

From <http://www.wired.com/news/technology/1,68480-0.html>

Kutztown 13 Face Felony Charges

By [Associated Press](#) | [Also](#) by this reporter
17:10 PM Aug, 09, 2005

KUTZTOWN, Pennsylvania -- They're being called the Kutztown 13 -- a group of high schoolers charged with felonies for bypassing security with school-issued laptops, downloading forbidden internet goodies and using monitoring software to spy on district administrators.

The students, their families and outraged supporters say authorities are overreacting, punishing the kids not for any heinous behavior -- no malicious acts are alleged -- but rather because they outsmarted the district's technology workers.

The Kutztown Area School District [begs to differ](#). It says it reported the students to police only after detentions, suspensions and other punishments failed to deter them from breaking school rules governing computer usage.

In Pennsylvania alone, more than a dozen school districts have reported student misuse of computers to police, and in some cases students have been expelled, according to Jeffrey Tucker, a lawyer for the district.

The students "fully knew it was wrong and they kept doing it," Tucker said. "Parents thought we should reward them for being creative. We don't accept that."

A hearing is set for Aug. 24 in Berks County juvenile court, where the 13 have been charged with computer trespass, an offense state law defines as altering computer data, programs or software without permission.

The youths could face a wide range of sanctions, including juvenile detention, probation and community service.

As school districts across the nation struggle to keep networks secure from mischievous students who are often more adept at computers than their elders, technology professionals say the case offers multiple lessons.

School districts often don't secure their computer networks well and students need to be better taught right from wrong on such networks, said internet expert [Jean Armour Polly](#), author of *Net-mom's Internet Kids & Family Yellow Pages*.

"The kids basically stumbled through an open rabbit hole and found Wonderland," Polly, a library technology administrator, said of the Kutztown 13.

The trouble began last fall after the district issued Apple iBook laptops to every student at the high school about 50 miles northwest of Philadelphia. The computers were loaded with a filtering program that limited internet access. They also had software that let administrators see what students were viewing on their screens.

But those barriers proved easily surmountable: The administrative password that allowed students to reconfigure computers and obtain unrestricted internet access was easy to obtain. A shortened version of the school's street address, the password was taped to the backs of the computers.

The password got passed around and students began downloading such forbidden programs as the popular iChat instant-messaging tool.

At least one student viewed pornography. Some students also turned off the remote-monitoring function and turned the tables on their elders, using it to view administrators' own computer screens.

The administrative password on some laptops was subsequently changed but some students got hold of that one, too, and decrypted it with a password-cracking program they found on the internet.

"This does not surprise me at all," said Pradeep Khosla, dean of Carnegie Mellon University's engineering department and director of the school's cybersecurity program. IT staffers at schools are often poorly trained, making it easy for students with even modest computer skills to get around security, he said.

Fifteen-year-old John Shrawder, one of the Kutztown 13, complained that the charges don't fit the offense. He fears a felony conviction could hurt his college and job prospects. "There are a lot of adults who go 10 miles over the speed limit or don't come to a complete stop at a stop sign. They know it's not right, but they expect a fine" not a felony offense, he said.

Shrawder's uncle, James Shrawder, has set up a website that tells the students' side of the story.

"As parents, we don't want our kid breaking in to the Defense Department or stealing credit card numbers," said the elder Shrawder, a businessman. "But downloading iChat and chatting with their friends? They are not hurting anybody. They're just curious."

The site, CutUsABreak.org, has been visited tens of thousands of times and sells T-shirts and bumper stickers, including one that says: "Arrest me, I know the password!"

The district isn't backing down, however.

It points out that students and parents were required to sign a code of conduct and acceptable use policy, which contained warnings of legal action.

The 13 students charged violated that policy, said Kutztown Police Chief Theodore Cole, insisting the school district had exhausted all options short of expulsion before seeking the charges. Cole said, however, that there is no evidence the students attacked or disabled the school's computer network, altered grades or did anything else that could be deemed malicious.

An association of professional computer educators, the International Society for Technology in Education, believes in a less-restrictive approach to computer usage. The more security barriers a district puts in place, the more students will be tempted to break them down, it believes.

"No matter how many ways you can think to protect something, the truth is that someone can hack their way around it," said Leslie Conery, the society's deputy CEO. "The gauntlet is thrown down if you have tighter control."

Wired News: [Contact Us](#) | [Advertising](#) | [Subscribe](#)

We are translated daily into [Korean](#) and [Japanese](#)

Wired.com Â© 2006 CondÃ©Net Inc. All rights reserved.

Your use of this website constitutes acceptance of our [User Agreement](#) and [Privacy Policy](#)