BACKUP STRATEGY AND DISASTER RECOVERY POLICY STATEMENT

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 school administration and curriculum networks. The data to backup includes school management data files, administration network user documents, teaching staff documents and student documents.

The strategies in place will be robust enough to ensure the recover of data in any circumstance, including fire, catastrophic hardware and software failure, file deletion and virus or hacker 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, people 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 policy is intended to detail the accepted good practice policies in the backing up and restoring of data on networked computer systems.

The Network Manager provides the framework, design and implementation of backup strategies employed at School Business Services. The Network Manager and authorised persons within ICT\Network Department are then responsible for the operation of these strategies.

The Network Manager administers this policy with the full support of the Leadership Group and the Governing body.

Disk Based Backups

The following data will be backed up every weeknight onto the School's Backup SAN (Storage Area Network)

MIS data files

Finance data files

Administration network user documents

Curriculum network user documents

Student documents

School reports

Shared documents on the school's network

Snapshot Backups

Snapshot backups (A full copy of the data at a particular point in time) are to be kept for a period of six months and stored on an external RAID device and external USB device. This is to provide a means of restoring data from a backup at any time period, up to a maximum of six months previously.

Due to the amount of data to be backed up and the storage space required to provide backups, only selective critical data will be stored in this way. This will include –

MIS data files

Finance data files

Shadow copy Backups

This is a means of restoring previous versions of documents that inadvertently become corrupted over time, where the normal backup process is insufficient as it would become corrupted over time, where the normal backup process is insufficient as it would be the corrupted file that is backed up. This is particularly prevalent with Microsoft Office, where the end user doesn't close the document correctly or inserts objects (Video, audio or graphic files that corrupt the document). Shadow Copy Backups allow any of the last fourteen saved instances of a document to be restored. Shadow Copy runs twice a day across the servers holding staff and student documents.

Backup Hardware

It is the responsibility of the Network Manager to determine the appropriate hardware necessary to provide reliable backup and archiving of data. As the amount of data to backup increases over time so the hardware requirements will need to be reviewed annually. This review will be submitted to the Leadership Group.

Backup Software

It is the responsibility of the Network Manager to determine the appropriate software necessary to provide reliable backup and archiving of data. As the amount of data to backup increases over time so the software requirements will need to be reviewed annually. This review will be submitted to the Leadership Group.

Frequency of Backups

Disk backups are performed every weeknight on the backup server. Each backup, which is unattended runs through the night. Backups of whole system are also backed up offsite, in the cloud using Acronis online.

Offsite Storage

It is established good practice to keep a copy of all important data stored off-site. 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. Any sensitive data stored off-site is first encrypted.

Backup Logs

The Network Manager will monitor backup logs to ensure that the network data has been fully backed up.

Backup of data stored on Laptops\Departmental computers

All data should be stored centrally on the network servers, personal data should be stored in a user's home directory. There are instances though where users may want to store their data locally on the computers and\or laptops hard drive. In this instance it is the responsibility of the user to ensure that their data is backed up. The means of doing this will be dependent on the capabilities of their machine but could include external USB hard drives.

In the event of a user losing work that is stored locally on a Laptop or Desktop PC, the Network Department using various undelete and disaster recovery software shall attempt recovery of these lost files. The success of this will be very dependent on a mixture of circumstances beyond the control of the Network Department.

Disaster Recovery

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 would need to be in place-

- To ensure that school timetabling, staff, cover, financial transactions, and any other critical school management systems can still run the member of staff responsible for these areas should ensure that they have their own disaster recovery plan. This will then enable them to at least continue working in these areas. The person responsible for their particular area should follow the following guidelines in formulating their own disaster recovery plan-

- 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.
- Document procedures to implement this disaster recovery plan.
- Make sure the plan can work effectively in the event of a disaster.
- Make sure staff who work within these critical school management areas are aware of the plan and are able to carry it out effectively.
- Plan for the alternative processing of data to use during a disaster. This would include keeping hard copies of certain data and documents and documentation of any disaster plan.
- Make the Leadership Group aware of what strategies would be employed in the event of a disaster.

When the server and network have been restored any new information can then be transferred or entered back into the network system.

If a user on the administration network needs to load up an important document this should be possible since extra backups are made independent of the network servers. A user could then work locally (not attached to the network) on their desktop PC or laptop with the document.

On the curriculum network, as the amount of data files and documents is so much greater it may not always be possible to have an up-to-date backup stored on media separate from the network server backups.

To provide the maximum protection against the possibility of server failure it is the schools policy that all network servers that are purchased have built in fault tolerance and redundancy.

Server Backup and Restore

Each Virtualised Server is backed up every weeknight, this backup includes the server operating system, configuration files and in the case of the Primary Domain Controller this would include network data such as usernames, policy and profile data and security information. In the event of complete server operating system failure, the server operating system would initially need to be re-installed then the server backup restored. In the event of server hardware failure, the server would first need to be repaired, then the server backup restored.

Data Restoration

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

Any requests for restoration of user data will be made to the Network Manager.

In the event of complete server failure where a full restoration of school management software and data files is necessary, a member of the Leadership Group after discussion with the Network Manager will need to give approval.

	Name of School	**Christ Church & Holy Trinity CofE Primary Schools**
	Policy review Date	**March 2024**
	Date of next Review	**March 2026**
	Who reviewed this policy?	**ACHIEVEMENT COMMITTEE**