Code: IJNDB

Collection, Access, Privacy, Security and Use of Student Data

It is the policy of Platte County School District #2 (PCSD#2) that the following guidelines shall to the extent reasonably possible be implemented.

Data Collection

PCSD#2 staff will eliminate collection of Social Security Numbers (SSN) whenever possible.

Collect only the minimum amount of personal information necessary to achieve your purposes and collect only that which you are authorized.

When providing student data electronically ensure that an encrypted connection is used when available.

The Technology Director shall secure connections from the district SIS PowerSchool shall be encrypted using SSL security.

Online access to confidential data shall be done using a secure web connection such as HTTPS.

Accessing Student Data Passwords

PCSD#2 Staff shall not share their passwords with anyone (including peers and supervisors).

District staff are encouraged to change passwords regularly.

The district SIS shall have a lockout for consecutive failed logins.

Exiting Staff Electronic Accounts

The Technology Director shall disable accounts for exiting employees within 3 days so that sensitive data is no longer accessible.

Physical Security

Never leave sensitive data on your desk, in unlocked cabinets, written on whiteboards or paper.

If a staff member's computer is in a public area that staff member must make sure his/her computer screen is locked if unattended.

Appropriately destroying sensitive data by use of the district shredders for printed documents.

The Technology Director shall wipe computer hard drives or properly destroy them as staff exit or as devices are retired to ensure that sensitive data is properly destroyed.

Server rooms shall be dry and temperature controlled.

Server rooms shall be restricted access to only authorized personnel.

Logical Security

The Technology Director shall maintain a district Firewall or comparable security appliance for the protection of the districts electronic network.

Should a breach of the firewall occur the Technology Director shall inform the Superintendent of PCSD#2 as well as the Wyoming Department of Enterprise and Technology Services help desk.

All district Wi-Fi access connections shall be password protected.

Malicious Data Breach

If a PCSD#2 staff member has his/her laptop or computer stolen, the theft is to be reported to the Technology Director as soon as possible.

Backup and Disaster Recovery

The Technology Director shall ensure an offsite data solution for the backup and recovery of district systems.

Adopted: 11/13/17