

CONCORDIA COLLEGE

Policy and Procedure Manual

**Subject: Mobile Computing Devices
and Protected Information**

Effective Date: 06/01/2008

Scope: The College

Section: General

Number: 1.10

Purpose

This policy sets out to ensure that all Concordia College protected information stored on mobile devices is secured from unauthorized disclosure, destruction, and/or modification.

Policy

The growth of mobile computing has enabled College computer users great flexibility in performing their work. SmartPhones, PDAs, handhelds, tablet PCs, laptop/notebook computers (AKA mobile devices) have allowed people to take their work with them to places away from the College network. With the added ease at which individuals are able to perform their work comes added responsibility to protect College information.

In the work setting, policies are in place to protect data stored on shared resources, traffic flowing across the network is managed (e.g., packet managing peer to peer, spam protection, intrusion detection), infrastructure equipment is locked away in a controlled room, and procedures are in place to back up centrally stored data.

Special security issues that relate to mobile devices include:

- Any malware (viruses, worms, Trojans) that infects the device can bypass the College's security and spread rapidly to other devices connected back to our network
- If data stored on a mobile device is not backed up by the user it could be completely lost if the devices is stolen or mechanically fails
- Any confidential data stored on a mobile device would be compromised should it be stolen or lost

The President or designee must approve any exceptions to this policy.

Scope

The policy applies to all persons authorized to work with a mobile device that is used for the purpose of transporting or holding protected information.

Responsibilities

All users are responsible for taking the steps necessary to protect College information protected by privacy laws and rights according to Guidelines and Standards.

Enforcement

The Chief Information Officer (CIO) is responsible for monitoring and reporting compliance with this policy. In all cases, the College will disclose information as required by controlling law.

Procedures/Guidelines

The issuance of mobile computer devices that may hold protected information, including but not limited to USB keys, thumb drives, sticks, laptops, notebooks, PDAs, SmartPhones or other mobile devices must be approved by the immediate supervisor

College owned or controlled mobile computing devices must be used for College approved business according to Acceptable Use Policy

Physical access to the mobile device(s) must be protected to prevent theft

When traveling by air the mobile device must be carry-on luggage

All College information stored on the mobile device must be afforded the same level of security as information maintained within the College network

- Encryption standards must be used for all College information protected by privacy laws or rights
- Software will be provided by Information Technology Services (ITS) when connecting to the College network from a remote location to allow a secure connection to be used (Virtual Private Network)
- When connected to the College network all College information protected by privacy laws and rights must be backed up to a designated network storage space

History: Approved: 04/07/2008; Effective 06/01/2008