516 Technology Resource Usage

Effective Date: 9/1/2015

Revision Date: 11/15/2023

Technology resources include, but are not limited to, computers, networks, communications systems, equipment, software, devices, and access to cloud services.

This policy is designed to establish acceptable and appropriate use of technology resources and digital files used by United General District 304 staff, contractors, volunteers, and others who conduct District business. This Policy does not attempt to address every possible situation that may arise. Good judgment, etiquette, and common sense should be exercised while using District technology resources. The main points to remember are:

- Technology resources are provided to carry out legitimate District 304 business. All use of technology resources must be consistent with the intent and requirements of all District policies and work rules.
- There is no right to privacy in the use of District technology resources. As a public entity, all communications transmitted through or saved on District technology resources are subject to Public Records Requests and may be monitored or reviewed by management at any time without notice to the user.
- Users are expected to act lawfully, ethically, and professionally, and to exercise good judgment. District 304 strives to maintain a workplace free of harassment and sensitive to the diversity of its employees. Therefore, District 304 prohibits the use of technology resources in ways that are disruptive, offensive to others, or harmful to morale.
- Users who are granted access to critical data are responsible for its protection.
- Incidental use for personal needs is allowed as long as that activity does not interfere with District business or conflict with any District policy or work rule.
- Use of technology resources in violation of this policy is subject to disciplinary action up to and including termination.

Security

All members of staff are required to take and pass annual Cybersecurity training at the start of employment, and every year thereafter.

Multi-factor authentication (MFA) is provided by the District and must be used when logging into staff work accounts. MFA may also be required when accessing certain applications.

Staff with access to critical information are responsible for its protection. Any concerns about a potential security breach must be reported to a member of the Executive Team who will determine the next course of action.

Staff who encounter or observe vulnerability in any application or network security must immediately report it to a member of the Executive Team who will determine the next course of action.

Passwords

The District provides a password manager application to be used as the method for logging and maintaining passwords to District-related accounts. It is safe to store credit card information in this application, but not required.

Passwords and credit card information should not be stored in Internet browser applications. Users should disable the collection and auto-fill of such information in their browsers. Please request assistance if needed.

Stealing, using, or disclosing someone else's password without authorization is prohibited.

Passwords for all District-related accounts should be:

- A minimum of 8 characters long, including at least one of the following:
    - Number
    - Lower case letter
    - Upper case letter
    - Special character such as -_+!$,/()*& (if allowed by the app)
- Unique – passwords should not be reused within a year, and the same password should not be used across multiple applications.
- It is recommended that passwords are changed at least once per quarter. Some applications or those with access to critical data may be required to change their passwords more frequently.

Network Access and Usage

The installation, removal, or altering of any software on District-owned equipment is

prohibited without authorization from their supervisor. The supervisor may consult with the Tech Supervisor and/or the Executive Team. During installation, new software is virus-scanned by our IT services provider.

Disabling, altering, overriding, or turning off any mechanism put in place for the protection of the network and workstation environments is prohibited.

Transmission, distribution, or storage of any information or materials in violation of federal, state, or municipal law is prohibited. Software that is copyrighted or licensed may not be shared or illegally distributed. Copyright violations are federal offenses that may result in civil and criminal penalties.

Internet Usage

Use of the Internet, as with the use of all technology resources, should conform to all District policies and work rules. Internet usage may be monitored at any time. Except for District business related purposes, accessing/visiting sites such as the following are prohibited:

- Adult Content
- Games
- Violence
- Personals and Dating
- Gambling
- Hacking

Messaging System Usage

Messaging systems include email, chat, instant messaging, voice, and telephone services.

Use of messaging systems must be consistent with the standards expected in any other form of written or verbal communication within the District. Users are expected to act lawfully, ethically, and professionally, and to exercise good judgment. Communication from District accounts must adhere to District policies and may not contain:

- Harassing or threatening content
- Sexually explicit messages or images, or off-color jokes
- Hate speech or discrimination against any person or group based on race, national origin, religious affiliation, gender, sexual orientation, socioeconomic status, disability, or age
- Personal views on political or religious causes

- Language that defames or slanders an individual or group, or disparages another organization's products or services
- Commercial ventures not related to District business
- Messages or material that could damage the District's image or reputation

Use of the All-Staff email list is monitored and approved on a case-by-case basis by a member of the Executive Team. Do not use "Reply-All" when responding to an All-Staff email message.

Email addresses of those outside our organization may not be added to any mass mailing list without their expressed permission.

Credit card information must never be sent or received via email or chat systems.

Personal Use
Technology resources may be used during non-work time for incidental personal use as long as it does not:

- Interfere with business
- Reduce productivity or performance
- Pose a risk to security
- Expose the District to liability or financial loss
- Conflict with District policy or work rule

Users may not download or install third-party software on District devices unless used in the course of District business.

Please note that any data stored on District systems or cloud services are subject to search and may be disclosed in response to public disclosure requests.

Social Media
See the Social Media Quickstart Guide and Social Media Acknowledgment located on the staff intranet page which address:

- The creation and use of social media accounts
- Intellectual property and media consent
- Content guidelines
- Reposting/sharing previously created social media content
- Appropriate conduct on social media platforms
- Charges and payments

NOTE: Policy 516 Computer and Email Usage and Policy 517 Internet Usage have been combined into comprehensive Policy 516 Technical Resource Usage.