

Computer Security

Access to computer data stored within all computer systems may be carefully monitored for security purposes.

Disposal of reports and/or other information after it is no longer or when the information has been removed to a central back-up system shall be done with the consent and knowledge and in accordance with an established policy by the supervisor responsible for the department utilizing the information.

The Administrative Director and/or designated members of the administrative staff shall have responsibility for determining who will have access to information and who will have access to information stored on computers personally utilized by individual staff members.

To the extent passwords are issued to individual users, such passwords shall not be recorded in any location accessible to any other staff member except such administrative staff as are responsible for issuing them and/or their specific designee.

No user shall be permitted to utilize the computer for an inappropriate, or offensive purpose. Any employee who becomes aware that this policy is being violated shall immediately notify his/her supervisor of the violation.

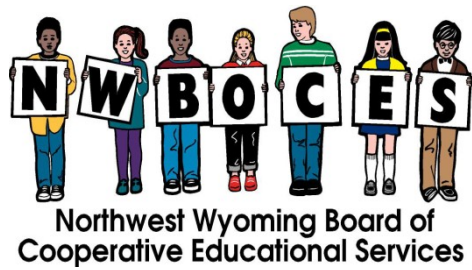
Information other than general educational/program information is not available for all staff should be carefully secured by all staff working with the information in order to avoid divulging confidential information to students or other staff except as may be appropriate on a need-to-know basis. Access to and maintenance of data should be limited. Accessing data for which there is no need to know is prohibited. Disclosure of information should not occur either by intent or negligence except as is necessary to carry out the staff member's assigned duties. Confidential and secure information should be safeguarded to the maximum possible. If it is copied onto a storage device, the storage device and other backup information should be secured in a locked location where it cannot be accessed by persons who are not intended to have the information.

Computer-generated reports or displays are not to be released outside NWBOCES except as provided for in NWBOCES policies, regulations or by approval of the Administrative Director and/or his/her designee.

All computers utilized within NWBOCES shall be utilized only for educational/program purposes unless specific consent is otherwise given by the Administrative Director or his/her designee. No employee of NWBOCES shall have any expectation of privacy regarding the information stored on the computer utilized by the employee. In order for an employee to utilize the computer for educational/program purposes, the employee must obtain consent to allowing his/her supervisor, as well as other staff, to access supervisor and/or Administrative Director may designate to have access to information stored on the employee's computer and/or any other storage device or backup system.

Policy 4022

Adopted 7-24-13
Reviewed 7-22-15
Reviewed 3-22-17
Revised 01/26/22



Acknowledgement of Receipt and Consent to Comply With Electronic
Policies and Guidelines 4021; 4021a-R to 4021e-R; and 4022

The undersigned acknowledges having received a copy of Board Policies and Procedures 4021; 4021a-R to 4021e-R; and 4022 and states that he/she and understands the policy regulation and agrees to comply with the same. The undersigned does further acknowledge that there is no expectation of privacy as to the computer information stored on the computer utilized by the undersigned and the undersigned does consent to allow his/her supervisor or other persons designated by the Administrative Director to have access to any information stored on the computer or any storage device.

Date: _____
Employee/Parent/Guardian

Policy 4022-R

Adopted 7-24-13
Reviewed 7-22-15
Revised 10-26-16
Reviewed 3-22-17
Revised 01/26/22