Jefferson R-VII School District

2024/2025 Employee Technology Acceptable Use Agreement

Overview

Access to technology is necessary for the District's mission The Internet offers extensive and diverse resources. We believe in the educational value of technology to support curriculum and learning.

The Jefferson R-VII School District takes exhaustive steps in providing safe and secure technology. Employees will access the Internet through web filters and other monitoring systems. The District complies with the Children's Internet Protection Act (CIPA); however, the Internet also includes material that is not of educational value in the context of a school setting. There is information which may be judged inaccurate, abusive, profane, sexually oriented, hate-based, or illegal. Jefferson R-VII School District does not condone or permit the use of this material.

Activities Not Permitted

- Searching for or viewing content that is sexually explicit, profane, violent, abusive, or illegal is prohibited.
- Employees are prohibited from sending messages containing threats, profanity, sexual references, insults, harassment, or obscene language.
- Employees must not share account information, such as usernames and passwords.
- Employees are responsible for ensuring that no malicious damage is done to District technology.
- Employees may not copy, save, or distribute copyrighted material without permission.
- Employees may not participate in any activity that violates District policy, school rules, local, state, or federal law.
- Employees will not use privately owned technology on District networks unless approved by the Technology Department.
- Employees may not use Virtual Private Networks (VPN) whose purpose is to circumvent filtering.
- Employees will promptly disclose to an administrator or director any message received that is inappropriate or makes the employee feel uncomfortable.
- Employees will not register students with 3rd-party service providers without approval from District Administration.

Password Security

Staff members are responsible for managing their passwords and shall be responsible for all actions and functions performed by their username. School personnel must comply with all District-established rules regarding passwords. These rules dictate the number of characters in the password, the nature of the characters used in the password, and the frequency of password changes. Any school employee who suspects their password has been compromised must report the situation to administrators as soon as possible. Intentionally divulging a password will be considered serious misconduct. The consequences of password security violations will be commensurate with the seriousness of the breech. All employees will be required to use two-factor authentication for accessing critical information systems as determined by the District.

Equipment Rules

Under no circumstances are employees to alter the hardware configuration of the technology assigned to them. All technology related purchases must be coordinated through the Technology Department. Additionally, employees are not permitted to change network wiring or the configuration of network devices in their offices or classrooms. Tampering with or modifying computers or network devices are grounds for disciplinary action.

Information Content & Uses of the System

Employees will not publish any information which violates or infringes upon the rights of any other person or any information which would be abusive, profane or sexually offensive to an average person, or which, without the approval of the system administrators, contains any advertising or any solicitation of other members to use goods or services. All employees must comply with the guidelines of the Family Educational Rights and Privacy Act (FERPA).

District technology is for professional use only. Commercial and personal uses are prohibited unless prior written consent from District administration is given. Employees will not use systems to conduct any business or any activity, or solicit the performance of any activity which is prohibited by law.

Employees understand that the system administrators of the Jefferson R-VII School District do not have control of the content of information residing on these other systems. Users are advised that some systems may contain defamatory,

inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material. The District does not condone the use of such materials and does not permit usage of such materials.

Copyrighted Material

Jefferson R-VII School District requires employees to be familiar with copyright law and to act ethically in the use of copyrighted material for instruction. Copyrighted material must not be placed on any system connected to Jefferson R-VII Public Schools without the author's permission. Illegal (pirated) software will not be allowed on the system under any circumstances.

Email

All employees have Email accounts. The District expects each employee to check their Email frequently as instructed by their supervisor. Messages sent and received by employees are retained indefinitely.

Email should not be considered private. System administrators will not intentionally inspect the contents of Email sent by an employee to an identified addressee, or disclose such contents to other than the sender, or an intended recipient, without the consent of the sender or an intended recipient, unless required to do so by law or policies of Jefferson R-VII School District, or to investigate complaints regarding mail which is alleged to contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material. Employees must use their District provided Email accounts to conduct District business or instruction.

By signing this agreement you have read and agreed to the terms outlined in this document.

Signed:_____ Date:_____

Printed Name: _____