Cleburne County Schools

Acceptable Technology Practices for Employees and Teachers

Rules, Restrictions, and Guidelines

The following rules, restrictions, and guidelines have been developed in accordance with Board Policy §4.8.4. All users, in the process of logging onto the District's network or onto web-hosted applications used by the District, must agree to abide by all District, must agree to abide by all District and school rules, Board policies, state, local, and federal laws, and these Acceptable Use Practices. The District may use software or other measures to monitor network and Internet activity, as needed. Administrators, the District Technology Coordinator, and other designees will make determinations as to whether specific uses of technology are consistent with applicable rules and policies.

General Rules

Passwords

Employees will be held responsible for activity on their account, Therefore, employees should:

- Create "strong" passwords, keep them secure, and change them annually or more frequently.
- Use different passwords for the District's Student Information System, Chalkable, and general network use.
- Use only their authorized network account. (Unauthorized attempts to login as any other individual are prohibited.)
- Not give students their login credential or allow students to use technology that has been logged into by a staff account.
- Close programs and lock or log out of devices when they will be unattended even for a short time.

Equipment

Employees shall not:

- Intentionally harm, destroy, disable, or remove parts from any district technology. Employees may be held financially responsible for the repair, replacement, or reconfiguration of affected equipment.
- Employees shall not modify computers in any way without the permission of school administrators.
- Invite or allow outside individuals to repair or modify district technology without first obtaining permission from the Technology Department.
- Move or dispose of district equipment without following proper equipment transfer procedures.
- Remove equipment from their building without first completing the appropriate permission form.
- Bring in, buy, or use Wireless Access Points or network switches which have not been specifically approved of by the Technology Department for use on the District's network.
- Use personal equipment or accounts to provide students with unfiltered Internet access.

Use

Employees shall not:

- Attempt to disable or circumvent security measures, including Internet filtering software.
- Use technology for non-educational, commercial, political, or "for-profit" purposes.

- Use technology for antisocial behaviors such as harassment and discriminatory remarks, etc.
- Intentionally view, seek, obtain, or modify information, other data, or passwords belonging to other users.
- Install unlicensed software onto any District device.

Wasting or Monopolizing Resources

Employees shall not waste or monopolize resources. For example, over consumption of network bandwidth or server storage space for personal purposes such as streaming radio stations or other media; downloading software updates onto personally owned devices; storing personal graphic, video, or audio files; or 'spamming' fellow staff with non-work related messages.

Internet Filtering and Access

Access to the Internet

It is the policy of the Board to provide its employees and students with Internet access for the purpose of supporting activities that serve, and are consistent with, the identified educational and administrative objectives of the District.

Filtering

The District filters Internet access in order to comply with Federal rules and to ensure that staff and students are protected from harmful and inappropriate material. However, no technology protection measure will be 100% effective. Therefore, all users should report any sites which contain inappropriate materials or materials harmful to minors to the Technology Coordinator or his/her designee. The District will not be responsible for any damage suffered by the user due to a technical failure to block or filter inappropriate Internet sites or electronic communications.

- Teachers should pre-screen websites before showing to their class to ensure suitability.
- Teachers should supervise and monitor their student's use of Internet and/or electronic communications in order to assist in ensuring that their use is consistent with all rules, regulations, and protection measures.
- Teachers should know which of their students have a letter on file from the parent disallowing them from using the Internet independently, and enforce these restrictions.

Data Plans and Filtering

- Employees may not purchase data plans which would provide students with unfiltered Internet access with "school" funds (l.e., local school funds, District, Federal, or donated funds passing through system accounts} .
- Employees may not "tether"' a device to District technology on a District campus in order to bypass the District's Internet filter.

Requests for Opening up Filtered Sites

Employees may request a review of filtered sites. They may also request a temporary release of specific sites at specific workstations to complete their work. Such requests should be directed to the District Technology Coordinator

Working with Students

Supervision of Students

Employees are expected to monitor their student's use of technology in order to ensure that they comply with the Technology Acceptable Use Practices (AUP) found in the Student Code of Conduct. Providing Online Behavior Education Teachers and school staff should model appropriate online behavior and educate students about all aspects of being a responsible digital citizen, including cyber bullying, digital copyright issues, reputation building, plagiarism, privacy, identity theft, and risks from various forms of predators.

FERPA and Technology

The use of technology can greatly increase the exposure of protected information whether via email, websites, or use of various software programs. Employees are expected to understand and comply with the provisions of Federal Family Education Rights Protection Act, which requires that schools provide and protect information regarding its students. Employees should take extra precautions when using technology to transmit any protected information in order to be sure it will only reach the appropriate recipients. Employees with higher levels of data permissions may be asked to sign Security Agreements that further define rules regarding protecting data.

Online Media Publications

Teachers should familiarize themselves with the Media Release provisions of the Student Code of Conduct. This portion of the Code of Conduct refers to a wide range of media, both in print and online formats. Even in cases where parents have not written the school denying the school permission to publish their child's image, employees should never publish pictures of students on their own personal websites or upload them to other websites not officially used by the School/District. Parents must be able to expect to find any images of their child published by District employees on our websites. They should not have to seek out the many different online media sites that teachers may use as individuals to ensure that the use of their child's image is keeping with their expectations.

Anti-Virus, Phishing, and other Forms of Cyber Attacks

Everyone must do their part to prevent our devices and network from being infiltrated and damaged by various forms of malicious behavior. Employees should:

- Not disable the antivirus software on District technology.
- Never respond to emails claiming that they need you to update your email account or password. The Technology Department will NEVER ask you to do this. Delete these emails NEVER click on links within these emails whether from home computers or work computers.
- Make sure that laptops which are taken off site or used infrequently are connected to the network periodically so that the antivirus software can be updated.

Cleburne County Schools

Acceptable Technology Practices for Employees and Teachers

Rules, Restrictions, and Guidelines

I acknowledge that I have received and read the Cleburne County Schools Teacher Technology Practices Rules, Restrictions, and Guidelines.

Employee Signature:______________________________________Date:__________________

Employee Name Printed:____

Home School Assignment:____