



COLLEGE OF THE NORTH ATLANTIC
OPERATIONAL PROCEDURE

TOPIC: MOBILE COMPUTING DEVICES PROCUREMENT & USAGE

Procedure No.	IS-504-PR	Division	Information Systems
Related Policies	IS-504; CS-310	Board Policy Ref.	GP-GR-807
Related Procedure	CS-310-PR	Effective Date	November 4, 2016 (R1)

PROCEDURE

1.0 Mobile Computing Devices - Procurement

Approval must be obtained prior to the procurement and use of any mobile computing devices such as, but not limited to notebooks, netbooks, PDAs/Pocket PCs, blackberries, cellular phones, Bluetooth devices and digital cameras used within the college operations.

Academic and administrative managers as well as the purchasing division are responsible for monitoring compliance with this policy.

2.0 Approval Criteria

Approval of the procurement of these mobile devices to a position within the College will be based on, but not limited to the following criteria:

- 2.1 Positions requiring regular travel on behalf of the College.
- 2.2 Employees who are not provided office space within the College under the conditions of their employment and work from remote locations may be considered.
- 2.3 Requirements for development and delivery of instructional programming.

3.0 Procurement

- 3.1 Where appropriate, all mobile computing devices must be procured using the College's internal standing offer agreements. Where such devices are not included in any current standing offer agreements, they will be subject to College purchasing procedures, in compliance with the College's standard technical specifications. These specifications are available from the purchasing division.
- 3.2 Exceptions to the College's standard technical specifications are subject to review and approval by the Purchasing Department and Provincial Information Technology Management.

4.0 Data Protection

No private or confidential data as defined under ATIPPA is to be stored or transported on the internal storage media of any college owned portable computing device. This data may only be transported or stored off campus as defined in the college's Private & Confidential Data Encryption Policy IS-505.

5.0 Technical Support

- 5.1 The college does not permit Administrative Rights access to desktop or mobile computing devices without the approval of the Vice President Corporate Services and Chief Operating Officer.
- 5.2 All mobile computing devices covered in this policy must, where the technology permits, be attached to either the ED or AD domain of the college's networks.
- 5.3 All mobile computing devices such as notebooks or other devices covered in this policy must, where the technology permits have the Colleges inventory control client application installed and functioning.
- 5.4 All mobile computing devices covered in this policy must, where the technology permits have a college approved antivirus application installed and functioning.
- 5.5 All mobile computing devices covered in this policy must, when connecting remotely to the college networks use the Colleges VPN client and approved security protocols.

6.0 Device Control

- 6.1 College employees occupying positions approved for use of a mobile computing device must sign a document accepting responsibility for the appropriate use and safe keeping of the mobile college asset.
- 6.2 College employees assigned the use of a mobile computing device must present the device immediately upon the request of the fixed asset control clerk of the college.
- 6.3 College employees assigned mobile computing and data storage devices must assure that all confidential data and digital images have been removed from those devices prior to return to the Information Technology Department for disposal or reassignment to another employee.
- 6.4 Information Technology staff must ensure data storage devices are properly cleaned of all remaining data and digital images prior to disposal or reassignment to another College employee.
- 6.5 Devices that are reassigned by Information Technology staff must be properly documented within the College's fixed assets system and may require a budget adjustment within the receiving department accounts.
- 6.6 Mobile data computing and storage devices are assigned to positions and do not follow employees if they move to other positions within or outside the College. Employees are not permitted to transfer devices directly to other employees but must turn them in to the IT division for redeployment.

7.0 Cross Reference

Mobile Communications Technologies Policy CS-310
Mobile Communications Technologies Procedure CS-310-PR

Approval History	
Approved by President	March 20, 2010
Revision 1	November 4, 2016