# DATA AND HARDWARE DISASTER RECOVERY POLICY *Policy Code:* **3221**

## Overview

Elkin City Schools' local and wide area networks store a great deal of vital information that is critical to the normal operation of the school district. In the event of a disaster, there should be a plan to recover data which may be lost or corrupted with as little time and information loss as possible. Some catastrophic events, such as the total destruction of critical facilities may be both unpreventable and unrecoverable due to the fiscal and physical limitations of the operation of redundant systems. Steps should be taken do as much as prudently possible to protect and recover critical data.

## Scope

The primary component of data recovery will be effective, timely data and system configuration backup. The secondary component will be hardware and communications restoration. This will require an evaluation as to the extent of the disaster by the Superintendent, Technology Director, Finance Director, Facilities Director and others. Operations may need to be temporarily hosted in other school owned property or an offsite location. Disaster recovery decisions will be based on education and business continuity objectives. Other components should include but not be limited to; 1) the acquisition of top quality equipment that operates efficiently and effectively with built-in redundant features to help avoid data loss due to system failure, 2) centralized management and acquisition of all network equipment and workstations to ensure recoverability of configurations and settings, 3) implementing effective, up-to-date network security procedures on all network servers and workstations, and 4) other measures deemed necessary by the district level technology director as newer issues emerge.

## Responsibilities

1. District technology staff will be responsible for the following backups: All centralized backups from designated schools and Central Office, all email servers and centralized file servers, all web servers, router settings and configurations, firewall settings and configurations.

2. School based technology personnel will be responsible for any backups that are not handled centrally. By working with district technology staff, all mission critical files, configurations, data, etc., will be backed up centrally in order to maintain data integrity and security.

3. Finance, Personnel, and Transportation will be responsible for backing up systems configurations and data exclusive to their individual systems.

4. All Elkin City Schools' employees are responsible for backing up important data stored on their individual workstation hard drives. This may be done by copying this data to external media such as floppy disks, CD's, etc. In the course of normal maintenance to workstations, it may be necessary to reconfigure workstations thereby losing any data saved on individual hard drives. Employees are expected to maintain critical data on network hard drives to assure proper file back ups.

Adopted: May 22, 2006