Background info on 3-2-1 Backup

Risk Context

Schools are now frequent targets for ransomware and account-takeover attacks, and Microsoft 365 tenants are often compromised through phishing, credential theft, or misconfigured admin access. When this happens, attackers typically gain the same rights as a Global Admin, meaning they can delete mailboxes, purge retention, encrypt SharePoint/OneDrive files and in many cases disable or corrupt backup integrations. The primary risk is that both the live data and the most recent automated backups become compromised at the same time.

An independent backup alone does not fully mitigate this. If the backup platform is administered through the same identity plane, or if its storage can be modified or deleted by an attacker who has compromised the school's tenant or the Managed Service Provider (MSP) operational accounts, then the school is still exposed to a single point of catastrophic failure. This is the risk that offline backups historically protected against.

An immutable, separately governed copy directly mitigates this risk by ensuring that:

- Even if attackers gain full control of the school's Microsoft 365 tenant, they cannot alter or delete the backup.
- Even if the MSP's operational accounts are compromised, the immutable copy remains protected by a different identity boundary and enforced retention.
- Even if recent backups contain encrypted or corrupted data, earlier clean versions remain intact and recoverable.

This approach aligns with the intent of DfE and NCSC guidance, which now emphasises independent, tamper-resistant backups rather than specific technologies like tapes. It is widely recognised across regulated sectors that immutability and separate governance are the modern equivalents of offline media, and they materially reduce the likelihood and impact of a total data-loss event.

3-2-1 Backup Pattern for Cloud/365 Environments

The 3-2-1 backup pattern exists to achieve three specific outcomes: survivability (at least one copy must remain intact after any single failure or attack), independence (no single platform, identity, or compromise should be able to destroy all copies), and recoverability (you must always be able to restore a clean, recent version even if the latest backups are corrupted).

For schools using Microsoft 365, the MSP should maintain at least three recoverable copies of critical data:

1. The live data in the school's Microsoft 365 tenant
2. A fully independent backup held in the MSP's own cloud environment, outside the school's Microsoft 365 tenant and not controlled by the same Global Admin accounts. As well as the MSP's cloud, it could be held on a specialist backup provider's platform, or another cloud account, as long as the backup is outside the school's Microsoft 365 admin area.
3. An immutable copy stored in a separately governed environment (i.e. not accessible by the school's Microsoft 365 admins or the MSP's normal support accounts) that attackers cannot alter or delete.

Deep versioning and long retention ensure the MSP can roll back to a clean backup even if recent backups contain compromised data. Immutable, isolated storage protects those clean backups against the risk of any tenant compromise. Logical separation and immutability (not physical offline media) are what DfE and NCSC expect for modern cloud-based school environments.