PRAIRIE SPIRIT SCHOOL DIVISION

Administrative Procedures

AP-517 MOBILE CELLULAR DEVICES	**Date of implementation:** June 2019 **Date of update:**
	Related Administrative Procedures: AP-511 Employee Acceptable Use of Technology

Background: Employees who are deemed to require a mobile cellular device either for safety reasons or to perform their work are expected to furnish said device as a condition of their employment. The Board will reimburse the employee at a standard rate for a non-data device and an alternate rate for a data device. These amounts are intended to provide an approximate level of reimbursement reasonable to expected use and are subject to change upon annual review.

Procedure:

1) Eligibility

   a) An employee may be deemed to require a mobile cellular device based on demonstrated need, job function efficiency, safety and/or security. Eligibility may be granted by your Superintendent or by the Director.

2) Approved Devices

   a) Approved data devices must be capable of sending and receiving data with Microsoft Office 365 email and OneDrive applications. This requirement is met by most modern versions of Apple, Microsoft, Android and Blackberry devices.

   b) Where data is not deemed a requirement, then a non-data cell phone with network coverage with the Division boundaries is acceptable. This includes phones that operate on networks such as SaskTel, Bell, Telus or Rogers. Please check with IT personnel to determine viability of other network providers.

3) Data Device Reimbursement

   a) As partial reimbursement, an “annual” allowance payable in monthly amounts based on number of months paid for a data device will be issued to the employee in adherence with the Canada Revenue Agency (CRA) Taxable Benefits and Allowances Guidelines. The CRA requires that a portion of the reimbursement will be withheld for tax purposes.

b) The employee may occasionally be required to provide a copy of a cellular plan bill in a format acceptable to the Division if they wish to continue receiving monthly reimbursement.

4) Non-Data Device Reimbursement

a) As partial reimbursement, an "annual" allowance payable in monthly amounts based on number of months paid for a data device will be issued to the employee in adherence with the Canada Revenue Agency (CRA) Taxable Benefits and Allowances Guidelines. The CRA requires that a portion of the reimbursement will be withheld for tax purposes.

b) The employee may occasionally be required to provide a copy of a cellular plan bill in a format acceptable to the Division if they wish to continue receiving monthly reimbursement.

5) Safety and Acceptable Use

a) In all circumstances, Division employees must abide by the laws of the area in which the mobile device is being utilized and are required to respect all laws that prohibit use of a mobile device while operating a motor vehicle for Division business.

b) Appropriate use of Division technology and IT infrastructure including cell phones, smart phones and specific devices as listed above are to be appropriately utilized as per AP-511 Employee Acceptable Use of Technology.

6) International Travel

a) Be wary of open wireless access. Secure (encrypted padlock) and trusted sources are important when connecting to public Wi-Fi.

b) The Division encrypts email and data traffic, so you are never transmitting data in clear text should you mistakenly connect to an insecure or vulnerable network. This helps to protect your work data, but possibly not your personal data and nor your physical device.

7) Security

a) Employees should be aware that cell phone statements or summaries, when used in the course of your work, are public documents.

b) Security policies will be applied transparently to data devices upon first connection to email to achieve the following ruleset:

- Require an unlock password
- Require the device have encryption enabled
- Enable remove wipe/erase of the device

- Deny access if the device is rooted or jail-broken
- Enable local wipe/erase after 10 failed unlock attempts

Device wipe will not occur unless it is warranted (i.e. theft, criminal activity).

The Division is not responsible for data loss resulting from a remote or local wipe and encourages all users to regularly backup their devices.

The Division is not able to view your personal email, texts or documents on your personal device.