Acceptable Use Policy (AUP)
Staff Responsibilities for Using Alief ISD District Technology

The use of Alief ISD electronic devices, computer systems and networks, software, and Internet is to support research and education in and among academic institutions by providing access to unique resources and the opportunity for collaborative work. Content residing on district owned resources is property of Alief ISD. The use of Alief ISD electronic devices, computer systems, computer networks, software, and Internet is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. Illegal activities are strictly forbidden. All information including electronic mail (email) is not guaranteed to be private. Messages relating to or in support of illegal activities may be reported to the appropriate authorities. The campus and central administrative team will deem what is inappropriate use, and their decision and the consequences are final. Appropriate use of digital resources and devices must follow all requirements, approval processes, and guideline statements set forth in the Responsible Use Practices Guideline document and the Bring Your Own Device Policy. **"Alief ISD will educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response".**

Network Standards

1. Using the network resources in such a way that would disrupt the use of the network is prohibited.
2. Training and monitoring students in the safe and proper use of both internet and network resources and Student AUP, RUP, and BYOD.
3. Revealing personal information of yourself or others is prohibited.
4. Logging off or locking the device when your session is complete.
5. Sharing your district issued username and password is prohibited.
6. Learning proper network navigation techniques to facilitate printer selection, document saving, and data confidentiality.
7. Using personal cell phones or devices must adhere to the district Bring Your Own Device Policy and campus guidelines.
8. Minimum technology competency skills are an expectation.
9. Use and connectivity to Alief BYOD network is only for instructional purposes.
10. District reserves the right to delete potentially harmful content identified on any device utilizing district networks or resources.

Use of Data

1. Access, utilize, and store confidential data responsibly.
2. If any device storing data is lost or compromised in any way, report immediately to a campus administrator.
3. The district reserves the right to remove any inappropriate or potentially harmful data from any media storage device that is being used in the school environment.
4. Use strong passwords and follow network etiquette to secure sensitive data.
5. Do not allow access to others by placing student information on unsecured network devices/ personal devices/or cloud storage.
6. When using a BYOD device, all student data and pictures must be deleted daily.
7. Protect confidentiality and act responsibly when accessing data or resources.
8. Protect Staff and Student identifiable data from misuse.
9. Do not falsely manipulate/alter or misrepresent data.
10. It is a violation to knowingly attempt to access resources at work that you don't have permission to utilize as part of your job function.
11. It is your responsibility to report instances where you have access to data/resources that are not part of your job function.

Email Use

1. Email is a district service and is to be used for instructional and administrative purposes.
2. Group mailing to the whole staff must first be cleared with the administrator to ensure appropriateness.

3. Sent messages cannot always be retrieved. Be just as careful when sending e-mail as you would be in committing to paper your thoughts or reactions.
4. Be polite. Messages typed in all capital letters are the computer equivalent of shouting and considered rude.
5. Using inappropriate language such as swearing or vulgarity, or ethnic or racial slurs, or obscene pictures is prohibited.
6. Pretending to be someone else when sending/receiving messages is prohibited.
7. Board policy can be viewed at: http://pol.tasb.org/Policy/Search/584?filter=email%20use
8. Student email is a district service and is to be used instructionally upon teacher training.

Internet Acceptable Use

1. Access only course related materials for educational purposes.
2. Credit all resources appropriately when utilizing information accessed (observe all copyright guidelines).
3. Train students in the proper use of all Internet resources.
4. Train students to be responsible digital citizens, to report cyber bullying, and to consider the consequences of their digital footprint.
5. Convey to students expectations for appropriate use.
6. Convey to students consequences for inappropriate use such as: cyber bullying, off-task behavior, impolite or abusive language, accessing unapproved sites, sending/printing material or information without permission.
7. Monitor student use to keep students on task and maintaining focus.
8. Supervise student use and intervene when necessary to ensure appropriateness of materials being accessed.
9. Follow school procedures for preventing unauthorized use.
10. Campus must maintain student/parent/staff agreement forms on file.
11. Use of extended opportunities for internet access, such as sites currently blocked by the filter, requires following all requirements, approval processes, and guidelines including understanding statements set forth in the Responsible Use Practices guideline document.

Restrictions

1. Installing programs to the district's network system without appropriate authorization is prohibited.
2. Copying and distributing unauthorized materials such as, but not limited to, video, audio, and image files is prohibited.
3. Use of district equipment for personal financial gain is strictly prohibited.
4. It is prohibited to use any personally owned electronic devices, such as, but not limited to, computers, mobile tablets, printers, scanners, projection devices, or wireless network cards for instructional or administrative use on school property without following guidelines and training requirements established by the district.
5. Damaging and vandalizing any electronic devices, computer systems or computer networks is prohibited.
6. Staff assumes responsibility for damage, theft or loss of equipment taken off school property.
7. Printing non-work related related materials is strictly prohibited.
8. Accessing and using non-district provided email at work using district resources during work hours is strictly prohibited.
9. Unprofessional use of personal devices at work is prohibited.

Violations of the above may result in disciplinary actions and/or loss of access privileges.

District Training

1. All new staff members are required to take online professional development training covering digital citizenship, tools and resources facilitated by Instructional Technology.
2. All staff members are required to review the AUP and RUP annually and have current signature pages of compliance on file at the campus and/or department level.
3. All staff utilizing extended opportunities for device use and internet access opportunities must

meet minimum technology competency standards and follow all requirements, approval processes and guidelines including understanding statements set forth in the Responsible Use Practice Guideline document and Bring Your Own Device Policy.

Substitutes

Daily Substitutes

1. No network, email, and computer access allowed.
2. Students are not allowed to access computers while a substitute is present unless it is a technology curriculum based class or facilitated by a staff member
3. Teachers must never give a substitute their login or password information under any circumstances.

Long Term Substitutes & Student Teachers

1. Network and email access allowed.
2. Must follow Staff AUP and RUP guidelines where appropriate, and have signature form on file.
3. Remote access/terminal server access is not allowed.
4. Grade book access
    a. Will have access to teacher's online grade book and is expected to enter grades.

Visiting Instructors

1. Network access only.
2. Must follow Staff AUP and RUP guidelines and have a signature form on file.
3. Email access, online grade book, and remote access/terminal server access is not allowed.

Family Engagement Center Visitors

1. Family Engagement Center visitors will log in with the district-issued parent center login account.
2. Must follow Staff AUP and RUP guidelines and have a signature form on file.

Disclaimers

- Alief ISD makes no warranties of any kind, either expressed or implied, for the provided access.
- The staff, faculty, school, and Alief ISD 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 Alief ISD resources.
- The staff, faculty, school, and Alief ISD are not responsible for information obtained through district network resources resulting in criminal or terrorist activities.
- Alief ISD is not responsible for damage or theft of any personally owned devices.