PRAIRIE SPIRIT
SCHOOL DIVISION

Administrative Procedures

AP-511 EMPLOYEE RESPONSIBLE USE OF TECHNOLOGY (FORMERLY AUP)	**Date of implementation:** June 2014 **Date of review:** June 19, 2024
	Related Administrative Procedures: AP-517 Mobile Cellular Devices AP-519 Privacy AP-708 Records

Purpose: To guide employees and Trustees in the use of technology, including the on-premises use of any personal devices or when connected to any Board networks or online services (hereinafter collectively referred to as "the computer network").

Definitions: Technology is defined as any hardware, software, or cloud services including any objects with the ability to connect to a wired or wireless network. This includes desktops, laptops, phones, copiers, Internet of Things (IoT) devices like smart fridges or smart lightbulbs, network devices like routers, wireless extenders and hotspots.

Procedure:

1) Employees are expected to use the computer network in a legal, ethical, and non-destructive manner consistent with a spirit of respect and in accordance with the policies and procedures of the Division and provincial and federal law.

2) Employees are prohibited from using the computer network for:

   a) Accessing sexually explicit or violent material not connected to curricular outcomes.

   b) Unauthorized transmission of copyrighted material.

   c) Installing unlicensed software.

   d) Any use by an employee that interferes with the duties of employment; or that exposes the Division to significant cost or risk of liability.

   e) Commercial or for-profit purposes unless approved by the supervisor.

3) Employees must guard against targeted phishing schemes such as those that request information or actions through deceptive emails that may appear to be sent from a supervisor or some other familiar person, vendor or third-party. Confirm any unexpected email requests via secondary means such as by phone or in-person. Employees are asked to report all phishing attempts that they recognize to the Prairie Spirit Help Desk.

4) Employees must use Prairie Spirit email only for the purposes of performing their duties. Prairie Spirit email should not be used for personal or commercial purposes. Employees should not forward

any other email accounts to their Prairie Spirit email nor use Prairie Spirit email to "sign-up" for offers from non-educational vendors or third parties.

5) Employees must lock computing devices when leaving them unattended.

6) Sharing of passwords, PINs, multi-factor tokens or authentication information is prohibited. Passwords are not to be shared with other employees or students or any agency or individual and not to be recorded on any physical media such as a sticky note or under a keyboard. Employees must immediately report the loss, or suspected loss, of any authentication information to the Prairie Spirit Help Desk.

7) Employees must change their password at least once every twelve (12) months. Passwords must meet complexity requirements. Passwords must be unique each time they are changed and should never be reused elsewhere with other accounts.

8) Employees must use Multi-Factor Authentication with their Prairie Spirit account.

9) All technology purchases and implementations within the Division, including everything from devices to software to network cabling, must be done in consultation with the Prairie Spirit Learning Technology Department.

10) All employees must adhere to privacy and data security as set out in legislation under *The Local Authority Freedom of Information and Protection of Privacy Act (LAFOIP)* and immediately report any privacy breach.

    a) Never store student or sensitive information on a website or blog. Search engines crawl all online folders and will find this information and create links in search results.

    b) Employees must take extra care when sending mass email or parent announcements. It is especially important to never attach student or sensitive information to group communications and to always be very sure of the recipient list before sending.

11) The Division stores information in the cloud with Level 1 registered partners only as outlined on the Division website.

    a) Employees must store personal student and staff information only with Level 1 cloud providers by default and Level 2 providers with parent consent.

    b) Data stored on any device, computer or external storage such as memory sticks must be encrypted:

        i) How to encrypt data instructions are on the Division website.

12) Employees who are required to transport technology as part of their job must:

    a) Take measures to make certain the technology is appropriately secured when left briefly in an unattended vehicle or a public space, such as locking the technology in a vehicle trunk and never leaving technology in plain view inside the vehicle.

b) Never leave technology in a vehicle overnight.

13) Monitoring

a) The Board owns the computer network and reserves the right to access the contents of all files stored on the network and all messages transmitted through its computer network.

b) The Division maintains logs of equipment usage that may reveal information such as:

i) Contents of files, network activity, and communications of all Division-owned devices, regardless of their location.

ii) Network activity and perform vulnerability scanning of all devices connecting to Division networks.

c) Access to data and logs is protected by AP-708 Records.

References:

The Local Authority Freedom of Information and Protection of Privacy Act

Prairie Spirit Help Desk

Prairie Spirit Privacy Breach Reporting

Prairie Spirit Technology Guides

Protection of Student Data on the Web, Level 1 Web Services