



Secure learning starts at the endpoint



One campus. Many endpoint realities.

A simpler foundation for digital learning

Higher education IT teams support shared, distributed, and specialized endpoints across labs, classrooms, libraries, faculty offices, and remote learning environments. The IGEL Adaptive Secure Endpoint Platform™ provides a trusted, governed foundation that helps colleges and universities improve security, strengthen resilience, and reduce operational overhead.

Campus endpoint pressure

- Shared fleets create constant configuration and maintenance work
- General-purpose operating systems add local complexity and attack surface
- Refresh cycles compete with other campus technology priorities
- Department-level choices can create inconsistent endpoint experiences

The IGEL approach

- Immutable IGEL OST™ supports secure endpoint access
- Centralized management applies configuration across distributed endpoints
- Ecosystem integration supports VDI, DaaS, and cloud workspaces
- Compatible hardware stays productive longer

Why the IGEL Adaptive Secure Endpoint Platform matters

Modern campus computing needs more than another endpoint tool. It needs a simpler, more trusted way to deliver secure digital workspace access across shared labs, classrooms, offices, and remote learning environments.

BUILT FOR CAMPUS IT

- **Immutable operating system**
A controlled foundation for secure endpoint access.
- **Centralized management**
Consistent configuration across distributed environments.
- **Broad ecosystem support**
Works with existing VDI, DaaS, and cloud workspace investments.
- **Hardware reuse**
Extends the useful life of compatible devices.

WHAT INSTITUTIONS GAIN

- **Stronger security**
Reduce local complexity and strengthen the endpoint layer.
- **Greater resilience**
Keep endpoint state controlled across shared environments.
- **Lower operational overhead**
Simplify configuration and maintenance at scale.
- **More value from hardware**
Reduce refresh pressure on compatible devices.

Where IGEL Fits.

Built for the modern campus

From high-turnover shared devices to controlled research workspaces, IGEL gives IT teams a consistent way to govern endpoint access while preserving the digital tools students, faculty, and staff already use.

Student labs & classrooms

Deliver consistent, governed endpoint experiences.

Libraries & shared workstations

Standardize high-turnover devices for dependable access.

Virtual labs & remote learning

Support VDI, DaaS, and cloud workspace access.

Faculty & staff endpoints

Apply centrally managed configuration at scale.

Research & specialized access

Provide a trusted foundation for controlled workspaces.

Hardware reuse initiatives

Keep compatible devices productive for longer.

Modernize your campus with IGEL

Ask IGEL how your institution can modernize lab and shared-device computing, support VDI or DaaS initiatives, strengthen endpoint security, and get more value from the hardware you already own.

Zero Trust starts before sign-in

IGEL supports Zero Trust-aligned architectures by strengthening the IGEL Adaptive Secure Endpoint Platform before users connect to campus and cloud resources. Its app-centric architecture and centralized management model help IT teams keep endpoint state controlled while preserving familiar access.

1

Establish a governed endpoint

Use an immutable operating system designed for secure access.

2

Apply configuration centrally

Manage distributed endpoints with greater consistency.

3

Connect to existing workspaces

Preserve investments in VDI, DaaS, and cloud access.

One endpoint strategy, campus-wide

- **Standardize the experience**
Bring labs, libraries, offices, and remote environments under a more consistent model.
- **Control endpoint state**
Reduce the burden created by local complexity and change.
- **Modernize on your terms**
Support current digital workspace investments while extending compatible hardware life.