with District policies. [See Board policy DH]

- Student-created projects, writings,/artwork are permitted on campus/District Web sites if the appropriate parental consent has been obtained.
- Student photographs and names are permitted if the directory information privacy code specified for the student allows for it (code "A" only).
- For a student with an "N" or "O" directory information privacy code, specific parental consent must be obtained in writing to display each photograph of the student. Verbal consent from the parent, guardian or adult student is not sufficient.
- All student photographs/student work must be displayed with either no name, first name only, or first name and last initial only. No other personal student information is allowed including, but not limited to, e-mail address, phone number, home address,/birth date.

Hyperlinks
The following requirements must be met to utilize hyperlinks on any District Web page. If these conditions are not met, the individual responsible for those hyperlinks will be asked to eliminate the offending condition within a reasonable amount of time, after which the District's MIS Department will take action to rectify the situation. If the condition is a violation of (or promotes the violation of) any District policy or regulation or any local, state, or federal regulation or law, immediate disciplinary action of the individual responsible for the content/file may be recommended.

- Hyperlinks to external (non-District) Web sites must include the following text on the District Web page where the hyperlink exists: "Galveston ISD is not responsible for content on external sites or servers."
- Hyperlinks to all external (non-District) Web sites must open those Web sites in a new window.
- Hyperlinks to external (non-District) Web sites are only allowed where the content in those Web sites support/enhance learning, academic knowledge,/provide information necessary to provide service to District Web patrons. However, if the content in these Web sites is judged unsuitable at any time, the hyperlink to the site will be removed.
- Hyperlinks to Web sites, whose content is prohibited by the District's Web filtering system, will not be allowed.
- Hyperlinks to District employee or volunteer personal Web sites and personal Web pages are not allowed.
- Hyperlinks to personal student Web sites and personal Web pages are prohibited.

E-mail Links
District e-mail addresses (those e-mail addresses ending with "@GISD.org" will **not** be displayed on District public Web sites without being linked to a **District e-mail Web form**. If an e-mail address is using the traditional "mailto" html code, the individual responsible for that e-mail link will be asked to revise his/her code in a reasonable amount of time, after which, the situation will be rectified by the District's MIS Department. E-mail links can be displayed in one of these two methods:

1. If the e-mail link is being displayed in a Galveston ISD Web page, one must use a Web control specifically provided to display contact information including the contact's e-mail address.
2. If an e-mail link is being displayed in Web sites other than a Galveston ISD Web page, one must utilize code that invokes the e-mail Web form. Upon request, this code will be provided to the individual desiring to display an e-mail link.

Special Features
There are special Web sites features that will not be allowed on District Web sites.

- "Guestbooks", "chat areas", "message boards" or similar non-District, unmonitored,/user-community developed/maintained facilities are prohibited, without written permission
- No executable programs or applets are allowed on District Web sites.

Security

Reporting Security Problem. If a user is made aware of or has knowledge of inappropriate material or a security problem on the computer/network/Internet, the user should immediately notify the District's Help Desk. The security problem should not be shared with others.

Impersonation. Attempts to log on to the computer/network/Internet impersonating a system administrator or District employee, student, or individual other than oneself, will result in revocation of the user's access to computer/network/Internet.

Other Security Risks. Any user identified as having had access privileges revoked or denied on another computer system may be denied access to the District's Network/Internet.

Consequences of Agreement Violation

Any attempt to violate the provisions of this agreement may result in revocation of the user's access to the computer/network/Internet, regardless of the success or failure of the attempt. In addition, school disciplinary action/appropriate legal action may be taken.

Denial, Revocation, or Suspension of Access Privileges. With just cause, the System Administrator/building principal, may deny, revoke, or suspend computer/network/Internet access as required, pending an investigation.

The final decision regarding whether any given use of the computer/network/Internet is acceptable or unacceptable lies with the Superintendent or his/her designee in consultation with the System Administrator.

Warning

Sites accessible via the computer/network/Internet may contain material that is illegal, defamatory, objectionable, inaccurate or controversial. Each District computer with Internet access has filtering software that blocks access to visual depictions that are obscene, pornographic, objectionable, or inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act. The District makes every effort to limit access to objectionable material; however, controlling all such materials on the computer/network/Internet is impossible, even with filtering in place. With global access to computers and people, a risk exists that students may access material that may not be of educational value in the school setting. The Galveston ISD Internet connection is the only system to be used in schools. No commercial Internet accounts may be used.

Disclaimer

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error free, or that defects will be corrected.

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.

Computer/Network/Internet Acceptable Use Agreement Receipt

I hereby acknowledge receipt of my personal copy of the Galveston ISD Computer/Network/Internet Acceptable Use Agreement ("AU Agreement"). I have read and I understand the GISD AU Agreement, and I agree to abide by these provisions.

The information in this AU Agreement is subject to change. I understand that changes in district policies may supersede, modify, or eliminate the information summarized in the AU Agreement. As the District provides updated policy information, I accept responsibility for reading and abiding by the changes.

I understand that violation of these provisions is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges will be revoked with or without notice, and disciplinary actions and/or the appropriate legal action will be taken.

Name (please print) **Staff Member's Signature** **Date**

Campus or Department:

Note: You have been given two copies of this form. Please sign and date one to keep for your records. Sign and date the other copy and forward it to your campus principal or supervisor.

Sign and Return This Copy To Your Immediate Supervisor!

Computer/Network/Internet Acceptable Use Agreement Receipt

I hereby acknowledge receipt of my personal copy of the Galveston ISD Computer/Network/Internet Acceptable Use Agreement ("AU Agreement"). I have read and I understand the GISD AU Agreement, and I agree to abide by these provisions.

The information in this AU Agreement is subject to change. I understand that changes in district policies may supersede, modify, or eliminate the information summarized in the AU Agreement. As the District provides updated policy information, I accept responsibility for reading and abiding by the changes.

I understand that violation of these provisions is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges will be revoked with or without notice, and disciplinary actions and/or the appropriate legal action will be taken.

Name (please print) **Staff Member's Signature** **Date**

Campus or Department:

Note: You have been given two copies of this form. Please sign and date one to keep for your records. Sign and date the other copy and forward it to your campus principal or supervisor.

Please keep this copy for your records