Central Heights ISD
Acceptable Use Policy For Technology Services

Definition of District Technology Resources

The District's computer systems and networks are defined as any combination of hardware, operating system software, application software, stored text, and data files. Examples include electronic mail, local databases, externally accessed resources (such as the Internet), CD-ROM, optical media, clip art, digital images, digitized information, communications technologies, and new technologies as they become available. The district reserves the right to monitor all resource activity.

Acceptable Use

The District's technology resources are to be used for learning, teaching and administrative purposes consistent with the District's mission and goals. The District will make copies of the acceptable use policy available to all stakeholders (students, parents, faculty members, administration and the community).

Access to the District's system is a privilege not a right. You are required to be aware of, understand, and comply with all administrative regulations governing the use of the technology resources. Noncompliance may result in suspension of access or termination of privileges and other disciplinary action consistent with district policies. (Student Code of Conduct, Employee Handbook, Administrative Procedures Manual, and School Board Policy)

Anyone knowingly accessing or bringing prohibited materials into the school's electronic environment will be subject to a suspension and/or a revocation of privileges and will be subject to disciplinary action in accordance with district policy (Student Code of Conduct, Employee Handbook, Administrative Procedures Manual, and School Board Policy).

Access Availability

Access to the District's Electronic Communications System, including the Internet, is made available to students and employees primarily for instructional and administrative purposes and in accordance with administrative regulations. Limited personal use of the system shall be permitted if the use;

1. imposes no tangible cost on the district;
2. does not unduly burden the district's computer or network resources; and
3. has no adverse effect on the employee's job performance or on a student's academic performance.

Monitored Use

The District reserves the right to monitor all technology resource activity. Student use of the computers and computer network is only allowed when supervised by staff members Electronic mail transmissions and other use of the electronic communication system by students and employees are considered a matter of public record and should not be considered private. Designated District staff shall be authorized to monitor such communication at any time to ensure appropriate use.

Network

Improper or illegal use of any computer or the network is prohibited. This includes the following:

- Using racist, profane, or obscene language or objectionable materials
- Attempting to or harming equipment, materials or data
- Attempting to or sending anonymous messages
- Using the network to access inappropriate material

- Knowingly placing a computer virus on a computer or on the network
- Using the network to provide addresses or other personal information that others may use inappropriately
- Accessing of information resources, files and documents of another user without their permission

Security

Each user is assigned an individual account for accessing district technology resources. You may not share your account with anyone or leave the account open or unattended. Attempting to log on or logging on to a computer or E-Mail system by using another's account and password is prohibited, and is a punishable disciplinary offense. Assisting others in violating this rule by sharing information or passwords is unacceptable. Users are expected to change passwords regularly to maintain security and confidentiality. Users are responsible for saving all documents to the server. Technology support staff will attempt to recover lost or damaged documents only if they have been saved to the server.

Internet Safety / Filtering

As required by the Children's Internet Protection Act (CIPA) the district maintains a filtering system that blocks access to information considered obscene, pornographic, inappropriate for students or harmful to minors as defined by the federal CIPA guidelines. The following measures are in place to protect students' Internet use.

1. Student's access to inappropriate materials is controlled through the Internet filter.
2. The district's private E-Mail system does not allow outside access to the directory of users.
3. Students are not allowed to reveal personal address or phone number information when using the Internet or other electronic communication systems.
4. Chat and Instant Messaging using the district system will be supervised and monitored.
5. Students may participate in prearranged Internet chat and instant messaging sessions with experts that have been scheduled by Central Heights ISD staff and approved by the appropriate campus administration.
6. Chat and Instant Messaging is restricted to pre-approved activities only and will be actively monitored.

Although the district will use these preventative practices, stakeholders 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 and/or objectionable material, and that these systems reside outside the administrative control of the district. The following guidelines should also be observed:

1. Never assume that someone you encounter online is who they say they are.
2. Never arrange a face-to-face meeting with someone you encounter online.
3. Never respond to messages or communications that you feel are threatening, obscene, or make you uncomfortable.
4. If you come into contact with one of the above situations, please notify your campus administrator.

Copyright

All users are responsible for adhering to existing copyright laws and District Policy pertaining to software, resources, reference materials, video, sound and graphics. For displayed works you are expected to cite the source of your information. Questions concerning copyright can be referred to the campus or district administrative staff, or campus librarians, for clarification or assistance.

E-mail

The district E-Mail system is used to communicate both internally in the district and with outside agencies. E-Mail communications are a matter of public record and should not be considered private. All users are expected to adhere to the following district policies regarding e-mail communications.

1. E-Mail should not be used for private or commercial offerings of products or services for sale or to solicit products or services.
2. E-Mail should not be used for political or religious purposes.
3. Forgery, or attempted forgery, of electronic mail is prohibited.
4. E-Mail messages that cause network congestion or interfere with the delivery of mail to others are not acceptable. E-Mail from mailing lists (also known as “list serves”) must not affect the system’s performance.
5. E-Mail messages and conference postings will not contain improper language, swearing, vulgarity, ethnic or racial slurs or any other inflammatory language or content. Conference postings will follow these District guidelines or be removed.
6. Do not reveal personal information about yourself or others.
7. Do not send chain letters, or forward messages to large groups of users.
8. You are expected to be polite and professional.
9. You are responsible for material sent by and delivered to your e-mail account.

Electronic Phishing

Any electronic publication or web site that represents the District or any organizational unit of the District must meet all guidelines and requirements in accordance with district policy.

Forgery

Forgery or attempted forgery of electronic data is prohibited. Attempts to read, delete, copy, or modify the electronic data (including E-Mail messages) of others are prohibited. Using another individual’s account or materials for the purpose of copying academic work is a punishable disciplinary offense.

Software

Please contact the District Technology Department to install software on District computers. The installation of software or files not owned by the district on District computers is prohibited. Only software approved, licensed and/or purchased by the District should be installed on District computers. Proper licensing documentation must be maintained.

Vandalism

Any malicious attempt to harm or destroy District equipment or materials, the data and files of another user on the District's system, or any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance may be viewed as violations of District policy and administrative regulations and, possibly, as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creating of computer viruses. Vandalism as defined above will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, hardware, or software costs and is a punishable disciplinary offense.

Disclaimer

The District shall not be liable for inappropriate use of electronic communication resources, violations of copyright restrictions or other laws, mistakes or negligence, and costs incurred. The District shall not be responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the Internet. The District's system is provided on an “as is, as

available” basis. The District does not make any warranties, whether expressed 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.If you have questions or need further information, please contact the campus principal or the Technology Department.

Technology Responsible Use Policy

Our staff and students use technology to learn. Technology is essential to facilitate the creative problem solving, information fluency, and collaboration that we see in today’s global economy. While we want our students to be active contributors in our connected world, we also want them to be safe, legal, and responsible. This Responsible Use Policy (RUP) supports our vision of technology use and upholds in our users a strong sense of digital citizenship. This policy applies to all CENTRAL HEIGHTS ISD computer networks (including the resources made available by them), and all devices connected to those networks.

Responsible Use and Digital Citizenship

Respect Yourself: I will select online names that are appropriate, and I will be polite and use appropriate language/content in all online posts.

Protect Yourself: I will not publish personal details, contact details or a schedule of activities for myself or anyone else. I understand that unless otherwise authorized, I am the owner of my accounts, and I am responsible for all activity initiated by and/or performed under these accounts. I understand that it is my responsibility to appropriately secure my account credentials. I understand that I am responsible for maintaining and backing up all of my own data. If I am uncertain whether a specific computer activity is permitted or appropriate, I will ask a teacher/administrator before engaging in that activity.

Respect Others: I will not use technologies to bully or tease other people. I will not make audio or video recordings of students/employees without their prior permission. I understand that posing as someone else is forbidden and I will not pose as a user other than myself when online. I will be careful and aware when printing to avoid wasting resources and printing unnecessary items.

Protect Others: I will help maintain a safe computing environment by notifying appropriate campus officials of inappropriate behavior, vulnerabilities, risks, and breaches involving campus technology.

Respect Intellectual Property: I will suitably cite any and all use of websites, books, media, etc. I will respect all copyrights.

Protect Intellectual Property: I will request to use the software and media that others produce.

General Policies

- The purpose of a Central Heights ISD user account is to access the Central Heights ISD network and facilitate creativity and innovation. We use this network to support

communication and collaboration. We use technology to extend research and information fluency, to collect and analyze data and to solve problems.

- Access is a privilege, not a right. Access entails responsibility, and inappropriate use may result in cancellation of those privileges.
- Central Heights ISD user accounts are owned by the Central Heights ISD; consequently they are subject to the Open Records Act. All digital files associated with user accounts may be retrieved by Central Heights ISD staff at any time without prior notice and without the permission of any user. The Central Heights ISD reserves the right to monitor all accounts in order to maintain system integrity and to ensure responsible use.
- Students should have no expectation of personal privacy in any matters stored in, created, received, or sent through the Central Heights ISD computer network. These are subject to review by the Central Heights ISD at any time, with or without notice, with or without cause and without the permission of any student or parent/guardian.
- A content filtering solution is in place in order to prevent access to certain sites that may contain inappropriate material, including pornography, weapons, illegal drugs, gambling, and any other topics deemed to be of non-educational value by the Central Heights ISD. The Central Heights ISD is not responsible for the content accessed by users who connect via their own 3G type service (cell phones, air-cards, etc.).

Governmental Laws

Technology is to be utilized in conformity with laws of the United States and the State of Texas. Violations include, but are not limited to, the following:

- Criminal Acts – These include, but are not limited to:
- unauthorized tampering, cyber stalking, vandalism, harassing email, child pornography, cyber bullying
- Libel Laws - You may not publicly defame people through published material.
- Copyright Violations - Copying, selling or distributing copyrighted material without the express written permission of the author or publisher (users should assume that all materials available on the Internet are protected by copyright), and/or engaging in plagiarism.

Google Apps and Other Third Party Accounts

In accordance with our district mission, goals and our vision for technology our students may require accounts in third party systems. Many of these accounts will be used at school for school related projects but may also be accessed outside of school with their parents' permission. The use of these accounts will help our students to master effective and proper online communications as required in the PreK-12 Technology Applications Standards.

Consequences

I understand and will abide by the Technology Responsible Use Policy. Consequences for breaking the agreement could include suspension of your accounts and network access. In addition you could face disciplinary/legal action including but not limited to: criminal prosecution and/or penalty under appropriate state and federal laws.

The following actions are not permitted and could result in the consequences outlined above:

- Users may not attempt to disable or bypass the CENTRAL HEIGHTS ISD content filter.
- Users may not illegally access or manipulate the information of a private database/system such as txGradebook and other student information systems.
- Users may not install unauthorized network access points, or other connections that may not effectively integrate with existing infrastructure.
- Users may not use their accounts for non-school related activities including but not limited to:

- Using the Internet for financial gain, personal advertising, promotion, non-government related fundraising, or public relations
- Political activity: lobbying for personal political purposes, or activities such as solicitation for religious purposes.
- Users may not take a Chromebook out of the assigned classroom without a teacher's permission.
- Users may not take a Chromebook off campus without permission.
- Illegal downloads of any sort (Apps, VPN's, Movies, Music, etc…) are strictly prohibited.
- Users may not access other students' accounts without permission.
- Inappropriate profile pictures are strictly prohibited.
- Inappropriate use of language while using Central Heights accounts are prohibited.
- Users may not send, save, view, forward, or create harassing or offensive content/messages. Offensive material includes, but is not limited to, pornographic, obscene, or sexually explicit material, sexual comments, jokes or images that would violate school policies. The school policies against harassment and discrimination apply to the use of technology.

The Director of Technology and the campus principal will deem what is considered to be inappropriate use of the Central Heights ISD computer network. They may suspend an account or network access at any time. In addition, the administration, faculty, and staff of Central Heights ISD may request that a user's account be suspended or denied at any time. If a signed copy of this document is not returned to school by the end of the first week, it will be assumed that you agree to the provisions outlined within it.