Sutton Valence Senior School

svs.org.uk

Backup and Restore Policy

Policy Summary

This policy document defines the obligations placed upon Information Communication Technology (ICT) staff and management. It outlines the underlying requirements for backup and restore requirements and is supported by the backup and restore procedure.

Key Principles

Policy statements regarding backup and restore are as outlined below:

- Where strategically identified, SVS information assets managed by the ICT department will be backed up (or replicated) on a regular basis. This will be to both onsite and offsite storage and have restore ability;
- Where strategically identified, SVS services managed by the ICT department will be backed up (or replicated) on a regular basis. This will be to both onsite and offsite storage and have restore ability.

The backup schedule is set to the business requirement for the system or asset:

Asset	Backup Schedule	Method
iSams		
Email		
Oasis		
User Files		

Restore testing will be performed as part of the Disaster Recovery test planning.

ICT will be responsible for managing the backup schedules.

Backup Policy

- Full backups of data are performed weekly. Full backups are retained for three months before being overwritten;
- Incremental backups of all data are performed daily. Incremental backups are retained for one month before being overwritten;
- Where possible backups are run overnight and are completed before 8am on working days;
- Upon completion of backups, media copies are moved automatically to a secure remote site for disaster recovery purposes;
- Backups are stored in secure locations. A limited number of authorised personnel to the backup application and media copies;
- The IT backup systems have been designed to ensure that routine backup operations require no manual intervention;
- The IT department monitor backup operations and the status for backup jobs is checked on a daily basis during the working week;
- Any failed backups are re-run immediately the next working day.

Restore

- Data is available for restore within a few minutes of a backup job completing on the daily schedule;
- Data will be available during the retention policy of each backup job – which is currently defined as three months;
- Recent data is available from this system on completion of the daily backup jobs, which means that there is potential data loss during a working day on some systems. The IT systems have been specified to minimise data loss between backup windows by having elements of system redundancy;
- Requests for data recovery should be submitted to the IT Service desk.

Compliance

This policy has been prepared taking account of prevailing legislation. New legislative requirements or changes in current legislation may necessitate a review of this policy document.

Regulatory and Legislative requirements applicable to this policy:

- Data Protection Act 2018
- Computer Misuse Act 1990

Author: G Millbery
Policy review date: September 2022
Approval date by Governors: November 2022
Next Review Date: September 2023