Carlton VC Church of England Primary School

Disaster Recover SCM (Service Continuity Management) Policy

'I am the vine, you are the branches; those that abide in me and I in them will bear much fruit' (John 15:5)

Approved by: Jo Bevis Governors	Date:
Written by: Jo Bevis	Date:: 6th October 2025
Last reviewed on: -	
Next review: October 2025	

Carlton C of E Primary School Disaster Recovery SCM (Service Continuity Management), Policy

Security of information held on school ICT systems

- All access to school server accounts will be protected by individual passwords
- Staff and students must accept the responsibility of maintaining the security of their allocated password and report instances where the integrity of the password may have been compromised
- Client computer systems used by staff to access school management information will run a password protected screen saver which will activate after 10 minutes inactivity at the keyboard
- All school servers and individual client systems (including laptops) will be protected using an appropriate virus detection/removal system (automatically updated)
- Virus definition files will be updated on a regular basis, this process being automated where possible
- When a virus is reported on a system in the school, the ICT coordinator/office staff will be informed
- Where data from an external source is accessed on a system (e.g. memory sticks) it will only be via a computer that is known to have the latest antivirus protection.
- A copy of the passwords for the school's server systems are kept onsite, in a secure location
- Use of OneDrive, secure, individually password protected, cloud based storage to access information off site

Backup and restoration procedures (see grid below)

- All computers in the school that are used to store individual data and school management information will be backed up to the school's cloud based storage area. This backup must include the users' data together with any system information and programs that are needed to recover and access the data.
- the school's IT provider will test the effectiveness of data back-up every six months under the schools business continuity procedures. A log of the tests completed will be retained for reference.
- The school has an SCM/Disaster Recovery plan with the roles and responsibility of staff clearly identified and the procedures to be followed clearly mapped

System and Service support

- All software used on the school system will be appropriately licensed and a record kept of the licenses held by the school with supporting certificates where provided
- All ICT systems used by the school, including networks, will be supported by :-
  A service level agreement with an external ICT services provider - Partnership Education
- When servers are replaced, the school will ensure that the new servers are compatible with system replaced and that data can be successfully migrated
- Office computers are checked regularly (under the service contract) to ensure there is sufficient capacity and that they are suitable for purpose
- Manual records of accounts and financial documents are retained in the office and returns are submitted to the LA

- Adequate insurance arrangements are in place to cover any loss or damage to computer equipment

Internet use - please refer to Policy for e-safety

School system file names	Locations (PC and path name eg; K:keydata\integris\integris.df1)	Networked or Single user?	Main user name(s)	What is system used for? (i.e. for statutory returns, tracking pupil progress etc.)	Is it critical; essential: necessary; desirable?
SIMS FMS	Server C:\Program Files (x86)\SIMS\FMSSQL\FMSLoad.exe Server D:\Program Files\Microsoft SQL Server\MSSQL11.SIMS2012\MSSQL\DATA\FMS2011.LDF Server D:\Program Files\Microsoft SQL Server\MSSQL11.SIMS2012\MSSQL\DATA\FMS2011.MDF	networked	Office Manager	Finance records CFR	critical
FPS	https://www.hcss-web.co.uk/login.aspx?ReturnUrl=%2f	Web based	Office Manager Head Teacher	Financial planning	essential

SIMS	Server C:\Program Files (x86)\SIMS\SIMS .net\Pulsar.exe Server D:\Program Files\Microsoft SQL Server\MSSQL11.SIMS2012\MSSQL\DATA\SIMS.LDF Server D:\Program Files\Microsoft SQL Server\MSSQL11.SIMS2012\MSSQL\DATA\SIMS.MDF	Networked	Office Manager Head Teacher Class Teachers	School/Workforce Census Pupil information CFR	critical
Anycomms	https://anycomms.bedford.gov.uk/Login.aspx	Web based	Office Manager Head Teacher	Secure transfer of data to local authority	essential
DfE Secure Access (i.e. COLLECT, S2S)	https://sa.education.gov.uk/idp/Authn/UserPassword	Web based	Office Manager Head Teacher	Secure transfer of data to non LA schools and DfE	essential
Email	https://login.microsoftonline.com/	Networked	All staff	e-mail system	essential
Budget files	H:\BUDGET\2021-2022	Networked	Office Manager	Financial information	essential
SIMS assessment	Server – as SIMS above	networked	Office Manager Head Teacher	Assessment data	essential

Part 2 Current BACKUP practice

School critical system file names	Who is responsible for backing up?	Backup method		How often backed up?	Location of latest backup
		Included in system backup?	Separate backup (onto tape; CD; memory stick; portable hard drive? Etc.)		
All critical systems including SIMS, FMS	Overseen by Partnership Education, scheduled daily backup and weekly portable hard drive change "C:\Program Files\SIMS\FMSSQL\FMSLoad.exe E:\Program Files\microsoft SQL server\MSSQL>SIMS2008\MSSQL\Backup\fms2011	All critical systems including SIMS, FMS daily backup	All critical systems including SIMS, FMS onto portable hard drive weekly	backed up daily and portable hard drive changed twice weekly: backup log completed; random file retrieved termly	portable hard drive / home