

<p><b>PRESTON COUNTY BOARD OF EDUCATION</b></p> <p><b>FILE: 8 – PERSONNEL MANAGEMENT</b></p> <p><b>File: 8-23 Personnel Files</b></p>	<p><b>Last Reviewed: 6-28-10</b></p> <p><b>Next Review: 7-01-12</b></p>
---	---

The Director of Personnel will be responsible for seeing that a complete file is kept on each employee. This file will contain the application, contracts, health records, certification for teachers, evaluations and other information deemed pertinent. These files shall be kept in fireproof filing cabinets except when they are in use. They should not be removed from the personnel office.

Accessibility to personnel files will be limited to county office supervisory personnel who work with or are responsible for the employee and central office employees who work with the employee's records.

All employees have a right to inspect their personnel file. To do so they must file a written request or complete the appropriate form. This form will be placed in the file. To eliminate time conflicts and unnecessary pressure on personnel staff, an appointment must be scheduled to examine a personnel file. All appointments will be scheduled as soon as possible within a maximum of two weeks. To insure that no document is altered or removed from the file, the examination will take place in the presence of one of the personnel staff.

The employee will not have access to confidential material for which they have waived the right to review, such as application references or promotional references.

If the employee disagrees with some material in the file, s/he has the right to attach a letter giving his/her explanation or comments.

Any personnel files maintained in schools or work locations will be considered confidential and will be accessible only to the supervisor and employee.

[Home](#)

**R 8-23-1 Notification of Affected Employees of a Breach of Security of Consumer Information**

West Virginia Code §46A-2A-101 thru 104 requires the Preston County Board of Education to give notice of any breach of the security of any computerized data that includes personal information about its employees giving rise to the reasonable belief that the breach has caused or will cause identity theft or other fraud to the individuals involved. Personal information is a person's first name (or first initial) and last name where the name is linked to a person's:

- ❖ Social security number; or
- ❖ Driver's license or state identification card number; or
- ❖ Financial account, credit card or debit card number in combination with any required security code, access code or password.

When such a breach occurs, the Board must, without unreasonable delay, give notice to any employee whose personal information is reasonably believed to have been accessed by an unauthorized person. The following must be included in the notice:

- ❖ A description of the kinds of information believed to be accessed or acquired;
- ❖ A telephone number or web address at which individuals can learn what kinds of information the Board maintained about them; and
- ❖ Contact information for the major credit reporting agencies, with information on how to place a fraud alert or security freeze.

Said notice may be by mail, telephone, or certain electronic means. Where the cost of providing notice will exceed \$50,000 alternative forms of notice are permitted.

The Board may postpone giving notice if a law enforcement agency advises that notice will impede a criminal or civil investigation, or homeland or national security. Moreover, if the accessed data was encrypted, notice need not be given unless the data was acquired in an unencrypted form or the security breach involved a person who had access to the encryption key and it is reasonably believed that the breach has caused or will cause identity theft or fraud to an employee.

[Home](#)

Adopted: March 14, 1983  
Amended/Revised: June 28, 2010