

Student Tech Support

Security Best Practices with Students



Work with the System

- Review AUPs and student access rules
- Negotiate expectations and policy
- Negotiate rules for escalation, follow up and documentation
- Protect students from critical data and systems

Use Security Best Practices

- Differentiated access
- Passwords – change regularly
- Security reviews for ALL staff, teachers, students
- Who is violating security and why? Cracking down on “that’s how everyone does it.”

Communication

- Openly communicate rules and changes
- New policies should have educational objectives
- Open learning community
- Student-led culture

Contracts

- Should be “two-way” not just punitive
- Can have multiple levels for advanced students

Preventing Accidents and Mistakes

- Plan for the worst – mistakes happen.
- Use best practices: virus software, backups, track licenses, inventory
- Practice makes perfect – “what if” scenarios and guided explorations
- Police with policy (not technology)
- Encourage strong student/teacher and peer relationships

When Bad Things Happen

- One-strike policy, consistently enforced
- Responses should be fair, quick and appropriate

Structured Freedom

- The price of freedom is documentation, creating tangible evidence of learning and completing tasks
- Reward with increased responsibility and less supervision, not necessarily increased access
- Trust and responsibility

From: GenYES 2.0 Implementation Guide