



**WYOMING**  
DEPARTMENT OF EDUCATION



**Jillian Balow**

Superintendent of Public Instruction



**Cheyenne Office**

Hathaway Building, 2nd Floor  
2300 Capitol Avenue  
Cheyenne, WY 82002-0050  
Phone: (307) 777-7675  
Fax: (307) 777-6234

**Casper Office**

539 S. Payne  
Casper, WY 82609  
Phone: (307) 577-4686  
Fax: (307) 577-6785

**Riverton Office**

320 West Main  
Riverton, WY 82501  
Phone: (307) 857-9253  
Fax: (307) 857-9257

**On the Web**

[edu.wyoming.gov](http://edu.wyoming.gov)  
[www.wyomingmeasuresup.com](http://www.wyomingmeasuresup.com)

Acceptable Use Policy

Policy ID #: 4000-034

Version #: 2.0

Approved By: Jillian Balow, Superintendent, State of Wyoming Department of Education

Effective Date: January 5, 2015

**Purpose:**

Wyoming Department of Education (WDE) resources shall be used in an approved, ethical, and lawful manner to avoid loss or damage to WDE operations, image, or financial interests and to comply with official acceptable use policies and procedures. WDE employees shall contact the Information Security Officer (ISO), (307) 777-8014, prior to engaging in any activities not explicitly covered by this policy.

**Scope:**

This policy applies to all WDE workforce members including, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, and anyone else granted access to sensitive student information. In addition, some third parties such as contractors or vendors may be required to abide by parts of or in whole this policy as indicated in contractual requirements.

**Policy:**

**Ownership**

Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of WDE are the property of WDE and employee use of these such files is neither personal nor private. WDE management reserves the right to monitor and/or log all employee use of WDE Information Resources with or without prior notice.

**Acceptable Use Requirements**

1. Users must report any weaknesses in WDE computer security to the WDE ISO. Weaknesses in computer security include unexpected software or system behavior, which may result in unintentional disclosure of information or exposure to security threats.
2. Users must report any incidents of possible misuse or violation of this Acceptable Use Policy, to the WDE ISO.
3. Users must not attempt to access any data, documents, email correspondence, and programs contained on WDE systems for which they do not have authorization.
4. Users must not divulge remote connection, virtual private network, or other access points to WDE computer resources to anyone without proper authorization.
5. Users must not share their account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes.



**WYOMING**  
DEPARTMENT OF EDUCATION



**Jillian Balow**

Superintendent of Public Instruction



**Cheyenne Office**

Hathaway Building, 2nd Floor  
2300 Capitol Avenue  
Cheyenne, WY 82002-0050  
Phone: (307) 777-7675  
Fax: (307) 777-6234

**Casper Office**

539 S. Payne  
Casper, WY 82609  
Phone: (307) 577-4686  
Fax: (307) 577-6785

**Riverton Office**

320 West Main  
Riverton, WY 82501  
Phone: (307) 857-9253  
Fax: (307) 857-9257

**On the Web**

[edu.wyoming.gov](http://edu.wyoming.gov)  
[www.wyomingmeasuresup.com](http://www.wyomingmeasuresup.com)

6. Users must not use non-standard shareware or freeware software without the appropriate WDE Leadership approval.
7. Users must not purposely engage in activity that may harass, threaten or abuse others or intentionally access, create, store or transmit material which WDE may deem to be offensive, indecent or obscene, or that is illegal according to local, state or federal law.
8. Users must not engage in activity that may degrade the performance of Information Resources; deprive an authorized user access to WDE resources; obtain extra resources beyond those allocated; or circumvent WDE computer security measures.
9. Users must not download, install or run security programs or utilities such as password cracking programs, packet sniffers, or port scanners that reveal or exploit weaknesses in the security of a WDE computer resource unless approved by WDE's Leadership.
10. WDE Information Resources must not be used for personal benefit, political activity, unsolicited advertising, unauthorized fund raising, or for the solicitation of performance of any activity that is prohibited by any local, state or federal law.
11. Access to the Internet from WDE owned, home based, computers must adhere to all the policies. Employees must not allow family members or other non-employees to access nonpublic accessible WDE computer systems.
12. Any security issues discovered will be reported to the WDE ISO or his designee for follow-up investigation.
13. Users are not allowed to attach personally owned, external storage devices (hard drives, USB "Thumb" Drives, "i" devices, etc) to any WDE Information Resource.
14. If an encrypted external storage device is required, for official use only, one can be obtained through the Information Management Department.
15. Users are not allowed to install any type of data encryption software/hardware without permission from WDE Leadership.
16. Users are allowed to use WDE computer systems for approved professional development when utilization does not affect the users work related role in the organization.
17. Users are not authorized to utilize social media (blogs, Tweets, Facebook...), as a representative of WDE without prior approval from WDE leadership.
18. Users are allowed to stream media (audio, video, etc) for official WDE business only.
19. Information that had been deemed sensitive, to include but not limited to, educational, student, teacher data, Personally Identifiable Information (PII), and Protected Health Information (PHI) is not allowed to be stored, utilized, etc on any device that is not owned by the WDE.
20. Under no circumstance is sensitive information, to include but not limited to, educational, student, teacher data, Personally Identifiable Information (PII), and Protected Health Information (PHI) allowed to be sold or utilized in a way in which it was not intended for; data should be used only for official and authorized WDE business.



**WYOMING**  
DEPARTMENT OF EDUCATION



**Jillian Balow**

Superintendent of Public Instruction



**Cheyenne Office**

Hathaway Building, 2nd Floor  
2300 Capitol Avenue  
Cheyenne, WY 82002-0050  
Phone: (307) 777-7675  
Fax: (307) 777-6234

**Casper Office**

539 S. Payne  
Casper, WY 82609  
Phone: (307) 577-4686  
Fax: (307) 577-6785

**Riverton Office**

320 West Main  
Riverton, WY 82501  
Phone: (307) 857-9253  
Fax: (307) 857-9257

**On the Web**

edu.wyoming.gov  
www.wyomingmeasuresup.com

**Responsibilities:**

All individuals, groups, and organizations identified in the scope of this policy are responsible for, reading, understanding and complying with this Acceptable Use Policy.

The WDE ISO will ensure this policy is kept up to date in accordance to any new Federal, State, and/or organizational requirements.

WDE Leadership will ensure the compliance of this policy by all WDE employees.

**Compliance:**

Failure to comply with this or any other security policy will result in disciplinary actions as per HR Policy. Legal actions also may be taken for violations of applicable regulations and standards such as state and federal rules to include the Family Educational Rights and Privacy Act (FERPA).

Procedure(s): None

Form(s): Acceptable Use Employee Signature Form

**References:**

- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)  
<http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
- State of Wyoming, Department of Enterprise Technology Services, 1200-P143, Internet Acceptable Use Policy  
<http://ets.wyo.gov/resources/policies-and-standards>

**Contact:**

Aaron Roberts

E:aaron.roberts@wyo.gov

P: 307-777-8014

F: 307-777-6234

Policy History: Initial, effective date: June 1, 2014