

 <p>TUCSON UNIFIED SCHOOL DISTRICT</p> <p>POLICY REGULATION</p>	REGULATION TITLE: Acceptable Use of Technology Resources
	CODE: EJA - R
	LEAD DEPARTMENT: Technology Services

Acceptable Use of Technology resources means technology must be used in a responsible, efficient, ethical and legal manner and in accordance with the policies and educational objectives of Tucson Unified School District (TUSD).

This regulation is designed to guide employees in the acceptable use of computer systems, networks, and other information technology resources at TUSD, and should be read and interpreted in conjunction with all other TUSD policies including but not limited to policies prohibiting harassment, discrimination, offensive conduct or inappropriate behavior.

Guiding Principles

- The use of TUSD technology resources, including but not limited to, the Internet (World Wide Web), electronic mail, hardware, software and online services, to access, transmit, publish, display or retrieve any material in violation of any U.S. or State laws or regulations or any material that is contrary to the educational goals of the District is prohibited. This includes, but is not limited to:
 - Copyrighted material.
 - Pornographic, obscene or other sexually oriented material (pornographic means pictures or writings that are intended to stimulate erotic feelings by the description or portrayal of sexual activity or the nude human form).
 - Material protected by trade secret.
 - Material which is threatening, promotes violence or advocates destruction of property.
 - Material which advocates or promotes violence or hatred against a particular individual or groups of individuals or advocates or promotes the superiority of one racial, ethnic or religious group over another.
 - Material related to gambling.
 - Material related to any illegal activity.
 - Material related to political elections. State law prohibits the use of any district resources for political activities.

- Employees are reminded that use of any and all TUSD property is primarily for TUSD business. Any personal use of the Internet is expected to be on the user’s own time and is not to interfere with the person’s job responsibilities.

- In addition, employees, while using TUSD technology resources, may not:

- Use inappropriate or profane language or material likely to be offensive to others in the school community, including sexually harassing or discriminatory material.
- Use software without proof of proper licensing.
- Use software that has not been approved by TUSD's central Technology Department for support of learning/teaching.
- Impersonate another user or transmit or publish material anonymously.
- Conduct a business or other for-profit activity.
- Use district technology in such a way that the district will incur an expense unless spending authority has been granted by the appropriate administrator.
- Destroy, modify or abuse district owned technology or disrupt the operation of any network within the school district or any network connected to the Internet, including the use, attempted use or possession of computer viruses.
- Create, transmit or retransmit chain mail.
- Failure to report any violation of the provision contained herein to their supervisor.

Employees/contractors will:

- Use up-to-date virus protection software on any computer on which district files are created, saved or modified; this includes electronic mail.
- Take all reasonable precautions, including password maintenance and file and directory protection measures, to prevent the use of their account by other persons.
- Check district electronic mail accounts on a regular basis. Clean and destroy unused files on a regular basis.
- Be sensitive to the fact that electronic materials should contain proper spelling, grammar and appropriate writing conventions and accuracy of information in all electronic materials.
- Submit a request to TTS for any download; install or configuring that is necessary to perform a specific job.
- Protect the privacy of TUSD's confidential material, such as home addresses and/or personal phone numbers of others.
- Secure their workstation by logging off or by pressing Ctrl-Alt-Del and Enter. Staff members are not to leave workstations unattended at any time while logged on to the TUSD network or workstation.

Email Usage

To ensure the safety and security of sensitive data on the District's network, the following is a list (non-exhaustive) of Personally, Identifiable Information (PII) that shall be prohibited from transmitting via email:

- Full name
- Social security number
- Driver's license
- Mailing address

- Credit card information
- Passport information
- Financial information
- Medical records

District Services:

- The District reserves the right to log an employee's use of the Internet and monitor/limit/file-server space utilization.
- The District reserves the right to examine e-mail, personal file directories, Internet usage and other information stored on TUSD computers, including monitoring for appropriate use as defined in EJC – Electronic Mail.
- An Administrator may close an account at any time. The administrator's decision may be appealed to the Superintendent. The account shall remain closed throughout the process. The decision of the Superintendent is final.

Any infractions of the provisions of the acceptable use policy may result in suspension or termination of access privileges and/or appropriate disciplinary action up to and including termination.

Adopted: August 3, 2004
Revised/Updated: December 17, 2004 [To Board in Friday Report]
Reviewed: August 21, 2021
Revised:

Cross Ref: [EJA – Acceptable Use of Technology Resources](#)
[EJC – Electronic Mail](#)