Corporate Policies and Procedures			
DEPARTMENT: INFORMATION TECHNOLOGY			**POLICY #:** IT-08
POLICY: Mobile Data Protection			
DATE: June 2010	**REV. DATE:**	**COVERAGE:** All Employees	PAGE #: 1 of 1

POLICY STATEMENT:

This policy is designed to provide guidelines on how to manage and store County of Renfrew data on mobile data devices. It is the responsibility of the end user of the mobile data device to ensure that all files saved to the mobile data device are backed-up to the network for archival storage requirements. If data on the mobile data device is corrupted, the IT Division will not be able to restore it.

DEFINITION:

Mobile Data Device
Any easily portable device that is capable of receiving and/or transmitting data to and from information resources. These include, but are not limited to, notebook computers, handheld computers, PDA devices, USB drives, and cell phones.

Strong Password
A password must contain at least 8 characters including the following:

- at least 1 upper case character
- at least 1 lower case character
- at least 1 numerical character

Procedure:

1. Data on mobile data devices must be stored on encrypted hardware with at least 128-Bit AES Encryption. The entire drive must be encrypted with no public partitions.
2. All portable hardware must be purchased via the County of Renfrew's IT Division to ensure compliance.
3. Ensure that minimal amounts of data are stored on portable devices.
4. Ensure that data is deleted from all portable devices when it is no longer required.
5. If data is to be stored on a laptop hard drive, encryption and drive lock must be enabled.
6. Strong passwords used for encryption must be different from login passwords.
7. Passwords are not to be written down and left in public view.
8. **Do not** share passwords with anyone.