

[Type text]

| USOE Official IT Policies and Procedures | |
|---|----------------------------------|
| Policy: Confidentiality Agreement | Page: 1 of 5 |
| Subject: | Data Modified: 10/13/2008 |
| Purpose: | |

As an employee of the Utah State Office of Education (USOE), I acknowledge that in the course of my employment I may have access to confidential data and information. This policy provides protection for USOE employees as well as notice of inappropriate and unprofessional behavior.

At all times during and after my employment by the USOE, I agree to follow the directives of the USOE Security Plan (<http://www.schools.utah.gov/computerservices/Policies/Policies.htm>). In any instance in which the terms of this agreement are more restrictive than the USOE Security Plan, the terms of this agreement shall govern.

I acknowledge that in the course of my employment as a Utah State Office of Education employee I may have access to data in print or electronic form that contains confidential individual data.

I understand that, I may be disciplined and/or dismissed from employment if found to be in violation of this Agreement or the USOE Acceptable Use Policy below; and that, 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 and/or civil action against the employee.

I understand and agree that:

- **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). FERPA provides for the protection of student information by setting forth principles for the gathering and handling of student level data.**

Confidential information also includes confidential or secret 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 Internet provides the ability to communicate, collaborate with others and access information anywhere. Within the USOE network email files are protected from outside access. However, anything transmitted over the Internet is subject to interception, reading, and copying by others. Do not transmit personal information about yourself or anyone else using USOE resources without proper authorization. The confidentiality of such material cannot be guaranteed. Use caution when sending confidential information.**

The USOE has the right to access and disclose the contents of electronic files, as required for legal, audit, or legitimate state operations management purposes (Administrative Rule R365-4). Email and other electronic files may be accessible

[Type text]

| USOE Official IT Policies and Procedures | |
|---|----------------------------------|
| Policy: Confidentiality Agreement | Page: 2 of 5 |
| Subject: | Data Modified: 10/13/2008 |
| Purpose: | |

through the discovery process in the event of litigation. Each of these technologies may create a record and therefore are reproducible and subject to judicial use.

- I will access and distribute confidential data and information only as needed to conduct USOE business and within the scope of my specific assignment(s); and will not store confidential information on any computing or storage media not owned by the USOE.
- I will 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.
- I will maintain the confidentiality of all such data and will not disclose (whether verbally, electronically, by document or any other form of communication) any such information to any person except to authorized Agency employees or as authorized in writing by my USOE supervisor.
- I will maintain the confidentiality of my security authorizations (user IDs, passwords, electronic keys, smartcards etc.) and be personally accountable for all work performed under my security authorizations.
- I will protect confidential information displayed on my workstation from inadvertent exposure to passersby.
- I will immediately report any security and/or privacy breaches to the Information Technology Director, Network Administration, or USOE network help desk. If I receive or obtain information to which I am not entitled I will also notify one of the above as well as the owner and sender of such information. I will also report any inappropriate use of USOE-provided IT resources.
- Any request for access to information concerning any USOE data by any person other than authorized USOE employees will be directed to the office that owns the data or information.
- I will retain or dispose of electronic records in accordance with the Government Records Access and Management Act (GRAMA) (<http://attorneygeneral.utah.gov/GRAMA/GRAMARulesRecordsAG.html>). Please refer to GRAMA or seek counsel from the USOE records manager for guidance in this area.
- **Section 63-2-801 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**

[Type text]

| USOE Official IT Policies and Procedures | |
|---|----------------------------------|
| Policy: Confidentiality Agreement | Page: 3 of 5 |
| Subject: | Data Modified: 10/13/2008 |
| Purpose: | |

record to any person knowing that such disclosure is prohibited, is guilty of a class B misdemeanor. Furthermore, Subsection (2)(a) of Section 63-2-801 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.

I will not:

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

Acceptable Use Policy

The USOE characterizes as unacceptable and just cause for termination of use privileges, disciplinary action, and/or legal action, any of the following uses of information technology resources--e.g., computers, copiers, e-mail, fax, Internet, printed material, printers, telephones, video--provided by the agency:

- 1. Illegal Use.** Any use for or in support of activities that violate local, state, or federal laws.
- 2. 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 the agency, delete (from any computer) and return all state-provided software used for off-site work.
- 3. Commercial Use.** Any use for commercial purposes or activities resulting in personal financial gain, including product advertisements.

[Type text]

| USOE Official IT Policies and Procedures | |
|---|----------------------------------|
| Policy: Confidentiality Agreement | Page: 4 of 5 |
| Subject: | Data Modified: 10/13/2008 |
| Purpose: | |

4. 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 USOE servers. Incidental personal use may not have the potential to embarrass the State or the USOE. USOE employees may not use USOE e-mail to receive notifications of a personal nature. For example, these include: investment notifications and deals on airline tickets.

If you are unclear about the acceptable "personal" use of a state-provided resources or wish to use the resource for what may be considered a good cause, please seek authorization from the USOE network administration through the USOE help desk.

Installing or using instant messaging software other than USOE prescribed software is prohibited. Attaching executable programs to email is also prohibited. It is suggested that only the following file types be attached to USOE email. Never include confidential data in an email or attachment.

- Word processing documents (.doc, .pdf, .wpd)
- Spreadsheet files (.xls, .wb3)
- Presentation files (.ppt, .shw)

5. 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.

6. Religious or Political Lobbying. Any use for religious or political lobbying.

7. Security Violations. Any action which threatens the security of agency resources, including but not limited to 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.

8. 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).

9. Unnecessary Use. Otherwise appropriate use which intentionally wastes resources or disrupts performance by excessively consuming operating time, storage, paper, etc.

10. Use of non-agency owned computing devices on USOE's network. Employees are not permitted to connect non-agency computers (including PDA, phones, etc.) to the USOE network, either through a direct connection, over the internet or over a local wireless segment utilizing a VPN connection. Visitors to the USOE may connect to the Internet through an external

[Type text]

| USOE Official IT Policies and Procedures | |
|---|----------------------------------|
| Policy: Confidentiality Agreement | Page: 5 of 5 |
| Subject: | Data Modified: 10/13/2008 |
| Purpose: | |

wireless segment or through specially marked data jacks in conference rooms. Special arrangements can be made for persons doing work under contract for the USOE.

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

Employee Acknowledgement and Acceptance

I have read and understand the USOE Confidentiality Agreement and Acceptable Use Policy and agree with the Confidentiality Agreement and will follow the Acceptable Use Policy.

Name: _____

Wk Phone: _____ Employee ID: _____

Department/Unit: _____ Position: _____

Signature: _____ Date: _____

Supervisor: _____

Supervisor Signature: _____ Date: _____