Fleming College

LEARN | BELONG | BECOME

Guidelines for Use of College Smart Phones

June 25/ 2019

The College may issue smart phones to employees as a resource or tool required in the performance of their work. Smart phones are covered under the College Information and Communications Technology (ICT) Appropriate Use Policy (# 6-601).

The guidelines below outline the appropriate and secure use of College issued smart phones.

- 1. A smart phone issued by the College, and the number assigned to it, remains the property of Fleming College.
- 2. An employee must return the smart phone to the College no later than their final day of active duty when their employment with the College ends. A departing employee may request to keep the phone number; requests will be reviewed by the Manager and ITS. All decisions shall be at the sole discretion of the College.
- 3. Employees who place personal data on College issued devices, including smart phones, do so at their own risk. Refer to the **Information and Communications Technology** (ICT) Appropriate Use Policy (#6-601).
- 4. Non-college related charges are the responsibility of the employee. The College reserves the right to chargeback long distance calls or other charges which are not work related.
- 5. Employees issued a College smart phone will make every effort to use Wifi when using a web browser or other data intensive application.
- 6. Employees planning to use their College issued smart phone outside the Province must contact IT <u>in advance</u> to be assigned to an appropriate roaming plan.
- 7. College smart phones issued to Support Staff may be taken home on evenings, weekends and during holidays with prior agreement between the employee and the Manager. However, there is no expectation for the employee to answer a call or email outside of their standard working hours, unless they have been assigned "on call" responsibilities by the Manager.
- 8. College issued smart phones will be connected to college enterprise email system thus enforcing minimum security on the device. Employees will not disable or tamper with these settings.