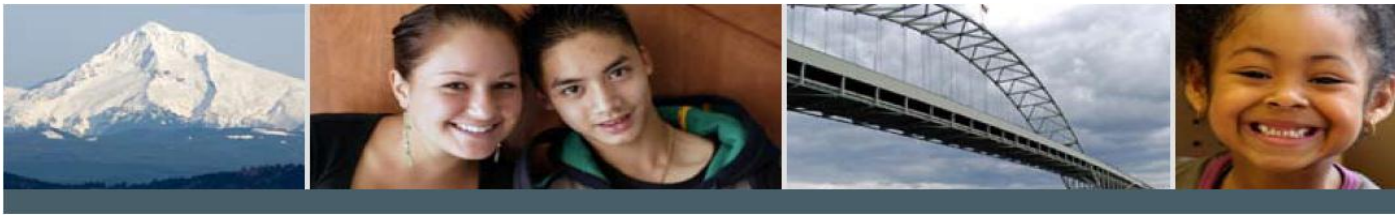

Portland Public Schools

Personal Technology:

A Guideline for PPS Staff

June 2011

Produced by:

Portland Public Schools

Information Technology Department

Introduction

This guideline outlines all required PPS users' best practices and personal responsibility regarding the use of any technology while acting in their District capacity.

Employees have the responsibility to use technology in an ethical and lawful manner. This guideline for personal technology complements similar District policies for PPS Network and Internet use *Student and Staff Acceptable Use Guideline (AUP) 8.60.041-AD*. All employees are required to read and follow those policies as well.

Personal Technology Best Practices

When using personal technology for District business or in your District capacity, please note:

- All email and calendar items sent or received in the District email system are archived and subject to public record law and subsequent eDiscovery when required.
- Any email dealing with District business sent or received via personal email is also subject to public record law and subsequent to eDiscovery.
- Any communication, including those from a personal email account, when acting in your District capacity becomes public record. As such, it is the employee's explicit responsibility to use District resources for conducting District business whenever possible.
- As a rule, District employees should refrain from conducting District business via personal email.
- Using District email on a public computer or one that is shared between family members could result in a breach of your account or release of confidential District information.

District data on personally-owned mobile devices

Given that mobile computing devices may be storing and transferring critical District data while connected to the internet, all District Policies are applicable and will be enforced, including the Acceptable Use Policy.

The following is also applicable:

- Each user's personal device is their responsibility.
- The PPS IT Department cannot support or configure any personal device.
- Users must seek guidance from their cell phone carrier or authorized technician if my personal device has issues connecting to District resources such as email or network.
- Confidential District data must not be stored on mobile computing devices.
- Take precautions to ensure the device is not lost or stolen. If the device is lost or stolen, it is the employee's responsibility to immediately notify IT so district email may be removed or disabled.
- Always protect the device with a password or PIN to prevent unauthorized access.
- Avoid or limit the storing of any District data on your device.
- Any personal device may be subject to eDiscovery. As such, employees should take precaution in storing private information on the device.
- If individuals in addition to the employee have access to the device, it is the employee's responsibility to ensure that access to any District information is secured.
- If an employee leaves the District, it is their obligation and responsibility to delete and remove any and all District data from their personally-owned device.

NOTE: Some content gathered from Azusa Pacific resources

Glossary

Personal Technology – Personal technology includes personal email, desktop or laptop computers or mobile electronic devices used for communications including telephone, text messaging or data transmissions (eg. email, web-browsing, streamlining media, file transfer, etc.) over any network.

Personal Mobile Device – A mobile device and the associated monthly or prepaid services that are acquired and paid for by the employee, using the employee's own credit.

District-owned Mobile Device – A mobile device and the associated monthly services that are acquired and paid for by Portland Public Schools and issued to employees for conducting District business.

Stipend – A set amount of money added to the payroll of any staff member whose supervisor/budget-holder agrees that their job requires access to communications (eg. Telephone, text messaging, email) on a personal mobile device.

eDiscovery - any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case.

NOTE: Some content gathered from Azusa Pacific resources