Backup and Restore Procedure

<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>1</td>
</tr>
</tbody>
</table>

**Issue Date:** January 22, 2012  
**Revision Date:** January 22, 2012  
**Approved by:** Ted Harvey  
**Title:** Director, Technology Services

**Version History**

<table>
<thead>
<tr>
<th>Version #</th>
<th>Version Date</th>
<th>Author</th>
<th>Summary of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Jan 22 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 #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ray Hoppins</td>
<td></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>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Document Control**

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Document Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Malware Protection</td>
<td><a href="http://xxx.chinookedge.ab.ca/">http://xxx.chinookedge.ab.ca/</a></td>
</tr>
</tbody>
</table>
Table of Contents

1.0 Overview..................................................................................................................................4
2.0 Purpose......................................................................................................................................4
3.0 Scope .......................................................................................................................................4
4.0 Risks .........................................................................................................................................4

The risks associated with the Procedure subject................................................................. Error! Bookmark not defined.
5.0 Procedure Detail .....................................................................................................................5

Detailed Procedure statements ............................................................................................... Error! Bookmark not defined.

Procedure Detail Sub Heading ............................................................................................... Error! Bookmark not defined.

More Content ............................................................................................................................... Error! Bookmark not defined.

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

If any member of IT staff is found to have breached this Procedure, they may be subject to
disciplinary action....................................................................................................................... Error! Bookmark not defined.

If any user is found to have breached this security Procedure, they may be subject to disciplinary action.
................................................................................................................................................. Error! Bookmark not defined.

Any violation of the Procedure by a temporary worker, contractor or supplier may result in the
termination of their contract or assignment................................................................................. Error! Bookmark not defined.

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

8.0 Definitions .............................................................................................................................9

Detail any necessary definitions ............................................................................................... Error! Bookmark not defined.

More Content ............................................................................................................................... Error! Bookmark not defined.

9.0 References ..........................................................................................................................10

List any reference material used ............................................................................................... Error! Bookmark not defined.

More Content ............................................................................................................................... Error! Bookmark not defined.
1.0 Overview

Chinook’s Edge School Division #73 (the Division) has a responsibility to ensure information and Data is routinely backed up, stored securely and verified for integrity. The information and data must be restorable or made available elsewhere in the event of loss, corruption, damage or when integrity is questionable.

2.0 Purpose

This procedure identifies processes and practices for the backup and restoration of Division information and data.

3.0 Scope

This procedure encompasses the backup of all learning critical and business critical information and data managed by Technology Services. Data user recommendations are also covered.

4.0 Risks

Irrecoverable loss of data can severely impact student learning and assessment. Business processes and Division reputation can also be negatively impacted.
5.0 Procedure Detail

Despite the best of intentions, there is always a risk that systems, procedures and facilities can fail or experience catastrophe. This following processes will help ensure the Division’s information is backed up and easily restored in the most efficient, effective and practicable manner.

Central Systems / Data Backup

1. The Division’s Data Owners are responsible for providing system support and data backup resources. They must ensure that backup and recovery practices, and processes are followed. This not only includes the Division’s recommended backup practices but also any retention policies set out by Records Management and Alberta’s FOIP Act.
2. All backup and recovery procedure are to be documented, regularly reviewed and made available to Technology Services and other parties who would be responsible for performing data and system backup and recovery.
3. All data, operating systems, Active directory and network configuration files must be routinely backed up, including custom patches and other software that may be needed in the event of a system re-installation.
4. All backup media must be encrypted and labeled including date. All encryption keys should be kept secure and procedures available to ensure rapid decryption in the event of a disaster.
5. All backups, restores must be logged.
6. Removable backup media must be removed from devices as soon as possible after the backup (or restore) has been completed.
7. Backup media must be stored in a locked, secure place with restricted access and must far enough away from the original data so it cannot be compromised.
8. Routine testing should be performed to ensure backups are capable of being restored.
9. When backup media has reached end of life it must be securely disposed, in accordance with the Divisions “Media Disposal” Procedure.

User Data Backup

Data users are responsible for ensuring their use of Division data and information is secure. They are also responsible for backing up their own data and information, e.g. lesson plans, contacts and software applications they may have installed themselves.

1. Data Users must follow the “Removable Media Procedure” if backing up to USB keys, external hard drives, etc.
2. Ideally backups should be made to Division owned Servers versus removable media.
3. Smart phones and tablets are not to be used as backup media for Confidential or Private data as determined by the “Information Sensitivity Procedure”.

Backup and Restore Procedure
4. The Division accepts no responsibility for Data Users locally stored data or information.

Central Systems Data Restore

Data Restore is usually carried out by the Technology Services Core team who will try to restore files from a date specified by the Data Owner. Data files will only be available from within the time range dictated by retention policies.

1. Data users must request files to be restored by contacting Technology Services Helpdesk or their local technical support. The Data user must be authorized to view the file before any action will occur.

2. In case of doubt Technology Services will confirm user rights with the Data Owner.

3. Restore requests must include the following:
   - Reason for Restore
   - Restore target File name(s) or directories.
   - Original location of files
   - Time of reason for restore request.
   - Last time file was accessed

4. All restore procedures will be documented and logged.

5. Third party requests for backup files must be approved by the Director of Technology Services.

6. Any backup media used for restore must be removed from the system as soon as possible after restoration. The media should then be returned to it’s secure location.

6.0 Enforcement
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>Role</th>
<th>Responsible</th>
<th>Accountable</th>
<th>Consulted</th>
<th>Informed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Director Technology Services</td>
<td>Data Owners</td>
<td>Technology Committee, SAT, ADCOS</td>
<td>All Employees, Contractors, Board, Parent, Students, Partner Organizations, Volunteers</td>
</tr>
</tbody>
</table>
### 8.0 Definitions

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Owner</td>
<td>an individual or group of people who have been officially designated as accountable for specific data that is transmitted, used, and stored on a system or systems within a department, school, or administrative unit of the division.</td>
</tr>
<tr>
<td>Data User</td>
<td>any employee, contractor or third-party provider of the division who is authorized to access Chinook’s Edge Information Systems and/or information assets.</td>
</tr>
</tbody>
</table>
9.0 References

Derbyshire County Council - ICT Backup Policy v3.0
www.derbyshire.gov.uk