Woolmore
Primary School

DISASTER RECOVERY POLICY

September 2025

Woolmore Primary School

ICT Backup Strategy and Disaster Recovery Policy

POLICY STATEMENT:

The purpose of this policy is to set in place strategies to ensure the secure backup and recovery of important data that is stored on the Woolmore Primary School network. The data to backup includes all management data files, administration network system user documents including staff and student documents, and other school data.

The strategy in place will be robust enough to ensure the recovery of data in any circumstance, including fire, catastrophic hardware or software failure, file deletion or virus attack. Data can be destroyed by system malfunction or accidental or intentional means. Adequate backups will allow data to be readily recovered as necessary.

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, the ICT team responsible for providing and operating the school network need to ensure that data is adequately backed up by establishing and following an appropriate system backup procedure.

Statement of Authority & Scope

This policy is intended to detail the accepted good practice policies in the backing up and restoring of data on networked computer systems. The ICT Manager provides the framework, design and implementation of 3-2-1 backup strategies employed at Woolmore Primary School. The ICT Manager and ICT technical support team are then responsible for the operation of these strategies.

Summary

On-Site Backup

Woolmore Primary School uses a Synology NAS drive and internal hard disk drives to store backups onsite. A full backup of the Microsoft 365 environment is carried out weekly on Monday, Wednesday and Friday to the NAS system using Synology 365 Backup software. The NAS is stored in a high-level locked network cabinet. All backups are verified and kept for a minimum of 2 months before being deleted to use the media for further backup requirements. Additional, incremental backup processed are carried out Monday, Wednesday and Friday. A full backup contains SharePoint data, Teams data, Outlook data, user documents, pupil documents, staff documents and shared documents. The school's SIMS MIS system is cloud connected and backups are included as part of the school's subscription with SIMS directly.

Off-Site Backup

Woolmore Primary School uses the recommended cloud backup system Azure Backup to connect to Microsoft's remote and encrypted servers and perform daily backups following completion of media based on-site backup. The system uses Direct Connect software to perform overnight backups of staff documents, shared documents and pupil documents. The allocation of 2TB is currently sufficient to perform the required backups and can be increased as needed. Azure uses API identification and IP address logging to carry out the backup ensuring only the school has access to files and recovery services whilst protecting the data from outside sources.

Additional Detail

Full NAS storage Backups

The following data will be backed up every Tuesday and Thursday onto the NAS drive:

- Administration software data files
- Administration network user documents
- Management Information System Data files
- Teaching staff data files
- Teaching staff network user documents
- Pupil network user documents
- Network software data files

Weekly full backups will be retained for two months on rotation.

Incremental Backups

Incremental backups of all of the above files will be taken on the NAS drive and Azure, on Monday, Wednesday and Friday of each week. (An incremental backup is any backup in which only the files that have been modified since the time of some previous backups, are copied) are to be kept for a period of two weeks.

Frequency of Backups

Full NAS disk-based backups are started manually Tuesday and Thursday on the NAS server. Each backup, which is unattended, runs through the night. Incremental backups are performed automatically, three times a week at the end of the day.

Storage Access and Security

All backup media to be used is stored in a secure, lockable area that is accessible only to authorised staff.

All backup media that is not re-usable will be destroyed thoroughly in an approved manner.

Backup media that is used for other purposes will be erased thoroughly.

Off Site Storage

It is established good practice to keep a full set of backup information stored on an encrypted cloud-based service. In the event of normal backup and restore devices being unavailable due to fire for example, it is imperative that alternative backups are available in a separate location. The approved Azure solution fulfills this requirement.

Disaster Recovery

Overview

In the event of a complete network failure, power cut, server breakdown, fire or any other eventuality where the network is unavailable a disaster plan needs to be in place to ensure the continued smooth running of the school. This would include periods when the time taken to restore the network would take more than a day.

The following emergency procedures have been established:

- In the event of a catastrophic system failure, off-site backed up data will be made available to users within 3 working days if the destroyed equipment has been replaced by that time.
- In the event of a non-catastrophic system failure or user error, on-site backed up data will be made available to users within 1 working day.
- Restoration Requests: In the event of accidental deletion or corruption of information, requests for restoration of information will be made to the ICT support team via the ICT helpdesk.

Emergency procedures will take into consideration the following information

- School operations, financial transactions and any other critical school management systems.
- Identify essential school management functions. Essential school functions are those functions that must take place in order to support an acceptable level of continuity for the school
- Availability of alternate processing of data to use during a disaster. This would include keeping hard copies of certain data and documents.
- When the network has been restored any new information can then be transferred or entered back into the network or cloud systems. However, due to the cloud-based nature of the school's system, users can continue to work as normal via a mobile device and internet connection.

Data Restoration

Only the ICT Manager and authorised personnel will have access to the means to restore network data. The ICT Manager will determine if a successful restoration is possible.

Any requests for restoration of user data will be made to the ICT support team.

In the event of complete data storage failure where a full restoration of school management software and data files is necessary, a member of the SLT will need to give approval.