Atlantic Provinces Special Education Authority

ASL Translation (To Follow)

Procedure Title: **Technology Resource Acceptable Use Procedure**

Issue Date: February 2025
Reviewed/Revised:

Introduction

The purpose of this procedure is to provide a framework that enables consistency of approach and practice across APSEA as it relates to the use of technology resources. This includes defining many scenarios for acceptable and prohibited use; however, the information below should not be considered exhaustive. In addition to the parameters below, APSEA employees are required to exercise good judgment and decision-making.

Application

This procedure applies to all APSEA employees, or any vendor or contractor with access to APSEA technology resource(s). All required documentation, such as the APSEA Employee Mobile Device Agreement Form, must be completed prior to technology resources being issued.

Acceptable Use

Employee Responsibilities and Acceptable Use:

1. Employees must only use approved technology and services for work-related purposes.

2. All APSEA technology resources are the property of APSEA and on loan to employees so they can perform all job functions and duties. Employees should treat technology resources with care and make their best efforts to maintain them in a reasonable, functional state.

3. Upon completion of employment from APSEA or contract termination, the employee must return all supplied technology resources, including any physical accessories (e.g., power adapters) and associated electronic data, to the IT Department, through appropriate means (i.e., direct supervisor).

4. Employees must ensure the security of the area surrounding their workstation and activate computer locks when temporarily stepping away.

5. It is crucial for employees to store Personally Identifiable Information (PII), confidential information, and any sensitive data covered by government or other regulations in a secure location that is not easily accessible from their desks or workspaces.

6. All employees must exercise due diligence in safeguarding information, systems, and associated resources provided to them, preventing potential loss, damage, or harm. Lost or damaged equipment must be reported to IT staff as soon as practical.

7. Employees must securely store their passwords.
    a. Always use a unique complex password/passphrase for every online site; never reuse passwords.
    b. APSEA-approved password managers (i.e. Keeper) may be used to store passwords digitally.

8. Employee-assigned accounts are strictly limited to accessing resources, operating systems, applications, files, and data to which employees have been granted access. The ability to unintentionally access, read, modify, delete, or copy data does not imply permission or authorization to perform such actions.

9. Only approved and authorized devices may be connected to networks owned or managed by APSEA. Personal smartphones, laptops, tablets, and USB sticks may not be connected, unless prior approval from the IT department has been received.

10. Only authorized users are permitted to post or express opinions on behalf of APSEA on social networking sites, blogs, or other internet sites.

11. Employees must maintain the confidentiality of information and systems they obtain during their tenure, even after their employment ends.

Prohibited Use

1. Unapproved or unauthorized devices must not be connected to networks owned or managed by APSEA. This includes portable end-user devices (e.g. smart speakers such as Alexa or Amazon Echo), removable devices (e.g., USB sticks) and personally owned devices.

2. Employees must not share their passwords with others or allow others to use their accounts.
    a. Employees are responsible for all activity originating from their usernames and accounts.

3. Employees must not bypass user authentication mechanisms or compromise the security of any user account or information system software or hardware.

4. Only APSEA-approved apps and software are to be used on APSEA resources. Please refer to the Comp Portal app on your APSEA-provided device (cellphone or tablet) for a list of acceptable apps for mobile devices. Requests for the addition of software or apps for learners or operational purposes to the approved list may be made by following the Digital Resource Request Procedure.

5. Employees must not install software or hardware or modify system configuration settings on any APSEA resources unless explicitly permitted by the employee's Supervisor and the IT department

6. Employees must not engage in activities intending to disrupt APSEA resources or networks.
    a. Employees must not perform network monitoring, port scanning, or security scanning unless explicitly authorized and part of their regular duties.

7. Employees must not use APSEA resources for personal economic gain.

8. Employees must not use the "Remember Me" or "Remember my Password" function inside a web browser.

Remote Work

1. All APSEA-related work must be performed using APSEA-approved resources.

2. All APSEA data must only be stored on approved APSEA resources.

3. Employees must only connect to secure wireless networks and cannot connect APSEA-owned resources to open unencrypted wireless networks. Public Wi-Fi available at various locations, such as hotels and coffee shops, is unencrypted and should not be used unless you also use a VPN connection provided by APSEA. If you can't access the APSEA-provided VPN, you can use the hotspot on your APSEA-provided mobile device connected to the cellular network instead.

4. When working remotely, employees must be aware of their surroundings to ensure others are not able to view confidential material.

Use of Personal Devices

1. Authorization from the IT department is required before personal devices are connected to any APSEA managed wired or wireless network.

2. APSEA data must not be stored on personal devices. In exceptional circumstances, prior authorization from the employee's direct Supervisor and the IT department must be obtained before saving any data.

3. Personal devices used to store APSEA data may be wiped to minimize data leaks. Reasons for device wipe include:
    a. Lost/stolen device.
    b. Termination of employee's employment.
    c. Compromised/hacked account or device.

Expectations of Privacy

1. When using APSEA resources, the user shall not expect privacy. Access and use of the Internet, including communication by e-mail, instant messaging, and related content, are not confidential except in certain limited cases recognized by law.

2. APSEA reserves the right to monitor, access, and disclose all information generated and actions performed using APSEA IT resources. Files, messages (including attachments), and logs may be kept and used as evidence in litigation, audits, and investigations. For additional information, see APSEA's Policy 4.12 Protection of Privacy.

Personal Use of APSEA Technology Resources

1. Employees are permitted limited personal use of APSEA resources, such as visiting websites and checking personal email accounts.
    - Employees may access web-based personal password managers on APSEA resources. However, APSEA must approve the local installation of a password manager.
        i. Users must not store APSEA-related passwords in personal password managers.
    - Employees must only sign onto a web browser (Chrome, Edge, Firefox, Safari) on an APSEA resource using their APSEA issued email account. They can review their personal email once signed into the web browser

2. Employees must not use APSEA license information to install software (e.g., Foxit) on personal devices unless authorized by APSEA.

3. APSEA data must not be stored on personal cloud provider platforms (e.g., Google Drive, Personal Microsoft OneDrive, Dropbox).

Exceptions

Employees must use APSEA technology resources in a manner that is consistent with the established policy. From time-to-time exceptions to this policy may occur for various organizational reasons. An example of where an exception to the policy may be necessary is if it is expected that a non-APSEA device be connected to the APSEA network or place APSEA data in the possession of a third-party contractor (e.g., HVAC technicians, external technical support, Security).

Any exception request must be made in writing to the IT department and, with the help of IT, must contain:

- The reason for the request.
- Required timeline for the exception.

All exceptions must be approved by the requesting department's manager and the IT department manager.

Reporting Violations

If employees become aware of any event that could potentially compromise the availability, integrity, or confidentiality of APSEA data, or if they notice any violation of any standard, policy, procedure, or any applicable requirement, or any illegal activity, they must immediately report the incident to their direct supervisor or the IT department. Failure to comply with the policies outlined regarding using APSEA resources could lead to disciplinary action, up to and including termination, if the situation demands it.

Onboarding and Offboarding

Upon employment, during the onboarding process, APSEA will provide required technology resources and access to associated networks etc., for employees in accordance with their role.

Throughout the course of employment, access and technological requirements may change for a variety of reasons (e.g., accessibility, change of job requirements) and APSEA's IT department will support these adaptations when given appropriate notice and direction.

Upon termination of employment, during the offboarding process, all technology resources must be returned on the employee's final day of work, at which point all accounts and access will be suspended.

Procedure Supports

- APSEA Digital Resource Request Procedure and Forms
- Technology Resource Acceptable Use Policy
- APSEA Employee Mobile Device Agreement Form