Emery County School District

Policy: IJNDCA—Employee or Visitor Network Acceptable Use

Date Adopted: 1 October 1997
Current Review / Revision: 1 May 2019

The Emery County School District recognizes the need for a policy governing the use of electronic information and resources as outlined in Utah State Code 53G-7-1002. The District's Acceptable Use policy is meant to prevent unauthorized access and other unlawful activities by users online, prevent unauthorized disclosure of or access to sensitive information, and to comply with Federal and State law. It also incorporates current industry standards as guidelines for proper use of resources and information.

Examples of Federal law, State law, and industry standards include:

- Children's Internet Protection Act (CIPA)
- Federal Educational Rights and Privacy Act (FERPA)
- Children's Online Privacy Protection Act (COPPA)
- Student Privacy Pledge - standards for third party vendors working with school districts
- Digital Advertising Alliance (DAA) standards for online behavioral and interest-based advertising
- Utah Code Ann. § 53G-7-1-1002 Internet and Online Access
- Utah Code Ann. §53E-3-512 Employee Ethical Conduct

As used in this agreement, "user" includes anyone using any electronic device, accessing the Internet, email, chat rooms and other forms of direct electronic information and communication systems (including individually assigned and network equipment) provided by the District regardless of the physical location of the user. The Network Acceptable Use policy applies even if District provided equipment (laptops, tablets, etc.) is used offsite.

The District will use technology protection measures to block or filter (to the extent practicable) access of visual depictions that are obscene, pornographic, and/or harmful to minors over the network. The District reserves the right to monitor users' online activities and to access, review, copy, and store any electronic communication including files and disclose them to others as it deems necessary. The District also reserves the rights to delete and/or permanently remove any files deemed unnecessary or unwholesome (this decision will be based on the sole judgement of IT Personnel, Principals, and/or District administrators). Users should have no expectation of privacy regarding their use of district property, network and/or internet access or files, including email or social media.

The District will take all necessary measures to fortify the network against potential cyber security threats. This may include blocking access to District applications—including but not limited to email, data management and reporting tools, and other web applications—outside the United States and Canada. Employees are advised not to reveal personal information such as names, addresses, telephone numbers, passwords, credit card numbers, or social security numbers. Releasing the personal information of others or that of organizations associated with the District is prohibited.

Irresponsible and Unacceptable Uses of the Computer Network or Internet

The following are examples of inappropriate activity. In addition to the items noted below, the District reserves the right to take immediate action regarding activities (1) that create security and/or safety issues for the District, students, employees, schools, network, or computer resources; (2) that expend District resources on content the District

determines to lack legitimate educational purpose; and/or (3) other activities as determined by the District to be inappropriate.

- Violating any State or Federal law or municipal ordinance, such as: accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information, or copyrighted materials.
- Criminal activities that are punishable under the law.
- Selling or purchasing illegal items or substances.
- Circumventing or attempting to circumvent the District's content filtering system(s).
- The unauthorized collection of email addresses ("harvesting") from the Global Address List and other District directories.
- Obtaining anonymous email accounts and/or using anonymous email sites; spamming; spreading viruses, spyware, and/or malware.
- Causing harm to others or damage to their property, such as:
    - Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others; cyber bullying or accessing, transmitting, or downloading offensive, harassing, or disparaging materials.
    - Deleting, copying, modifying, or forging other users' names, emails, files, or data; disguising one's identity, impersonating the identity of others, or sending anonymous email.
    - Damaging computer equipment, files, data or information, and/or communications equipment in any way. This includes intentionally accessing, transmitting, or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance.
    - Using any District computer to pursue "hacking/cracking," internal or external to the District, or attempting to access information protected by privacy laws.
    - Accessing, transmitting, or downloading large files in a way that will inhibit use or affect the performance of District information and communication systems.
- Engaging in uses that jeopardize access or lead to unauthorized access into others' accounts or other computer networks, such as:
    - Using another's account password(s) or identifier(s).
    - Interfering with other users' ability to access their account(s); or disclosing a personal password or anyone else's password to others, thus allowing persons to use an account that is not their own.
- Using the network or internet for commercial purposes (except approved fundraisers or approved visitors):
    - Using the Internet for personal financial gain.
    - Using the Internet for personal advertising or promotion.
    - Conducting for-profit business activities and/or engaging in non-government related fundraising or public relations activities such as solicitation for religious purposes, and lobbying for personal political purposes.

- Employees or visitors who formally publish school or district related information on the Internet must have proper approvals and abide by district publishing guidelines and procedures.

Responsible Uses of the Emery School District Computer Network or the Internet

The District shall verify that each employee, substitute, volunteer or visitor using District information and communication systems has signed this agreement. Signed agreements are maintained by each school.

Employees and other users are required to follow District policies for information and communication systems. Even without signature, all users must follow District policies and report any misuse of the network or internet to a supervisor or other appropriate District personnel.

Network access is provided primarily for education and District business. Incidental personal use by staff should follow District policies and occur during duty-free time. By using the network, users have agreed to comply with District policies. If a user is uncertain about whether a particular use is responsible or appropriate, s/he should consult a supervisor or other District personnel prior to engaging in that activity.

Staff Responsibilities Related to Students and Others regarding Internet Safety, Digital Citizenship, and Responsible Use of Information and Communication Systems

- Students or visitors under the age of eighteen should only access District accounts while under the supervision of an instructor or legal guardian. The student or visitors' parent or guardian is responsible for monitoring student use while out of school and instructors and/or administrators are responsible for monitoring student use while in school.

- The District will actively support the training and compliance by students, visitors, and peers with all policies relating to District information and communication systems. Any updates to District policies will be communicated to students, visitors and peers.

Penalties for Improper Use

The use of a District account(s) and District information and communication systems is a privilege, not a right. Misuse may result in the restriction or cancellation of the individual's account. Misuse may also lead to disciplinary and/or legal action; including, dismissal from employment and/or criminal prosecution. Disciplinary action will be based on the nature of the actions taken.

District owned items that are lost or stolen due to neglect, incidental, and/or deliberate actions require the completion of a damage report and may result in partial or full reimbursement to the District.

Disclaimer

The District makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from network use. Any additional charges a user accrues due to the use of the district's information and communication systems or accounts are to be borne by the user. The District also denies any responsibility for the accuracy or quality of information obtained through user access. Any statement, accessible on the District information or communication systems, or the internet, social media, and/or cloud services is understood to be the author's statement and not that of the District, its affiliates, or employees.

Emery County School District

Employee or Visitor Network Acceptable Use Agreement

I have read, understand, and agree to abide by the provisions in the Employee Network Acceptable Use policy, the Internet Safety policy, and the Use of Web Pages/Social Networking policy provided by Emery County School District.

Please return this signature page to the school or location where you work to be kept on file. It is required for all employees that will be using a computer, accessing the network, and/or accessing the Internet.

Employee or Visitor Name (please print): _____

Address: _____

Telephone: _____

Signature: _____ Date: _____