Why Rutgers University Faculty Rely on VPNs — And Why It's Not Optional



There's a version of academic work that never makes the campus brochure: the adjunct uploading final grades from a kitchen table at 11 p.m., the professor pulling journal PDFs from a conference hotel lobby, the lecturer grading discussion posts over a flat white in a New Brunswick café. Rutgers faculty don't do their jobs inside a firewall anymore. They do them wherever the laptop happens to be open. And every one of those locations is a place where institutional data, licensed research access, and student privacy are all quietly at risk.

That's why VPN use among Rutgers instructors is close to universal — and why treating it as a personal preference rather than a professional habit is a mistake.

The job followed faculty home

Hybrid instruction, remote office hours, cloud grading portals, and shared document review dissolved the line between "on campus" and "at work." A Rutgers instructor on a Tuesday might touch Canvas, a department drive, a grant database, an IRB submission system, and three publisher portals — from four different networks before lunch. Each of those hops is a trust boundary. A VPN collapses them into one encrypted tunnel, so the traffic looks the same to the network whether the user is in a seminar room or a Starbucks on Route 1.

Licensed resources only work from recognized addresses

The most mundane reason is the most decisive: off-campus access breaks without a VPN. Publisher subscriptions, citation databases, and internal administrative systems are licensed and firewalled by IP range. From a campus address you're "inside." From your apartment you're a stranger. Rutgers runs its own institutional VPN precisely so faculty and staff can tunnel in and appear as legitimate campus traffic, and the library's proxy system exists for the same reason.

Without that tunnel, an instructor writing a syllabus at home hits paywalls on journals the university already pays for, and an administrator can't reach a system that's supposed to be

reachable. A free VPN for PC on a personal machine can restore general privacy, but only the institutional tunnel restores access. Faculty end up needing both, and conflating them causes real friction.

Public Wi-Fi is a hostile default

Campus-adjacent cafés, airport lounges, hotel conference floors, and public libraries all share one trait: you don't control the router. Unencrypted traffic on those networks is readable by anyone with modest tooling, and rogue access points dressed up as legitimate hotspots are routine. An instructor logging into a grading portal over open Wi-Fi is handing credentials across a room full of strangers.

A VPN fixes this cheaply and immediately by encrypting everything between the laptop and the exit node. For faculty who bounce between networks all day, this is the single highest-value habit available — and it's why a desktop free VPN client, even a modest one, earns a permanent place on a work machine.

Student records and compliance aren't optional

FERPA governs education records. Rutgers Biomedical and Health Sciences adds HIPAA on top. IRB protocols, unpublished grant data, and pre-publication manuscripts all carry handling expectations. None of that framework cares that you were working from a laundromat.

The compliance argument is simple: a faculty member on a shared or public network without a tunnel is one credential capture away from an incident report. VPN encryption doesn't make anyone compliant by itself, but it removes the easiest failure mode, and it's the control most often cited after the fact when something goes wrong.

The home network is not automatically safe

Faculty often assume their own Wi-Fi is the safe option. Sometimes it isn't. Shared apartments, roommates' devices, aging routers on factory firmware, and a house full of smart plugs and doorbells all widen the attack surface. A VPN free for PC use on the home machine keeps traffic opaque to the local network, which matters when the local network is a group project rather than a controlled environment.

Where free VPNs fail — and what to check

Faculty budgets being what they are, the pull toward best free vpn lists is understandable. Some of them are genuinely fine. Plenty are not. The common failure modes: hard monthly data caps that a grading weekend blows through, throttled speeds that make video lectures

unusable, aggressive logging, and a small pool of exit IPs that publishers have already flagged.

For anyone comparing vpn alternatives or hunting the best vpn free option, the checklist is short and non-negotiable: a real no-logs policy, a published privacy statement, modern encryption, a kill switch, and enough bandwidth for video calls. Reputable vpn alternative roundups will name which free tiers cap data and which don't. Skip anything ad-injected or owned by an opaque holding company.

The honest trade-off: free tiers are adequate for casual browsing, café work, and light admin tasks. For sustained high-volume research, a paid tier or the institutional tunnel is worth the money. Free vpn for laptop and desktop clients are a floor, not a ceiling.

The practical routine

Use the Rutgers VPN for anything institutional — grades, records, licensed databases, internal systems. Use a reputable free VPN on public networks for everything else. Turn on a kill switch so a dropped connection doesn't leak. Keep the two habits separate and automatic.

None of this is exotic. It's the baseline cost of doing academic work in places that weren't designed for it. Faculty aren't paranoid for tunneling in from a café; they're just paying attention.