Leamington Community Primary School

Together we make a Difference

Disaster Recovery Plan




Completed by: Mrs. A. Belger (Computing Subject Leader) and Matthew Kicks (Computeam)

Courage Determination Friendship Honesty Respect

Leamington Community Primary School recognises the critical role that information technology plays in supporting high-quality teaching, effective administration and safeguarding the welfare of pupils and staff. As technology becomes increasingly embedded within education, the protection, management and responsible use of digital systems and data have become essential to the school's daily operations.

This policy outlines the school's approach to ensuring the confidentiality, integrity and availability of all information and IT systems. It establishes clear expectations for staff, pupils, contractors and visitors in relation to the secure use of school technology and the handling of data. The policy also supports compliance with relevant legislation and guidance, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Department for Education (DfE) Cyber Security Standards (2022).

Leamington Community Primary School is committed to maintaining a safe and secure digital environment. This includes implementing robust technical controls, promoting cyber awareness among staff and pupils, and ensuring that any incidents are managed promptly and effectively. Through this policy, the school aims to reduce risk, prevent data loss or misuse, and safeguard the continuity of education and school operations in the event of disruption.

School Profile & Recovery Objectives

School Name: Leamington Community Primary school
Address: Leamington Road, Liverpool, L11 7BT

IT Infrastructure Overview

- Servers
- Network: switches, firewall, routers, VLANs
- Workstations / laptops / tablets
- SaaS / cloud services
- Remote access / off-site locations

Recovery Objectives

System / Data	RPO (max data loss)	RTO (max downtime)	Priority Level
Student management / records	Daily	Same Day	High
Staff / Payroll / HR	Daily	Same Day	High
Lesson resources / curriculum content	Daily	Same Day	Medium
Staff / admin PCs & laptops	Daily	Same Day	Medium
Archived / historical data	Bi Monthly	72 Hours	Low

Risk Assessment and Mitigations

Category	Details
Threats / Hazards	• Fire, flood, storm damage • Hardware / disk failure • Cyberattack (ransomware, malware) • Human error (deletion, misconfiguration) • Theft, vandalism • Power failure, network outage • Backup corruption / loss
Impact & Likelihood Assessment	For each threat, estimate how likely it is, and the impact (operational, reputational, financial). Use that to prioritise mitigation.
Mitigation Measures	• Physical protection (fire suppression, environmental control) • UPS / generator for server rooms • Network segmentation, firewall, intrusion detection • Access control, user training, least privilege • Regular patching, anti-malware, vulnerability scans • Regular validation of backups

Roles and contacts

Role / Position	Name(s)	Contact (phone / email)
Headteacher / Principal	Paul Vine	headteacher@leamington.liverpool.sch.uk
IT Lead	Ashley Belger	ashley.belger@leamington.liverpool.sch.uk
Vendor / Acronis Support Contact	Matthew Hicks	M.hicks@computeam.co.uk

Backup Design & Strategy (Using Acronis)

Backup Topology & Storage

•Primary storage (on-site): NAS, backup server, local backup device
•Secondary / off-site / cloud: Acronis cloud or remote location
•Use immutable / write-once features (if available)
•Encrypt backups (AES-256 or equivalent)

Backup Types & Schedule

Backup Type	Frequency	Scope	Destination(s)	Retention / Versions
Full image (servers)	Weekly (e.g. Sunday night)	Entire server	On-site + off-site	Keep last 4 full images
Incremental / differential	Every 2–4 hours	Changed files / data	On-site + off-site	Chain back to last full
App / DB backups	Daily (or more frequent)	Database, logs	On-site + off-site	Keep 7–14 days of logs
Workstation / laptop images	Weekly	OS + applications + settings	Local + cloud	Last 2–3 images

File / shared drive backups	Daily incremental	User / shared files	On-site + off-site	Retain for 30 days (or per policy)

Retention / Archiving Policy

- Daily backups: last 30 days
- Weekly full backups: last 12 weeks
- Monthly full backups: last 12 months
- Archive critical history off-line

Monitoring & Validation

- Enable alerts / email on backup failures
- Review backup logs daily / weekly
- Perform test restores (files, VMs) periodically
- Quarterly integrity checks of backup sets

Disaster Recovery Procedures

Section	Details
1 Activation & Declaration	• Incident detected and assessed by IT / DR lead (Paul Vine) • Decision to activate DRP by Headteacher / DR Lead • Notify DR Team, leadership, stakeholders • If attack, isolate affected systems
2 Assessment & Prioritisation	• Determine which systems failed / are at risk • Identify which backups remain intact • Prioritise restore order based on priority list
3 Recovery Execution - Step 1: Prepare Hardware / Environment	• Use spare hardware if original is damaged • Configure network, firewall, IP settings
3 Recovery Execution - Step 2: Restore System / Image	• Restore the latest good full image via Acronis • Apply incremental backups in sequence
3 Recovery Execution - Step 3: Restore Applications / DB / Logs	• Restore databases, logs, applications • Bind services, accounts, network shares
3 Recovery Execution - Step 4: Restore Files / Shared Data	• Restore user files, shared drives • Merge increments if necessary
3 Recovery Execution - Step 5: Restore Client Devices	• Restore images or data to laptops / desktops • Reconfigure if needed
4 Verification & Testing	• Test login, apps, network, services • User acceptance / representative staff test • Confirm data integrity
5 Alternate / Failover Options	• Use alternate site / cloud VM if school site not usable • Use SaaS / online tools temporarily if possible
6 Communication	• Provide updates to staff, leadership, IT • External updates to parents, authority as needed • Use prewritten templates where possible

7 Post-Recovery & Closure	• Confirm full operation of systems • Reintegrate restored systems • Document timeline, challenges, deviations • Conduct lessons learned and update DRP

Testing, Exercises & Maintenance

Interval	Test Type	What to Test	Responsible
Weekly / Monthly	Backup validation	Restore random files / VMs	IT Lead
Quarterly	Partial DR test	Simulate single system failure	Computeam
Annually	Full DR test	Simulate serious disaster	Leadership, Computeam
After major change	Ad hoc test	New servers / apps / services	IT Lead, Computeam

Resource / Infrastructure Requirements

- Spare / standby servers or cloud capacity
- Backup storage (NAS, backup appliances)
- Off-site / cloud storage (Acronis cloud or remote)
- Adequate network bandwidth
- UPS / generator for server rooms
- Secure off-site location for physical backup media
- Licenses / vendor support for Acronis & hardware
- Staff time for backup management, testing, recovery