



# Greenville Independent School District

## Acceptable Use Policy

### Philosophy and Purpose

The district provides an electronic communications network and Internet access to electronic mail, voice mail, databases, libraries, museums, and other information sources in accordance with Board Policy CQ LOCAL and for the following limited purposes:

1. Promote educational excellence in its schools by facilitating resource sharing, innovation, and communication.
2. Improve learning and reach the district's instructional goals.
3. Achieve effective and efficient administration at the district and campus levels.
4. Comply with the Texas Education Agency's guidelines for technology in schools.

Any use of the district's information and communication systems and resources by authorized users must be in furtherance of these limited purposes and conform to the district's expectations for legal, efficient, and ethical use.

### Internet Safety and Limitations

Recognizing that the Internet can give access to sites containing information that is obscene, i.e., child pornography, or harmful to minors or that would be otherwise inappropriate for distribution to students, unsuitable for use in the approved curriculum, or irrelevant to accomplishing the district's stated purposes for operating an Internet-accessible network, the district has installed technology protection measures to filter, screen, analyze, and block site content in an effort to make it more difficult for students or staff to gain access to such material through the district's network.

The district makes no representation that it can control access to all Internet sites. Network users are responsible for their actions in accessing available resources and will be held accountable for sending or receiving information that is inconsistent with the requirements for acceptable and unacceptable use of the communication network and Internet

It is the responsibility of district classroom teachers to assist students in the learning of safe online behaviors, cyberbullying, information security, and digital citizenship.

### Social Media

Social Media is defined as the interactive use of online resources including, but not limited to, Facebook, YouTube, Twitter, Google Apps, Office 365, Skype, chat rooms, wikis, and blogs.

The use of any district technology resource (including, but not limited to, desktop computers, electronic devices, network-delivered services, the Internet, audio-visual equipment, digital content, and social media) must support the educational goals of Greenville Independent School district. Use during instructional time must be authorized by a district staff member and must lie within the bounds of the district's curriculum and educational purpose. Electronic, direct, non-automated communications with students are prohibited unless designated in writing by the Superintendent or campus Principal. Additional guidelines on this policy are outlined in the Employee Handbook. (Policy DH)

#### Authorized Users

The district permits staff members who have a GISD intended purpose to use the computer network. district visitors, and staff/student personal machines, may use the GISD visitor wireless network to obtain access to the internet, but not other network systems.

#### General Requirements for Network and Internet Use

Student and employee use of the district's communications network and access to the Internet must be in accordance with this policy.

Each authorized user is responsible for all activities, transmissions, or actions that occur under that account identifier. No account sharing or password sharing shall be permitted, without first obtaining written authorization from the Chief Information Officer or designee.

Employees and students shall not take district computers off-campus, without first obtaining written authorization from the Chief Information Officer or designee. Any user who identifies a security problem with the network must immediately notify the Chief Information Officer and may not communicate the problem to any other person.

#### Monitoring Use

Use of a personal communications network account through the district's system is voluntary and constitutes a privilege provided by the district, not a right. All network usage, including voicemail and email, is subject to monitoring, examination, and investigation by the system administrators without prior notice or the specific consent of the user. Accounts given out by GISD may be monitored for use both on premise as well as during use at a remote location.

The Chief Information Officer may establish standards and limits on email format, including the use of graphics and other attachments. By signing the user agreement, each authorized user acknowledges the possibility of such monitoring and consents to it. Professional employees overseeing student instructional use of the district's communications network or access to the Internet will be vigilant in determining that students are using the district's system only in compliance with this policy to enhance student safety and security, particularly when students are using email and other forms of electronic communication authorized under this policy.

#### Information Security

It is the responsibility of all district personnel to take action to protect data belonging to Greenville ISD. Data includes but is not limited to employee and student personal information, FERPA protected information, GISD intellectual property, and detailed systems information.

Employees will utilize caution when completing the following actions to ensure data is kept secure:

1. Double-check email recipients to ensure communication or data about staff or students is going to the intended individual.
2. Flash drives or USB memory cards containing staff or student information are never taken off-premises without prior approval from a campus or district administrator. It is recommended to utilize online cloud storage services over USB flash drives due to increase security as well as provide backups.
3. Files and folders stored with cloud storage services are not shared outside the GISD organization without prior administrator consent unless this task is performed routinely according to your job function.
4. Report any lost or stolen GISD technology as soon as possible.

#### Data Breaches

Upon discovery or receiving notification of a breach of system security, GISD will disclose the breach to affected persons or entities in accordance with time frames established by law. GISD may use one or more methods to give notice of a breach:

1. Written notice.
2. Electronic mail.
3. Conspicuous posting on the district website.
4. Publication through broadcast media.

#### Suspending or Revoking Privileges

Access to the communications network, the Internet, or both may be suspended or revoked and user identifications deleted if a student or employee is determined to have violated this policy or the user agreement each user signs as a condition for obtaining access to the district's communications network and/or the Internet. Any user identified as a security risk or who has a history of violations with other communications systems shall be denied access to the network. A user whose access has been suspended or revoked may request a conference with the Principal and Chief Information Officer to discuss the basis for that action and have an opportunity to respond. A decision by the Chief Information Officer to suspend or revoke system privileges may be appealed to the Superintendent or the board. System privileges are revoked during any appeal.

#### Acceptable Use

Occasional personal use is acceptable during non-instructional or break/lunch periods. Personal use shall be monitored. The final decision regarding whether any given use of the network or Internet is acceptable lies with the Superintendent or designee, in consultation with the Chief Information Officer. Any use described below is deemed "acceptable" and consistent with the User Agreement and this policy:

1. Supports instructional purposes and goals.
2. Furthers the district's educational and administrative purposes, goals, and objectives.
3. Furthers research related to education and instruction.
4. Does not violate the Student Code of Conduct or employee standards of conduct.
5. Is consistent with network rules established by the Chief Information Officer.

Users may use Internet audio or video for academic purposes, but such use may be disconnected without notice if it affects the performance of the district's communications network.

### Unacceptable Use

The final decision regarding whether any given use of the network or Internet is unacceptable lies with the Superintendent or designee, in consultation with the Chief Information Officer. Any of the following uses is deemed unacceptable and a violation of the user agreement and this policy:

- Unauthorized use of copyrighted material, including violating district software licensing agreements and sharing of copyrighted audio files. (See EFE)
- Posting or distribution of threatening, racist, harassing, cyber bullying, excessively violent, sexually explicit, or obscene material.
- Personal or political use to advocate for or against a candidate, officeholder, political party, or political position. Research or electronic communications regarding political issues or candidates shall not be a violation when the activity is to fulfill an assignment for class credit.
- Participating in chat rooms, Internet games, or multi-user games, other than those sponsored and overseen by the district.
- Tampering, i.e., accessing, reading, deleting, copying, or modifying, with the electronic mail of other users, regardless of where the message is displayed or stored.
- "Hacking," i.e., attempting unauthorized access to any computer whether within the district's network or outside it.
- Any use that would be unlawful under state or federal law.
- Unauthorized disclosure, use, or distribution of personal identification information regarding students or employees.
- Forgery of electronic mail messages or transmission of unsolicited junk e-mail chain messages.
- Use that violates the Student Code of Conduct or employee standards of conduct or illegal activities.
- Use related to commercial activities or for commercial gain by a student or employee.
- Advertisement for purchase or sale of a service or product.
- All software and hardware downloads, and/or installations without prior written approval from the Chief Information Officer or designee.
- Users are prohibited from intentionally accessing objectionable material on the Internet. If you unintentionally access objectionable material, you are expected to immediately discontinue the access and report the incident to the site administrator. Objectionable material includes, but is not limited to, lewd or foul language or images, pornographic content, gang related information, materials that are abusive, threatening, harassing, or damaging to another's reputation, district's reputation, or information to assist in technology theft or misuse.
- Use of social media in a way that creates security or safety issues or creates a substantial disruption.

The unacceptable uses identified and referenced above serve as examples of inappropriate conduct which violate this policy and is in no way intended to be an exhaustive account of all prohibited conduct or activities which subject a user to disciplinary or corrective action in accordance with applicable district policy, handbooks, student code of conduct, handbooks, and rules. The district reserves the right to determine whether a violation of this policy has occurred on a case-by-case basis in keeping with the

purpose of this policy. Additionally, the district reserves the right to take immediate disciplinary or corrective action against a user that engages in conduct that: (i) creates security or safety issues for the district, students, employees, schools, networks, or technology resources, or (ii) is determined to be inappropriate or inconsistent with district policy or law.

#### Serious Violations

If the Principal determines that a student's or employee's use of the system violates the Student Code of Conduct or employee standards of conduct and that disciplinary action other than or in addition to suspension or revocation of system privileges is warranted, those disciplinary actions will be in accordance with the applicable policies.

#### System or Other Interference

Users must not attempt to exceed, evade, or change established resource quotas, i.e., allocations of local hard drive storage space or network time. The district quotas are designed to ensure all users have a fair opportunity to access resources.

Vandalism and mischief are prohibited. Vandalism includes any attempt to harm or destroy another user's data on the network or on any network connected to the district's network and any deliberate creation or propagation of a computer virus(es). Mischief includes any interference with another user's work, such as attempts to delete, examine, copy, or modify data, files, fields, or any other element of another user's information.

#### Disclaimer

The district makes no warranties of any kind, expressed or implied, for its communications network facilities and bears no liability for users' copyright violations; users' inappropriate or tortuous use of the communications network system or resources; any damages incurred by users, including loss of data resulting from the action or inaction of any district employee or a user's errors or omissions; and phone charges, credit card charges, or any other charges incurred by users without prior district authorization and according to established purchasing procedures. The district specifically denies any responsibility for the accuracy, age-appropriateness, or quality of information obtained through its communications network facilities.

#### Intellectual Property Rights

Students retain the copyright and all other intellectual property rights to works of any kind they create using the district's electronic information resources and system, including those created in fulfillment of course requirements or through participation in extracurricular activities.

The district is the copyright owner of any work created or developed by an employee within the scope of his or her employment, regardless of whether the work is prepared at school using school equipment or out of school using personally owned or other equipment.

#### Electronically Signed Documents

At the district's discretion, the district may make certain transactions available online, including student admissions documents, student grade and performance information, contracts for goods and services, and employment documents.

I have read and understand the Acceptable Use Policy and agree to abide by its terms and conditions.

---

Employee Signature

---

Date