FILE: GBCB

WINSLOW PUBLIC SCHOOLS
25 MESSALONSKEE AVE.
WATERVILLE, ME 04901

PRIVILEGED ACCESS POLICY (TECHNOLOGY)

Privileged Access:

As part of network and server management responsibilities, certain staff members have heightened administrative computer account privileges. These accounts have considerable authority to access, manage and even take over those accounts used by students, faculty and staff members of the Winslow Public Schools. Privileged access also enables an individual to take actions which may affect computing systems, network communication, or files, data, or processes of other users. These rights are granted for the purpose of maintaining reliable and secure systems, installing software, technical support, and the enforcement of relevant policies and regulation.

The purpose of this policy is to provide guidance and prevent inappropriate use of privileged access by the Technology Department staff members, contractors, consultants, or any individual provided with privileged access to information systems in performing their normal duties.

Eligibility:

Privileged access is only granted to employees whose job duties require special privileges over a computing system or network, unless otherwise authorized by the Superintendent. Before obtaining privileged access, individuals must first have the appropriate training and familiarize themselves with any procedures, business practices, and operational guidelines pertaining to their activities. Contractors and consultants may be granted the minimum temporary privileged access necessary for the performance of their duties, but only while under the direct supervision of WPS authorized personnel.

Obtaining Authorization:

Privileged access should only be granted with the approval of the Superintendent and after completing the Privileged Access Agreement form **(attached).** Contractors and consultants operating under the strict supervision of WPS authorized personnel are exempt from completing the Privileged Access Agreement form but nonetheless are to comply with this policy and all District policies.

Appropriate Use:

Privileged access may be used only to perform assigned job duties. Individuals with privileged access must not abuse their access capability and strictly respect the limits of their authority, respect the rights of the system users, respect the integrity of the systems and related physical resources, and comply with any relevant laws or regulations. Under no circumstances will privileged access be done in a manner that is untraceable and not subject to audit.

Routine logging and auditing of all data and communication is performed by Technology Department staff members in the normal course of their duties to ensure the proper functioning of the network, technical support, and to monitor compliance with relevant policies and regulations. In all cases, access to other individuals' electronic information shall be limited to the least action necessary to resolve a situation. The trust of faculty and staff in the privacy and confidentiality of their communication and information holds important implications for normal business operations, and access to such communication and information by the Technology Department staff will only be performed at the written request of the individual owner of the account or with the approval of the Superintendent.

Expiration/Deactivation/Revocation:

Non-compliance with this policy could expose the individual to disciplinary actions including termination of employment and/or legal actions, and will result in the immediate loss of privileged access. Privileged accounts will be set to expire after a certain period of inactivity, and should be disabled immediately if privileged access is no longer needed or if the staff member leaves the employment of the district. Privileged accounts provided to contractors or consultants should be active only during the performance of their duties and be subject to periodic review.

Privileged Account Password Management:

The passwords for the privileged accounts should be kept in a secure location, and the number of user accounts with privileged access must be kept to a minimum. Passwords for these accounts must be changed on a regular basis, or immediately if it is suspected that the password has been exposed. Additionally, access to the password for any shared account and the Administrative/root/service passwords should be only available based on a ‘need to have’ basis.

ADOPTED: November 21, 2011

SOURCE: Board Policy

WINSLOW PUBLIC SCHOOLS
25 Messalonskee Avenue
Waterville, ME 04901

PRIVILEGED ACCESS AGREEMENT

As part of network and server management responsibilities, I have heightened administrative computer account privileges. I understand that my account has considerable authority to access, manage and even take over those accounts used by students, faculty and staff members of the Winslow Public Schools. Privileged access also enables me to take actions which may affect computing systems, network communication, or files, data, or processes of other users. These rights are granted for the purpose of maintaining reliable and secure systems, installing software, technical support, and the enforcement of relevant policies and regulation.

I will only use my privileged access to perform assigned job duties. I will not abuse my access capability and strictly respect the limits of my authority, respect the rights of the system users, respect the integrity of the systems and related physical resources, and comply with any relevant laws or regulations. Under no circumstances will privileged access be done in a manner that is untraceable and not subject to audit.

I acknowledge that non-compliance with this policy could expose me to disciplinary actions including termination of employment and/or legal actions, and will result in the immediate loss of privileged access.

I agree to change the passwords for my accounts on a regular basis, or immediately if it is suspected that the password has been exposed.

SIGNATURE:_____

Please Print Name:_____

Date:_____

Word:Policies/lljw: November 21, 2011