PSESD Operating Procedure No. 5292P
Human Resources

ELECTRONIC INFORMATION SECURITY AND RETENTION

Designated email system: Microsoft Exchange located at mail.psesd.org. Employees may use any Microsoft Exchange compatible email client or a browser to access our email server through Outlook Web Access. Employees are allowed to use Mobile device (e.g., Apple iOS or Android phones or tablets) apps to access our Exchange server so long as those apps are compatible.

Retention The Superintendent or designee shall identify staff responsible for the above-listed email communications. Staff members shall be trained to identify and manage designated records in accordance with established procedures.

Access to the protected email archive data is limited to the Superintendent or designees in order to fulfill records requests, legal requirements and maintain data security.

The PSESD Technology Department is authorized to act on behalf of PSESD to apply to the State of Washington Archives to develop transmittal agreements for electronic documents and for permission to destroy communications older than seven years on an annual basis (commencing March 2018) prior to automated destruction of documents that do not meet any of the above retention exceptions.

Data integrity and security protection: The following provisions are intended primarily for the protection of the security and integrity of PSESD's network and data infrastructure, and to the maintenance of confidentiality of PSESD data which may be stored on or accessed through the use of personal devices.

Personal or PSESD-owned device(s) connected to the PSESD Exchange Server or accessing the PSESD file servers by means of Virtual Private Network (VPN) or through an agency cloud network are subject to the following conditions:

1. PSESD Technology Department will not support personal device(s) except to the extent that it has resources to do so.
2. A PIN number or other password protected screen lock on device(s) is required.
3. Any loss, theft, replacement, or ownership change of the device(s) must be reported to the Technology Department immediately.
4. Should it be necessary, as a result of the loss, theft, or replacement of a device or an employee separation from employment, the Technology Department may remotely reset a device to factory settings deleting PSESD data. This may result in the inadvertent loss of personal data.

Adopted: March 2011
Revised: March 2014