05-01. Acceptable Use of Information Technology Resources

Internal Policies and Procedures of the Utah State Board of Education
Policy # 05-01
Subject: Acceptable Use of Information Technology Resources
Effective Date: 08/01/2018 **Revision Date:**
Purpose: To provide protection for USBE employees, as well as notice of inappropriate and unprofessional behavior.
Policy: A USBE employee shall read and understand this policy, and sign the Acceptable Use Policy Acceptance Form.
References: Board Policy 3006, Data Governance Plan

Procedures:

- Within the first week of employment, all USBE employees and contracted partners must sign the Acceptable Use Policy Acceptance Form.
- The following uses are defined as unacceptable and just cause for termination of use privileges, disciplinary action, and/or legal action. These uses apply to any type of information technology resources provided by the USBE, including computers, electronic device, copiers, e-mail, fax, Internet, printed material, printers, telephones, or video.
- **Illegal Use.** Any use for, or in support of, activities that violate local, state, or federal laws.
- **Infringement of Intellectual Property Rights.** Any use in violation of software license agreements or other contractual arrangements relating to the use of copyrighted materials. At all times adhere to all copyright law regarding the use of software, information, and attributions of authorship. Upon the request of USBE, delete (from any computer) and return all state-provided software used for off-site work.
- **Commercial Use.** Any use for commercial purposes or activities resulting in personal financial gain, including product advertisements.
- **Personal Use.** Any use for personal reasons on a more than incidental basis or for mass distribution of chain letters, jokes, etc. Documents, photos, and other files of a personal nature are not to be stored on USBE servers. Incidental personal use may not have the potential to embarrass the State or the USBE. USBE employees may not use USBE e-mail to receive notifications of a personal nature, including investment notifications and deals on airline tickets.

- **Offensive or Harassing Material.** Any use of material which may be deemed vulgar, sexually explicit, or disparaging of others based on race, national origin, sex, sexual orientation, age, disability, or political or religious beliefs.
- **Religious or Political Lobbying.** Any use for religious or political lobbying or persuasion.
- **Security Violations.** Any action which threatens the security of agency resources, including such actions as: giving your password to another person; accessing accounts for which you are not authorized; or spreading computer viruses, spyware or other malicious software.
- **Confidential Information.** Transmitting information classified as other than "public" under the Government Records Access and Management Act without proper security; or violating the privacy of others by reading e-mail or other private communications (unless you are specifically authorized to support communication systems).
- **Unnecessary Use.** Otherwise appropriate use that intentionally wastes resources or disrupts performance by excessively consuming operating time, storage, paper, etc.
- **Use of non-agency owned computing devices on USBE's network.** Employees are not permitted to connect non-agency computers (including PDA, phones, etc.) to the USBE network, either through a direct connection, over the internet or over a local wireless segment utilizing a VPN connection. Visitors to the USBE may connect to the Internet through an external wireless segment or through specially marked data jacks in conference rooms. Special arrangements can be made for persons doing work under contract for the USBE.
- If a USBE employee is unclear about the acceptable "personal" use of a state-provided resources, or wishes to use the resource for what may be considered a good cause, the employee is encouraged to seek authorization from the employee's USBE supervisor and the USBE network administration through the USBE Help Desk.
- A USBE employee may not:
    - install or use instant messaging software other than USBE-prescribed software;
    - include confidential data in an email or attachment without proper encryption in place; or
    - attach executable programs to email
- When attaching a file to an email, USBE suggests using only the following file types:
    - word processing documents (.doc, .pdf, .wpd);
    - spreadsheet files (.xls, .wb3); and
    - presentation files (.ppt, .shw).

Confidentiality

- A USBE employee may have access to confidential data and information, including data in print or electronic form that contains confidential individual data.
- At all times during and after employment by the USBE, a USBE employee shall agree to follow the directives of the USBE Data Governance Plan and the USBE Information

Security Policy. In any instance in which the terms of this agreement are more restrictive than these policies, the terms of this agreement shall govern.

- A USBE employee may be disciplined and/or dismissed from employment if found to be in violation of this Agreement; and, under state and federal law, misuse or mishandling of data acquired and maintained by a public agency or that agency's information technology may result in criminal, civil, or professional action against the employee.
- Confidential information includes, without limitation, any individually identifiable student, teacher, client, employee or customer data, including all data that are protected by the Family Educational Rights and Privacy Act (FERPA) and Criminal Justice Information Services (CJIS), such as FBI background check information. FERPA provides for the protection of student information by setting forth principles for the gathering and handling of student level records and data.
    - Confidential information also includes confidential or protected information necessary for the proper functioning of the public education system. Such information includes high-stakes test questions and keys, as well as professional practices cases.
- The confidentiality of sensitive information cannot be guaranteed when sending it through non-encrypted methods. A USBE employee shall only use USBE-authorized methods to transmit sensitive or confidential information. For example, typing "encrypt" in the subject line of an Office 365 e-mail message will provide end-to-end encryption of that message and any attachments.
    - The USBE has the right to access and disclose the contents of electronic files, as required for legal, audit, or legitimate state operations management purposes. Email and other electronic files may be accessible through the discovery process in the event of litigation. Each of these technologies may create a record and therefore is reproducible and subject to judicial use.
- A USBE employee shall access and distribute confidential data and information only as needed and only through authorized means (e.g., MOVEit®) to conduct USBE business that is within the scope of a specific assignment(s) and may not store or share confidential information on any computing or storage media, including personal OneDrive, Google Drive, Dropbox, or any other cloud-based storage not owned and/or managed by the USBE.
- A USBE employee may not store work-related data on local machines except for incidental and temporary use. Personal or other sensitive data must never be stored on a local machine or peripheral device.
- A USBE employee shall maintain the confidentiality of all such data and may not disclose (whether verbally, electronically, by document or any other form of communication) any such information to any person except to authorized USBE employees or as authorized in writing by a USBE supervisor.
- A USBE employee shall maintain the confidentiality of security authorizations (user IDs, passwords, electronic keys, smartcards, security badges, etc.) and be personally accountable for all work performed under security authorizations.

- A USBE employee shall protect confidential information displayed on a workstation from inadvertent exposure to passersby.
- A USBE employee shall immediately report any security and/or privacy breaches to the Information Security Manager through the USBE Help Desk. If the employee receives or obtains information to which the employee is not entitled, the employee shall promptly notify one of the above as well as the owner and sender of such information. The employee shall also report any inappropriate use of USBE-provided IT resources.
- Any request for access to information concerning any USBE data by any person other than authorized USBE employees shall be directed to the office that owns the data or information.
- A USBE employee shall retain or dispose of electronic records in accordance with the Government Records Access and Management Act (GRAMA). Please refer to GRAMA or seek counsel from the USBE records officer for guidance in this area.
    - Section 63G-2-801 of the Government Records Access and Management Act provides: A public employee or other person who has lawful access to any private controlled, or protected record under this chapter, and who intentionally discloses or provides a copy of a private, controlled or protected record to any person knowing that such disclosure is prohibited, is guilty of a class B misdemeanor. Furthermore the statute provides penalties against any person who by false pretenses, bribery, or theft gains access to or obtains a copy of any private, controlled or protected record to which he is not legally entitled, and classifies such acts as class B misdemeanors.
- A USBE employee shall use any telephone, PDA, or handheld device consistent with professional standards and this policy.
- The USBE recognizes participation and interaction in social media networks as a useful and innovative communication process; the USBE encourages participation on appropriate issues and topics so long as participation furthers accurate, timely, and productive discussion of public education.
- If a USBE employee participates in social media networks, the employee shall:
    - use USBE subsidized equipment for professional purposes only and consistent with other provisions of this policy; and
    - identify oneself and/or the possibility of being recognized as a USBE employee and participate appropriately, with a helpful and accurate tone and presence, even if the employee participates in a private capacity.
- If a USBE employee participates in social media networks on contract time or as a USBE employee, the comments shall be professional and may not disparage public education or public education entities generally, the USBE specifically, or reveal any confidential information to which the employee has access.
- If a USBE employee participates in social media networks in a private capacity on public education issues, the employee shall, in the spirit of transparency, disclose that the employee is a public education employee and state explicitly that the views expressed are the employee's own.

A USBE employee may not:

- Gain or attempt to gain unauthorized access to USBE data and information;
- Share a user ID(s) and passwords(s) or electronic keys or smart cards with anyone;
- Leave a workstation unattended or unsecured while logged in to USBE data systems;
- Personally use or knowingly allow other persons to use any USBE database or other USBE sources of data for personal gain or other unauthorized use;
- Make unauthorized copies of USBE data or computer applications; or
- Negligently or intentionally engage in any activity that could compromise the security or stability of any USBE data system;

As a general "rule of thumb," a USBE employee should not say, do, view, or acquire anything the employee wouldn't be proud of having everyone in the world learn about if the electronic records were made public.