Red Oak Community School District
Employee Technology Acceptable Use Policy

Introduction

The Red Oak Community School District authorizes district employees to use technology owned or otherwise provided by the district as necessary to fulfill the requirements of their position. The use of district technology is a privilege permitted at the district's discretion and is subject to the conditions and restrictions set forth in applicable Board policies, administrative regulations and this Technology Acceptable Use Policy.

The district expects all employees to use technology responsibility in order to avoid potential problems and liability. The district may place reasonable restrictions on sites, material, and/or information that employees may access through the system. The district is not responsible for financial obligations arising from unauthorized use of the system.

Each employee who is authorized to use district technology shall sign this Technology Acceptable Use Policy Agreement as an indication that he/she has read and understands the policy.

Employee Obligations and Responsibilities

Employees are expected to use district technology safely, responsibly and primarily for work-related purposes. Any incidental personal use of district technology shall not interfere with district business, operations or safety and security of district technology. Employees shall not share their assigned account information, passwords or other information used for identification. Employees shall not gain unauthorized access to the files or equipment of others.

Employees are prohibited from using district technology resources for improper purposes, including but not limited to;

- Access, post, display, or otherwise use material that is discriminatory, defamatory, obscene, sexually explicit, harassing, or threatening.
- Disclose confidential or sensitive district, employee or student information without prior authorization from Administration
- Disclose account information (passwords, passphrases, authorization codes)
- Engage in personal, commercial or other for-profit activities for personal benefit.
- Engage in unlawful use of district technology for political lobbying.
- Infringe on copyright, license, trademark or other intellectual property rights
- Intentionally disrupt or harm district technology
- Installation of unauthorized software.
- Engage in or promote unethical practices or violate any law or Board policy, administrative regulation or district practice.

Privacy

The district reserves the right to monitor and record all use of district technology, including, but not limited to, access to Internet or social media, communications sent or received from district technology, or other uses within the jurisdiction of the district. Such monitoring/recording may occur at any time without prior notice for any legal purposes including, but not limited to, record retention and distribution and/or investigation of improper, illegal, or prohibited activity. Employees should be aware that, in most instances, their use of district technology cannot be erased or deleted.

Cybersecurity

Employees are required to abide by all district cybersecurity policies and procedures. If a district employee becomes aware of any cybersecurity problem or misuse of district technology, he/she shall immediately report such information to the Director of Technology. This also includes reporting any mechanisms for scams, privacy breaches, phishing attempts, or potential security threats.

Employees shall participate in district cybersecurity training and will be exposed to multiple cybersecurity simulations throughout the year. Some software may require the use of MFA (Multi-Factor Authentication). Employees may be required to utilize various methods to authenticate including, but not limited to, personal cellular devices, prompts, and pre-generated codes.

Ownership

Access to computing resources is a privilege, not a right and the privilege can be suspended immediately without notice. All user accounts issued by the district are considered property of the district. School issued accounts should not be used for personal use. These user guidelines extend beyond the school district's physical building, such as school issued email accounts, hardware, or software used when off the school district's property. Staff members will not retain proprietary rights related to the materials designed or created by such user if district hardware/software is used unless those rights are transferred to the user. Staff members leaving the district will have their accounts disabled as of their final contract day unless other arrangements are made.

Employee Acknowledgement

I have received, read, understand, and agree to abide by this Technology Acceptable Use Policy and district policies and regulations governing the use of district technology. I understand that there is no expectation of privacy when using district technology. I accept the districts cybersecurity policies and procedures when utilizing district technology and software. I further understand that any violation may result in revocation of user privileges, disciplinary action and/or appropriate legal action.

I hearby release the district and its personnel from any and all claims and damages arising from my use of district technology or from the failure of any technology protection measures employed by the district.

_____
Signature

_____
Employee Name (Please Print)

_____
Date