Greenfield R-IV Technology Acceptable Use Agreement

The Greenfield R-IV School District's technology exists for the purpose of enhancing the educational opportunities and achievement of district students. Technology integration in education is vital for 21st Century learners to be equipped with necessary skills for higher education and for the workplace. In addition, technology assists with the professional enrichment of the staff and increases engagement of students' families and other patrons of the district, all of which positively impact student achievement and school community.

The purpose of this policy is to facilitate access to district technology and to create a safe environment in which to use that technology. Because technology changes rapidly and employees and students need immediate guidance, the superintendent or designee is directed to create procedures to implement this policy and to regularly review those procedures to ensure they are current.

Definitions

For the purposes of this policy and related procedures and forms, the following terms are defined:

Technology Resources – Technologies, devices and services used to access, process, store or communicate information. This definition includes, but is not limited to: computers; modems; printers; scanners; fax machines and transmissions; telephonic equipment; mobile phones; tablets; audio-visual equipment; Internet; electronic mail (e-mail); electronic communications devices and services, including wireless access; multimedia resources; hardware; and software. Technology resources may include technologies, devices and services provided to the district by a third party.

The Internet – a collection of interconnected computer networks around the world – expands classroom and library media resources by providing access to information, images, and even computer software from places otherwise impossible to reach. These resources can yield individual and group projects, collaboration, curriculum materials and idea sharing. Internet access also makes possible contact with people all over the world, bringing into the school, into the classroom, experts in every content area and students and adults from other nations and cultures.

User – Any person who is permitted by the district to utilize any portion of the district's technology resources including, but not limited to, students, employees, School Board members and agents of the school district.

User Identification (ID) – Any identifier that would allow a user access to the district's technology resources or to any program including, but not limited to, e-mail and Internet access.

Password – A unique word, phrase or combination of alphabetic, numeric and non-alphanumeric characters used to authenticate a user ID as belonging to a user.

Authorized Users

The district's technology resources may be used by authorized students, employees, and other persons approved by the superintendent or designee, such as consultants, legal counsel and independent contractors. All users must agree to follow the district's policies and procedures and sign or electronically consent to the district's User Agreement prior to accessing or using district technology resources, unless excused by the superintendent or designee.

Use of the district's technology resources is a privilege, not a right. No potential user will be given an ID, password or other access to district technology if he or she is considered a security risk by the superintendent or designee.

User Privacy

A user does not have a legal expectation of privacy in the user's electronic communications or other activities involving the district's technology resources including, but not limited to, voice mail, telecommunications, e-mail and access to the Internet or network drives. By using the district's network and technology resources, all users are consenting to having their electronic communications and all other use monitored by the district. A user ID with email access will only be provided to authorized users on condition that the user consents to interception of or access to all communications accessed, sent, received or stored using district technology.

Electronic communications, downloaded material and all data stored on the district's technology resources, including files deleted from a user's account, may be intercepted, accessed, monitored or searched by district administrators or their designees at any time in the regular course of business. Such access may include, but is not limited to, verifying that users are complying with district policies and rules and investigating potential misconduct. Any such search, access or interception shall comply with all applicable laws. Users are required to return district technology resources to the district upon demand including, but not limited to, mobile phones, laptops and tablets and accessories.

Technology Administration

The Board directs the superintendent or designee to assign trained personnel to maintain the district's technology in a manner that will protect the district from liability and will protect confidential student and employee information retained on or accessible through district technology resources.

Administrators of district technology resources may suspend access to and/or availability of the district's technology resources to diagnose and investigate network problems or potential violations of the law or district policies and procedures. All district technology resources are considered district property. The district may remove, change or exchange hardware or other technology between buildings, classrooms or users at any time without prior notice. Authorized district personnel may install or remove programs or information, install equipment, upgrade any system or enter any system at any time.

Content Filtering and Monitoring

The district will monitor the online activities of minors and operate a technology protection measure (“content filter”) on the network and all district technology with Internet access, as required by law. In

accordance with law, the content filter will be used to protect against access to visual depictions that are obscene or harmful to minors or are child pornography. Content filters are not foolproof, and the district cannot guarantee that users will never be able to access offensive materials using district equipment. Evading or disabling, or attempting to evade or disable, a content filter installed by the district is prohibited.

The superintendent, designee or the district's technology administrator may fully or partially disable the district's content filter to enable access for an adult for bona fide research or other lawful purposes. In making decisions to fully or partially disable the district's content filter, the administrator shall consider whether the use will serve a legitimate educational purpose or otherwise benefit the district.

The superintendent or designee will create a procedure that allows students, employees or other users to request that the district review or adjust the content filter to allow access to a website or specific content.

Educational Use of G Suite Accounts

Students will be issued a Google G Suite account in order to access Google Apps (i.e., Google Calendar, Google Sites, Google Docs, Google Drive). Google has already incorporated critical security features including student privacy, and data security. Google Classroom is used by teachers to communicate and deliver assignments and feedback to students. Student work can be created or uploaded for archiving, editing, live collaboration, and presentation. From home or from school, students can safely store their work, create documents, collaborate with classmates, and submit items for feedback. While a Google account does provide students with an email address, access will be restricted to communication only within the Greenfield R-IV School District unless specifically approved by the superintendent or designee. All student users of G Suite accounts must have a parent permission on file.

Online Safety, Security and Confidentiality

In addition to the use of a content filter, the district will take measures to prevent minors from using district technology to access inappropriate matter or materials harmful to minors on the Internet. Such measures shall include, but are not limited to, supervising and monitoring student technology use, careful planning when using technology in the curriculum, and instruction on appropriate materials. The superintendent or designee will develop procedures to provide users guidance on which materials and uses are inappropriate, including network etiquette guidelines.

All minor students will be instructed on safety and security issues, including instruction on the dangers of sharing personal information about themselves or others when using e-mail, social media, chat rooms or other forms of direct electronic communication. Instruction will also address cyberbullying awareness and response and appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms.

This instruction will occur in the district's computer courses, courses in which students are introduced to the computer and the Internet, or courses that use the Internet in instruction. Students are required to

follow all district rules when using district technology resources and are prohibited from sharing personal information online unless authorized by the district.

All district employees must abide by state and federal law and Board policies and procedures when using district technology resources to communicate information about personally identifiable students to prevent unlawful disclosure of student information or records.

All users are prohibited from using district technology to gain unauthorized access to a technology system or information; connect to other systems in evasion of the physical limitations of the remote system; copy district files without authorization; interfere with the ability of others to utilize technology; secure a higher level of privilege without authorization; introduce computer viruses, hacking tools, or other disruptive/destructive programs onto district technology; or evade or disable a content filter.

Cancellation of Accounts

Any user that has graduated, transferred, left employment or is otherwise not associated with the school will have his or her accounts terminated. This includes, but is not limited to the following accounts: network, G Suite, email, cloud storage, curricular websites and programs. It is permissible to transfer drive and cloud storage to a new account. The designee will assist with this process. The user is solely responsible for deleting all sensitive data containing sensitive information prior to the transfer of data process. The user is responsible for signing out of and removing account access from all devices that do not belong to the district. Termination of the account will occur after the final day of the user's association with Greenfield R-IV. Access of these accounts after association with the district has ended is unauthorized and specifically forbidden by the school.

Violations of Technology Usage Policies and Procedures

Use of technology resources in a disruptive, inappropriate or illegal manner impairs the district's mission, squanders resources and shall not be tolerated. Therefore, a consistently high level of personal responsibility is expected of all users granted access to the district's technology resources. Any violation of district policies or procedures regarding technology usage may result in temporary, long-term or permanent suspension of user privileges. User privileges may be suspended pending investigation into the use of the district's technology resources.

Employees may be disciplined or terminated, and students suspended or expelled, for violating the district's technology policies and procedures. Any attempted violation of the district's technology policies or procedures, regardless of the success or failure of the attempt, may result in the same discipline or suspension of privileges as that of an actual violation. The district will cooperate with law enforcement in investigating any unlawful use of the district's technology resources.

Damages

All damages incurred by the district due to a user's intentional or negligent misuse of the district's technology resources, including loss of property and staff time, will be charged to the user. District administrators have the authority to sign any criminal complaint regarding damage to district technology.

No Warranty/No Endorsement

The district makes no warranties of any kind, whether expressed or implied, for the services, products or access it provides. The district's technology resources are available on an "as is, as available" basis.

The district is not responsible for loss of data, delays, nondeliveries, misdeliveries or service interruptions. The district does not endorse the content nor guarantee the accuracy or quality of information obtained using the district's technology resources.

Restrictions

The following activities are not permitted on Greenfield School District electronic resources:

1. Accessing, uploading, downloading, transmitting or displaying or distributing obscene or sexually explicit material; transmitting obscene, abusive or sexually explicit language.
2. Damaging computers, computer systems or computer networks; vandalizing, damaging or disabling the property of another person or organization; debilitating or disabling computers, systems or networks through the intentional mis- or overuse of electronic distribution or storage space, or the spreading of computer viruses through the inappropriate use of files or diskettes.
3. Email use by students is prohibited except when approved by the building principal and monitored by the classroom teacher.
4. Violating copyright, or otherwise using another person’s intellectual property without his or her prior approval or proper citation; using another person’s passwords, trespassing in another person’s folders, work or files.
5. Violating local, state or federal statutes.

Rights & Privileges – The student user has full rights (within the limits of these guidelines, responsibilities and prohibitions) to the instructional networked resources provided by the Greenfield School District. The student’s network account provided for personal storage space on the Greenfield School District resources which may be treated as a student locker & should be cleared periodically. It is important that the students keep passwords secure & private. However, users should not expect that files always be private. The Greenfield School District network administrators have the right to review files to maintain system integrity & to be sure that the system is being used within the stated limits.

Disclaimers – The Greenfield School District makes no warranties of any kind, either expressed or implied, for the provided access. The staff, the school & the Greenfield School District are not responsible for any damages incurred, including, but not limited to, loss of data resulting from delays or interruption of service, for the loss of data stored on Greenfield School District resources, or for personal property used to access Greenfield School District resources; for the accuracy, nature or quality of information stored on Greenfield School District resources or gathered through corporation-provided access; for unauthorized financial obligations incurred through Greenfield School District-provided access. Further, even though the Greenfield School District may use technical or manual means to limit

student access, these limits do not provide a foolproof means for enforcing the provisions of this policy. All provisions of this agreement are subordinate to local, state & federal statute.

Sanctions – Violations of school networked information resources policies could result in the loss of access to electronic resources. Additional disciplinary action may be determined at the building &/or classroom level in line with existing practice regarding language & behavior. When appropriate, law enforcement agencies may be involved.

G Suite for Education Notice to Parents and Guardians

This notice describes the personal information we provide to Google for these accounts and how Google collects, uses, and discloses personal information from students in connection with these accounts.

Using their G Suite for Education accounts, students may access and use the following "Core Services" offered by Google (described at https://gsuite.google.com/terms/user_features.html):

Gmail
Google+
Calendar
Chrome Sync
Classroom
Cloud Search
Contacts
Docs, Sheets, Slides, Forms
Drive
Groups
Google Hangouts, Google Chat, Google Meet, Google Talk
Jamboard
Keep
Sites
Vault

In addition, we also allow students to access certain other Google services with their G Suite for Education accounts. Your child may have access to the following "Additional Services" including but not limited to:

App Maker
Blogger
Chrome Web Store
Google Alerts
Google Bookmarks
Google Books
Google Cloud Platform
Google Earth

Google Finance
Google Groups
Google Maps
Google News
Google Photos
Google Play
Google Scholar
Google Search
Google Takeout
Google Trips
Individual Storage
Location History
Project Fi
Science Journal
Studio
Third-Party App Backups
Tour Creator
Web and App Activity
Youtube

Google provides information about the information it collects, as well as how it uses and discloses the information it collects from G Suite for Education accounts in its G Suite for Education Privacy Notice. You can read that notice online at https://gsuite.google.com/terms/education_privacy.html You should review this information in its entirety, but below are answers to some common questions:

What personal information does Google collect?

When creating a student account, Greenfield R-IV may provide Google with certain personal information about the student, including, for example, a name, email address, and password. Google may also collect personal information directly from students, such as telephone number for account recovery or a profile photo added to the G Suite for Education account.

When a student uses Google services, Google also collects information based on the use of those services. This includes:

device information, such as the hardware model, operating system version, unique device identifiers, and mobile network information including phone number;
log information, including details of how a user used Google services, device event information, and the user's Internet protocol (IP) address;
location information, as determined by various technologies including IP address, GPS, and other sensors;
unique application numbers, such as application version number; and
cookies or similar technologies which are used to collect and store information about a browser or device, such as preferred language and other settings.

How does Google use this information?

In G Suite for Education Core Services, Google uses student personal information to provide, maintain, and protect the services. Google does not serve ads in the Core Services or use personal information collected in the Core Services for advertising purposes.

In Google Additional Services, Google uses the information collected from all Additional Services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and its users. Google may also use this information to offer tailored content, such as more relevant search results. Google may combine personal information from one service with information, including personal information, from other Google services.

Does Google use student personal information for users in K-12 schools to target advertising?

No. For G Suite for Education users in primary and secondary (K-12) schools, Google does not use any user personal information (or any information associated with an G Suite for Education Account) to target ads, whether in Core Services or in other Additional Services accessed while using an G Suite for Education account.

Can my child share information with others using the G Suite for Education account?

We may allow students to access Google services such as Google Docs and Sites, which include features where users can share information with others or publicly. When users share information publicly, it may be indexable by search engines, including Google.

Will Google disclose my child's personal information?

Google will not share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances applies:

With parental or guardian consent. Google will share personal information with companies, organizations or individuals outside of Google when it has parents' consent (for users below the age of consent), which may be obtained through G Suite for Education schools.
With Greenfield R-IV G Suite for Education accounts, because they are school-managed accounts, give administrators access to information stored in them.
For external processing. Google may provide personal information to affiliates or other trusted businesses or persons to process it for Google, based on Google's instructions and in compliance with the G Suite for Education privacy notice and any other appropriate confidentiality and security measures.
For legal reasons. Google will share personal information with companies, organizations or individuals outside of Google if it has a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:

meet any applicable law, regulation, legal process or enforceable governmental request.
enforce applicable Terms of Service, including investigation of potential violations.

detect, prevent, or otherwise address fraud, security or technical issues.
protect against harm to the rights, property or safety of Google, Google users or the public as required or permitted by law.

Google also shares non-personal information -- such as trends about the use of its services -- publicly and with its partners.

What choices do I have as a parent or guardian?

First, you can consent to the collection and use of your child's information by Google. If you don't provide your consent, we will not create a G Suite for Education account for your child, and Google will not collect or use your child's information as described in this notice.

If you consent to your child's use of G Suite for Education, you can access or request deletion of your child's G Suite for Education account by contacting your child's building office staff or Kristi Blankenship at kblankenship@greenfieldr4.org. If you wish to stop any further collection or use of your child's information, you can request that we use the service controls available to limit your child's access to features or services, or delete your child's account entirely. You and your child can also visit https://myaccount.google.com while signed in to the G Suite for Education account to view and manage the personal information and settings of the account.

What if I have more questions or would like to read further?

If you have questions about our use of Google's G Suite for Education accounts or the choices available to you, please contact Kristi Blankenship at kblankenship@greenfieldr4.org. If you want to learn more about how Google collects, uses, and discloses personal information to provide services to us, please review the G Suite for Education Privacy Center (at https://www.google.com/edu/trust/), the G Suite for Education Privacy Notice (at https://gsuite.google.com/terms/education_privacy.html), and the Google Privacy Policy (at https://www.google.com/intl/en/policies/privacy/).

The Core G Suite for Education services are provided to us under Google's Apps for Education agreement (at https://www.google.com/apps/intl/en/terms/education_terms.html)

GREENFIELD R-IV TECHNOLOGY USE AGREEMENT & GOOGLE SUITE AGREEMENT

Student Name: _____ Grade Level:_____
Teacher (if elementary): _____

The Greenfield R-IV Technology Use Agreement and Google Suite Agreement are available on the district website under "parent resources" for review at any time. Paper copies may be requested from your student's building office at any time.

- ❑ I have reviewed the policies outlined in the Technology Acceptable Use Agreement and Google Suite Agreement. I have discussed the guidelines with my child and he/she understands the expectations and consequences for not using the technology provided by the district in an appropriate manner. My child's signature below indicates that he/she understands that his/her access to district technology may be revoked if misused.

Student & Parent/Guardian Agreements:

Please read &/or discuss the Acceptable Use Agreement and Google Suite Agreement with your student. In accepting district-issued accounts, your student accepts the responsibility of using the accounts in a responsible & appropriate manner. It is important that you understand his/her responsibilities as well. Your signature indicating that you have read & agreed to the guidelines is necessary before accounts will be issued.

I have read, or have had read to me, &/or have discussed the Acceptable Use Agreement and the Google Suite Agreement & agree to use district technology and accounts in an appropriate & responsible manner.

Student Signature _____Date _____

I have read &/or discussed the Acceptable Use Agreement and the Google Suite Agreement with my student & give Greenfield R-IV School District permission to issue user accounts to my student.

Parent/Guardian Signature_____Date _____

The Greenfield R-IV School District supports and respects a family's decision whether or not to apply for student access and whether to terminate or suspend that access. Parents/Guardians have the right to request alternative activities that do not require access to networked information resources. Access, if issued, shall remain in effect unless suspended or terminated by the student, the school or the parent/guardian.