CRESWELL JUNIOR SCHOOL

IT Disaster Recovery Plan

Introduction

The purpose of this document is to set in place strategies to ensure the secure backup and recovery of important data that is stored on the school administration and curriculum networks. The data to backup includes school management data files, administration network user documents, teaching staff documents and pupil documents.

The strategies in place will be robust enough to ensure the recovery of data in any circumstances, Identified risks are:

- Fire or flood
- Electrical failure or surge
- Catastrophic hardware (including portable media) or software failure
- Virus or hacker attack
- Accidental damage to hardware
- Theft of hardware
- Accidental file deletion

Data can be destroyed by system malfunction or accidental or intentional means. Adequate backups will allow data to be readily recovered as necessary. Shadow copies have been enabled on the network shares which gives increased flexibility with work accidentally deleted, or purposefully deleted. The ongoing availability of important data is critical to the operation of the school. In order to minimise any potential loss or corruption of this data, individuals responsible for providing and operating administrative applications need to ensure that data is adequately backed up by establishing and following an appropriate system backup procedure.

Statement of Authority and Scope

This plan is intended to detail the accepted good practice in the backing up and restoring of data on the networked computer system.

The cluster ICT technician provides the framework, design and implementation of backup strategies employed at Creswell Junior School. The ICT technician, the ICT coordinator and the School Business Manager are then responsible for the operation of these strategies, with the full support of the Senior Leadership Team and the Governing Body.

Data to be backed up

- Administration document files including Outlook
- Curriculum network user files
- Staff document files
- Pupil document files

Backup Hardware

- 2 x encrypted 1TB external hard drives
- External USB hard drives for each teacher laptop
- 2 x Kingston DataTraveler 4GB encryptable USB flash drives
- CD-ROMS

Secure network drives on the server

One secure network drive has been set up on the server to provide continuous back up for the School Business Manager's computer.

Backup Frequency

- Incremental backups are performed every weeknight with a full system backup on Saturdays. The current backup is taken off site on one of the 1TB drives containing all necessary core data including essential user data to enable a complete recovery from failure or disaster. Backup drives are encrypted using Bitlocker.

Storage of Backup Media

External hard drives are designed to run continuously connected to the appropriate machine, i.e. the server or teacher laptops. The two 1TB external hard drives are changed over on a weekly basis and one is always kept off site.

Virus Protection

The school subscribes to Vipre which provides virus protection across the whole network. Vipre has a management console on the server which reports regularly if any of the clients need updating.

Disaster Recovery

The admin PC and the server are covered by a full hardware and software maintenance contract with Derbyshire County Council IT Services Division. The helpline number is 01629 537777 or servicedesk@derbyshire.gov.uk . They should be contacted immediately in the event of a server breakdown.

All other PCs, servers and laptops in school are covered by a maintenance contract provided through the Heritage Cluster of Schools. The ICT Technician will attempt recovery of lost data using disaster recovery software, provided that up to date backups are available.

Access rights

Management Information System (RM Integris): The School Business Manager and the School Business Assistant have access to RM Integris which is password protected with unique usernames. All teachers have access to RM Integris for pupil registration and other add- ons as and when they become available.

Finance system: SAP is web based and in accordance with the Financial Regulations and Procedures, only the School Business Manager, the Headteacher and the Deputy Headteacher have access rights according to their level of approval.

Network: All teachers, the ICT Technician, the clerical staff and some teaching assistants have access to the network and are allocated unique usernames that are password protected in order to ensure there is individual accountability for all activity on the network.

Key Holders

The physical key holders for the school are:

- The Headteacher
- The Deputy Headteacher
- The Site Supervisor
- The School Business Manager

Links to:
- Acceptable Use of IT for Staff
- Critical Incident Management Plan

Date approved: _____

Minute number: _____

Chair of Governors signature: _____