Staff Technology Acceptable Use and Electronic Data Security Policy

Adopted by the Springfield School Committee: October 28, 2021

Contents

Definitions

- **Personnel**
  - Any paid employee, volunteer, contractor, or partner with access to SPS-Provided Technology or access to Sensitive Electronic Records.
- **SPS-Provided Technology**
  - Any account, password, software, access to software, Technology Device, internet access, network connection, or electronic communication tool provided by the Springfield Public Schools.
- **Educational Purposes**
  - Activities related to the process of teaching and learning in both formal classes and extracurricular settings.
- **Technology Device**
  - Any piece of physical computing equipment AND the associated equipment required for its use (for example, a power cord).
- **OITA**
  - The Office of Information, Technology, and Accountability.

Definitions (continued)

- **Sensitive Electronic Records**
  - Electronic records that contain Personal Information, Student Education Records, or Personnel Records.
- **Personal Information**
  - Electronic records with a first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number.
- **Student Education Record**
  - Electronic records directly related to the student – and as defined by the Family Educational Rights and Privacy Act (FERPA) and as defined further by 603 CMR 23.02 – and maintained by the Springfield Public Schools and parties acting on behalf of the Springfield Public Schools..
- **Personnel Record**
  - Electronic records directly related to an individual employee or former employee of the Springfield Public Schools and maintained by the Springfield Public Schools and parties acting on behalf of the Springfield Public Schools for legitimate business purposes and in compliance with state and federal regulations.

Purpose and Scope of the Policy

- This policy defines the acceptable use of technology provided to Personnel of the Springfield Public Schools and the expectations for the handling and security of Sensitive Electronic Data.
- Technology provided to Personnel of the Springfield Public Schools is intended for Educational Purposes.
- Access to this technology is a privilege and not a right.
- This policy covers any technology or access to technology provided to Personnel of the Springfield Public Schools, including, but not limited to: user, email, and messaging accounts; software; access to online software; a network connection with internet access; and, technology devices such as computers, iPads, or headphones.
- This policy applies to the use of SPS-Provided Technology and Sensitive Electronic Data of the Springfield Public Schools both on and off school grounds and during and outside school hours.

Inappropriate Online Behavior

- When using SPS-Provided Technology, Personnel must never:
  - Share, post, or disseminate unlawful, inappropriate, profane, vulgar, sexually explicit, threatening, abusive, discriminatory, or harassing content;
  - Engage in activities such as phishing, spamming, or hacking that could harm or disable their device or anyone else's device;
  - Violate any U.S. or state law;
  - Access prohibited sites on the internet, including any sites blocked by SPS content filters;
  - Reveal their own or another person's private information;
  - Pretend to be someone else; or,
  - Use the Technology to promote or engage in any private business activities unrelated to the Springfield Public Schools' Educational Purposes.

While this policy is specific to the use of technology provided to Personnel by the Springfield Public Schools, Personnel should be conscious of the District's Social Media Guidelines when posting content on social media regardless of whether it is with SPS-Provided Technology or a personal device. The Social Media Guidelines are available on the Springfield Public School's website.

Accounts and Passwords

- When using any account or password provided by the Springfield Public Schools, Personnel must:
  - Set their passwords consistent with requirements provided by OITA;
  - Change their password whenever requested by OITA;
  - Keep their password confidential;
  - Notify OITA immediately if they suspect another person has access to their password;
  - Configure and maintain password recovery settings and/or multi-factor authentication settings as required by OITA;
  - Never create accounts or permissions for students in any software or web application without the express written permission from OITA; and,
  - Use their account for Educational Purposes.

Network and Internet Access

- When using wired or wireless network connections and access to the internet provided by the Springfield Public Schools, whether on or off school grounds, Personnel must:
  - Only connect SPS-Provided Technology Devices unless receiving access through OITA;
  - Not attempt to disable or circumvent software designed to block access to inappropriate content;
  - Not attempt to gain unauthorized access to any systems, software, or computer equipment;
  - Never plug in a switch, router, or other network equipment without written permission from OITA;
  - Never attempt to maintain, repair, remove, or replace any network equipment;
  - Not engage in inappropriate online behavior as defined in this policy;
  - Understand that the Springfield Public Schools are not responsible for material viewed or downloaded through the provided connections; and,
  - Use access for Educational Purposes.

Email and Communication Tools

- When using email and other communication tools and platforms provided by the Springfield Public Schools, including messaging tools within software applications, Personnel must:
  - Understand that their account is the property of SPS and is not confidential;
  - Understand they are responsible for all emails and messages sent from their accounts;
  - Be polite, using appropriate language and reporting inappropriate messages or use of tools to OITA;
  - Never reveal private information or send photos of themselves or others unless required for Educational Purposes;
  - Never attempt to bypass restrictions on the size or content of email attachments;
  - Never send an email related to SPS business via a personal or non-SPS provided email account;
  - Never create email or messaging accounts for students without the written permission of OITA; and,
  - Use email and communication tools for Educational Purposes.

Online and Cloud Storage

- The Springfield Public Schools provides online and/or cloud locations to store and share files and Personnel must:
  - Store files related to the Springfield Public Schools in the storage locations provided through OITA;
  - Never store files on portable media like flash drives or external hard drives;
  - Only store Sensitive Electronic Records in online locations designated for securing such information;
  - Never store private information unrelated to the Springfield Public Schools within SPS-provided file storage locations;
  - Never use SPS-provided file storage locations for personal audio or video files; and,
  - Adhere to storage limits in provided storage locations and notify OITA of special circumstances requiring additional storage.

Technology Devices

- When using a Technology Device – like a laptop computer – provided by the Springfield Public Schools, Personnel must:
  - Never loan the Device to another person;
  - Never use the Device to record audio or video without the consent of those recorded;
  - Never attach or affix their password to the Device;
  - Report immediately to their direct supervisor if the Device is damaged, lost, or stolen;
  - Return the Device to OITA if the Device is not working;
  - Return the Device to their direct supervisor or OITA immediately upon no longer Personnel of SPS;
  - Ensure the Device, when returned, is in good working order and is returned with all assigned accessories (for example bags and power cords); and,
  - Use the Device for Educational Purposes.

Using a Technology Device

- When using a Technology Device, Personnel must:
  - Shut down the Device when not in use;
  - For laptop computers, restart the Device at least once per week;
  - Store files and data in the online storage location provided (for example OneDrive) rather than on the Device and understand that the Springfield Public Schools are not responsible for lost data;
  - Never attempt to remove, alter, or disable software included with the Device;
  - Only install software or applications necessary for Educational Purposes;
  - Never sync the Device with any other technology device or with accounts not provided by the Springfield Public Schools;
  - Never attempt to remove content filtering or device management software; and,
  - Never attempt to repair the Device.

Caring for a Technology Device

- To appropriately care for a Technology Device, Personnel must:
  - Treat the Device with care, never dropping it, leaving it outside, leaving it in direct sunlight, leaving it visible in a vehicle, or leaving it in temperatures above 90 degrees or below 40 degrees;
  - Not leave the Device unattended and unsecured;
  - Not use the Device in busy areas such as gyms, playgrounds, or public environments;
  - Not place decorations, stickers, or writing on a Device;
  - Keep food, beverages, and water sources away from the Device at all times; and,
  - Only clean the device with a soft cloth and without using any cleaners, sprays, or soaps.

Data Security

- To ensure the security of Sensitive Electronic Records, Personnel must:
  - Never share their password(s);
  - Adhere to all password requirements and multi-factor authentication requirements established by OITA;
  - Understand spam and phishing attacks and always err on the side of caution by deleting suspicious emails;
  - Store Sensitive Electronic Records only in those locations designated by OITA;
  - Never transmit Sensitive Electronic Records via email unless the email is encrypted;
  - Never transport Sensitive Electronic Records using portable media such as flash drives unless the media is encrypted;
  - Permanently delete Sensitive Electronic Records when they are no longer needed for Educational Purposes and as long as deletion is allowed per state and federal regulations; and,
  - Never attempt to circumvent restrictions placed by OITA on the content that can be sent via email or stored in SPS-provided storage locations.

No Expectation of Privacy

- Personnel can have no expectation of privacy when using any SPS-provided accounts, devices, connectivity, or software.
- The Springfield Public Schools and OITA reserve the right to monitor use of technology accounts, devices, connectivity, and software to ensure appropriate use consistent with this Policy.
- By utilizing SPS-Provided Technology, Personnel are indicating their consent to monitoring by OITA for appropriate use.
- If legally required, communication – including text, audio, video, or images – may be disclosed to law enforcement or other parties in the course of litigation without prior consent of the sender or receiver.

Liability for Misuse of SPS-Provided Technology

- The Springfield Public Schools assumes no responsibility for:
  - Any unauthorized charges or fees incurred in the use of SPS-provided accounts, devices, connectivity, or software;
  - Any financial obligations arising out of unauthorized use of the system for the purchase of products or services;
  - Any cost liability or damages caused by a user's violation of these guidelines;
  - Any information or materials that are transferred through the network; or,
  - Any other inappropriate use of SPS-Provided Technology.

Consequences for Violating this Acceptable Use Policy

- Violations of this Policy may result in:
  - Suspension or termination of access to SPS-Provided Technology; and/or,
  - Violations of this Policy may also result in disciplinary action up to and including termination of employment or contractual relationship.

- As permitted by collective bargaining, the Springfield Public Schools reserve the right to seek restitution for costs incurred by the District, including legal fees, due to a Personnel member's inappropriate use of SPS-Provided Technology or vandalism of Technology.