# Mobile Computing and Communications

<table>
<thead>
<tr>
<th>Reference No.</th>
<th>Revision No.</th>
<th>Relevant ISO Control No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>xx</td>
<td>1</td>
<td>11.7.1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Issue Date:</th>
<th>July 18th 2012</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Revision Date:</th>
<th>July 18th 2012</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Approved by:</th>
<th>Ted Harvey</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Title:</th>
<th>Director, Technology Services</th>
</tr>
</thead>
</table>

## Version History

<table>
<thead>
<tr>
<th>Version No.</th>
<th>Version Date</th>
<th>Author</th>
<th>Summary of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>July 18th 2012</td>
<td>Ted Harvey</td>
<td></td>
</tr>
</tbody>
</table>

## Approvals

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Date of Approval</th>
<th>Version No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ray Hoppins</td>
<td>Associate Superintendent, System Services</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Distribution

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Date of Issue</th>
<th>Version No.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Personal Communication Devices

### Document Control

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Secure Logon to Operating Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Location</td>
<td><a href="http://xxx.chinooksedge.ab.ca/">http://xxx.chinooksedge.ab.ca/</a></td>
</tr>
</tbody>
</table>
## Table of Contents

1.0 **Overview** .........................................................................................................................3

2.0 **Purpose** ...........................................................................................................................3

3.0 **Scope** ...............................................................................................................................4

4.0 **Risks** ................................................................................................................................4

5.0 **Procedure Detail** .............................................................................................................4

5.1 Minimal Sensitivity: General corporate information; some personnel and technical information .......................................................... Error! Bookmark not defined.

5.2 More Sensitive: Business, financial, technical, and most personnel information ........Error! Bookmark not defined.

5.3 Most Sensitive: Student Information, operational, personnel, financial, IPP, & technical information integral to the success of students and division. Error! Bookmark not defined.

6.0 **Enforcement** ....................................................................................................................6

6.1 Compliance ..........................................................................................................................  6

7.0 **Procedure Governance** ....................................................................................................7

8.0 **Definitions** .......................................................................................................................7

9.0 **References** .......................................................................................................................8
1.0 Overview
Tablets, and other mobile computing and communication devices have become very popular because of their convenience and portability. However, the use of such devices is accompanied by risks that must be recognized and addressed to protect both the physical devices and the information they contain.

The most effective way to secure confidential data is **not to store it on mobile devices**. As a matter of procedure and best practice data should always be secured where it resides. This can be accomplished by storing sensitive data only on secure Chinook’s Edge approved services, and accessing them remotely using secure communication technologies.

Chinook’s Edge work requirements may, on occasion, justify storing confidential data on mobile computing devices. In these cases, users are required to assure that steps have been taken to keep the data secure. It is the responsibility of the user to recognize these risks and take the necessary steps to protect and secure their mobile computing device.

With the increasing use of smart phones, tablets, and other mobile devices it is necessary to establish a procedure governing the use of these devices to store or access Division information. This procedure is applicable to all such devices whether purchased by the division or purchased by employees for both division and personal use.

2.0 Purpose
This procedure is necessary to protect the confidentiality, availability, and integrity of Chinook’s Edge secured information while stored, transmitted, or processed on mobile computing devices. This procedure is not applicable to Chinook’s Edge Public information that is available on Chinook’s Edge public
Internet sites.

3.0 Scope
This procedure applies to any mobile computing device that is used to store, process or access secured Chinook’s Edge Confidential Private or Confidential information and has the capability to connect to Chinook’s Edge network resources. This procedure will not supersede any other existing Chinook’s Edge developed procedures but may introduce more stringent requirements than current policies dictate. The procedure is applicable to all mobile devices, whether purchased by Chinook’s Edge or personally purchased, and used by Chinook’s Edge employees for access to division information and networks. The intent of the procedure is to protect, enforce and control access to division resources irrespective of the type of device.

4.0 Risks

5.0 Procedure Detail
5.1 Implementation
Any mobile computing device, including laptops, accessing or storing division confidential or private information is subject to all division security policies and in addition, will adhere to the following. If the capability exists for the device, mobile computing devices will be configured or otherwise agree to:

- Connect to Private/Confidential or internal data through division networks using the security protocols required by Technology Services. This may include use of secured network connections, virtual technology and use of division approved Network services.
. Receive and install security and other operating system updates from the operating system vendor.

. Use a device and/or screensaver password. Portable computing devices must, at a minimum, be password protected in accordance with division security policies.

. Agree that Technology Services may restrict the access of any mobile computing device to secure Division networks if the mobile computing device presents a probable and demonstrable threat to the integrity of Division data or other computing resources.

Users of personally owned mobile computing devices that are registered to connect to secured Division network and computing resources agree to:

. Allow the Division access, for discovery purposes, to the content stored on the device;

. Give the Division the right to remotely disable or wipe the email content of the mobile device in the event the device is lost or stolen.

. Not require Division support services for the personally owned mobile computing device;

. Pay for any licenses or software required to access Division secured network and computing resources;

. Hold the Division harmless for any damage to the device or its operating system and related software as a consequence of using Division secured network or other computing resources.
Technology Services MUST inform all employees using mobile devices on Chinook’s Edge networks of the security procedures in place.

6.0 Enforcement

Compliance
Mobile devices and their users MUST comply with this security procedure and all other security procedure in place at Chinook’s Edge.
If any employee is found to have breached this security Procedure, they may be subject to disciplinary action.

Users are required to use their common sense in order to act in the best interest of Chinook’s Edge, it’s information and services. In case of doubt users shall contact the IT department to clarify a given situation.

Users of handheld devices MUST diligently protect such devices from loss and disclosure of private information belonging to or maintained by Chinook’s Edge.

Technology Services help desk or Technology Services Director MUST be notified immediately upon suspicion of a security incident, especially when a mobile device may have been lost or stolen.

The cost of any item beyond the standard authorized equipment is the responsibility of the employee.

Penalty for deliberate disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.
Any violation of the Procedure by a temporary worker, contractor or supplier may result in the termination of their contract or assignment and possible civil and/or criminal prosecution to the full extent of the law.

7.0 Procedure Governance

The following table identifies who within CESD is Accountable, Responsible, Informed or Consulted with regards to this Procedure. The following definitions apply:

**Responsible** – the person(s) responsible for developing and implementing the Procedure.

**Accountable** – the person who has ultimate accountability and authority for the Procedure.

**Consulted** – the person(s) or groups to be consulted prior to final Procedure implementation or amendment.

**Informed** – the person(s) or groups to be informed after Procedure implementation or amendment.

<table>
<thead>
<tr>
<th>Responsible</th>
<th>Director Technology Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountable</td>
<td>Associate Superintendent, System Services</td>
</tr>
<tr>
<td>Consulted</td>
<td>Technology Advisory Group, Technology Committee, FOIP Officer, Communications Officer, COLT</td>
</tr>
<tr>
<td>Informed</td>
<td>All CESD Employees, All Contractors, All temporary workers.</td>
</tr>
</tbody>
</table>

8.0 Definitions

Certain terms are used throughout this procedure; in order to avoid misinterpretation, several of the more commonly used terms are defined below.

**TERM / DEFINITION**
Appropriate measures - In order to minimize risk of Chinook’s Edge computer use by unauthorized personnel must be restricted so that, in the event of an attempt to access Chinook’s Edge corporate information, the amount of information at risk is minimized.

Information System- Any electronic system that stores, processes, or transmits information.

Information Assets- Definable pieces of information in any form, recorded or stored on any media that is recognized as “valuable” to the Division

Principle of Least Privilege- Access privileges for any user should be limited to only what is necessary to complete their assigned duties or functions, and nothing more.

Principle of Separation of Duties- Whenever practical, no one person should be responsible for completing or controlling a task, or set of tasks, from beginning to end when it involves the potential for fraud, abuse, or other harm.

9.0 References