wavenet education | Microsoft Solutions Partner

GUIDE

The future of backup in higher education

How consumption-based models and zero trust backup are shaping Microsoft 365 protection.

Data, collaboration, and risk in higher education

Over the past decade, higher education has undergone a digital transformation unlike any other sector. Cloud platforms such as Microsoft 365 have redefined how they deliver learning, conduct research, and collaborate globally.

But as digital adoption accelerates, so too does data risk. From ransomware attacks to accidental deletions and compliance breaches, higher education institutions are now managing petabytes of sensitive information, often with limited budgets and overextended IT teams.

Many assume that Microsoft automatically backs up their data. It doesn't. Microsoft ensures uptime and availability, but data protection and recovery remain the your responsibility.

This gap has led universities to ask a critical question:

How can we protect data efficiently and affordably, without compromising security or academic continuity?

The answer increasingly lies in two principles shaping the future of IT in higher education: **consumption-based backup models and zero trust data protection.**

The data dilemma in higher education

From virtual classrooms and research repositories to student records and Teams discussions, higher education data volumes are exploding.

This growth brings opportunity, but also strain:

- **Ransomware and phishing attacks continue to rise across academia.**
- **Data retention regulations demand greater visibility and control.**
- **Budget uncertainty makes long-term planning difficult.**

When data loss or downtime occurs, the impact reaches far beyond IT. It disrupts teaching, damages reputation, and can even halt critical research projects.

The financial reality: cost pressure meets data growth

Higher education operates in a perfect storm of constraints. Funding pressures and unpredictable enrolment patterns are squeezing budgets, while data volumes continue to rise across research, administration, and digital learning.

Traditional per-gigabyte (per-GB) backup models make this harder to manage. Every new SharePoint site, every Teams chat, every student upload expands the backup bill, even when that data is inactive or duplicated.

This model might have worked in the past, but for higher education institutions it now creates three core challenges:

- **Unpredictable costs:** data growth drives exponential expense.
- **Budget rigidity:** annual fixed contracts make it hard to respond to changing usage.
- **Operational inefficiency:** managing capacity, retention, and compliance consumes valuable IT time.

Understanding backup models: consumption-based vs per-GB

To overcome these challenges, many institutions are transitioning to consumption-based backup models - a shift from fixed capacity to flexible usage billing. Modern consumption-based backup models also provide unlimited, on-demand storage capacity at no extra cost, so institutions can scale protection during peak data periods such as admissions, research cycles, or digital exams, without increased cost or capacity planning.

The per-GB (capacity-based) model

The traditional per-GB model charges are based on how much total data you store. It's simple, but not always smart.

Drawbacks include:

- **Paying for dormant or archived data.**
- **Difficulty forecasting future costs.**
- **Inflexibility during academic or research cycles.**
- **Little alignment with real-world cloud usage.**

The consumption-based model

A consumption-based model aligns cost directly with how backup and recovery services are used, rather than how much data exists. It reflects real-world behaviour and allows institutions to flex spending dynamically.

Advantages include:

- **Predictable OPEX spending aligned with actual need.**
- **Dynamic scalability for changing demand.**
- **Reduced waste and overprovisioning.**
- **Simpler management through automation.**
- **Unlimited elastic storage at no extra cost that grows or shrinks with your Microsoft 365 environment.**

Quick comparison

For higher education institutions trying to balance service delivery with financial control, the consumption-based approach offers both adaptability and transparency.

Feature	Per-GB (Capacity-Based)	Consumption-Based
Billing basis	Total storage volume	Actual usage or protection level
Cost predictability	Low	High
Scalability	Manual	Automated
Budget model	Fixed CapEx	Flexible OpEx
Efficiency	Pay for unused capacity	Pay only for what's protected

Why zero trust protection matters

Cyber security is now an educational issue as much as a technical one. Higher education institutions are frequent targets for ransomware because of their open networks, distributed users, and valuable intellectual property.

The Zero Trust model addresses this by assuming no one. not even internal users is automatically trustworthy.

Every access attempt is verified, every system is segmented, and every backup is protected against tampering.

In backup terms, zero trust protection means:

- **Immutable backups that can't be modified or deleted.**
- **Air-gapped copies isolated from production systems.**
- **Granular access controls that limit who can restore data.**
- **Audit trails that track every change and restore event.**

This approach ensures that even if a ransomware attack encrypts production data, recovery remains possible from a clean, untouchable copy.

Backup and compliance in higher education

Higher education institutions operate under complex regulatory and ethical obligations:

- **GDPR and local privacy laws.**
- **Freedom of Information requests.**
- **Long-term retention for research and institutional records.**

A resilient backup strategy must therefore provide:

- **Policy-based retention to meet compliance requirements.**
- **Granular recovery at file or mailbox level.**
- **Geographic storage control to maintain data sovereignty.**
- **Audit trails and reports to demonstrate compliance.**

These capabilities not only protect against fines but reinforce trust with students, staff, and research partners.

The shift towards operational resilience

Combining Zero Trust protection with a consumption-based model allows universities to evolve from reactive backup to proactive resilience.

This modern approach provides:

- **Predictable, flexible cost control.**
- **Automation that reduces IT burden.**
- **Faster recovery for business continuity.**
- **Alignment with cloud-first strategies and OPEX budgeting.**

It represents a pragmatic balance between fiscal responsibility and digital security, two priorities that have never been more closely linked.

How institutions are implementing this model

Many higher education institutions are now adopting cloud-native backup platforms built around these principles. One proven approach integrates zero trust data protection with consumption-based economics, ensuring both affordability and assurance.

Example in practice: Microsoft 365 cloud backup

A modern, managed backup solution can provide:

- **Ransomware protection through air-gapped, immutable backups.**
- **Fast recovery of Exchange, SharePoint, OneDrive, and Teams data in minutes.**
- **Unified management via a single, intuitive dashboard.**
- **Flexible pricing through pay-per-use or monthly/annual options.**
- **Unlimited storage capacity at no extra cost so institutions never need to purchase additional space or renegotiate contracts.**

This approach ensures critical academic data remains recoverable, secure, and cost-effective, no matter how fast the university's digital footprint grows.

A managed approach to data protection

For many universities, the shift to consumption-based, zero trust data protection represents both an opportunity and a challenge.

The principles are clear, but implementing them effectively, at scale, across multiple systems and departments, can be complex.

That's where a managed approach becomes invaluable. Rather than maintaining and monitoring backups internally, universities are increasingly partnering with specialist providers who operationalise these frameworks as fully managed services.

A managed backup model offers several benefits for higher education institutions:

- **Expertise on demand:** Access to experienced security and data protection professionals without the cost of in-house expansion.
- **24/7 monitoring and response:** Continuous oversight ensures issues are identified and resolved before they cause disruption.
- **Operational efficiency:** IT teams can focus on research and teaching support while backup and recovery are automated and centrally managed.
- **Predictable OPEX spending:** Costs are tied to real usage rather than storage capacity, aligning with the financial realities of the education sector.
- **Elastic, unlimited storage:** storage that adapts instantly to institutional growth or seasonal data peaks, at no extra cost.

In practice, managed solutions built on zero trust architecture and consumption-based pricing give higher education institutions the confidence that their Microsoft 365 environments, including Exchange, SharePoint, OneDrive, and Teams, are always protected, recoverable, and compliant.

The key takeaway

As higher education institutions continue their digital evolution, data resilience is no longer optional. Balancing security, compliance, and cost efficiency requires a shift in both mindset and model.

A consumption-based, zero trust approach offers a way forward, one that's financially sustainable, operationally efficient, and strategically aligned with the sector's mission to innovate and share knowledge securely.

Whether through in-house strategies or managed service partnerships, the institutions that embrace this model will be best placed to protect their data, their people, and their reputation in the years ahead.

Need a helping hand?

We work closely with higher education institutions to bring these principles to life, combining technical expertise, sector understanding, and trusted partnerships to deliver practical, scalable data protection.

We enable higher education institutions to:

- **Securely protect and archive Microsoft 365 data with immutable, air-gapped backups.**
- **Restore information in minutes through predictive, file-level search.**
- **Manage protection policies for thousands of users from a single, intuitive dashboard.**
- **Maintain ransomware recovery readiness with clean, isolated copies of data.**

This managed model turns strategy into action, providing the tools, automation, and expertise to help you achieve cost-efficient, resilient data protection without adding internal complexity.

Call us on **0344 863 3000**

email enquiries@wavenet.co.uk
or visit wavenet.co.uk/education