

## [In Depth](#)

# Not safe for work: What's acceptable computer use in today's office?

**Online activity once considered off-limits is becoming the norm for many organizations. But what crosses the line from OK to NSFW in today's Web 2.0 office?**

By [Joan Goodchild](#), Senior Editor

June 16, 2010 — [CSO](#) —

How many minutes, or hours, did you spend on Facebook today? Even if you spent just a few minutes on the popular social networking site during office hours, you're not alone. Data from Nucleus Research finds 77 percent of workers who have a Facebook account use it during work hours.

Sports events, online games, and entertainment sites, many of which cross the line between interesting and inappropriate, are all common distractions in today's office. It's not that these things are entirely new, but [the Web 2.0 era](#)—think social networks, URL shortners, video sites and more—presents wrinkles that require rethinking acceptable use policies.

### **iTunes and Facebook: Productivity versus personal use**

Studies reveal a great deal of employee internet use is for personal, not professional, reasons. As much as 40 percent of internet surfing done during work hours is personal, according to IDC Research.

This isn't news to Kevin Quinlan, senior director of IT for restaurant chain Bertucci's. Quinlan is a realist. His policy is to allow employees six 15-minute slots each day to log on to websites for personal use and fun; that includes Facebook, Twitter, or any other site they want to see (within reason).

"People should be allowed to do what they want on their breaks," he said. "Coming into the office shouldn't be a bad thing. I know what I like to do when I'm using my computer. I don't want to set rules I can't follow myself."

[Also see The 7 deadly sins of social networking security](#)

Quinlan is one of a growing number of managers at companies that find new ways of communicating, and younger employees that demand access to varied online content, are leading to a redefining of acceptable computer use in the workplace. Research from security firm Clearswift found 79 percent of workers in several countries around the globe value being trusted to manage their own time, and being trusted to use the Internet as they wish, over pay. Additionally, 62 percent of employees feel they should be able to access web/social networking content from their work computer for personal reasons in order to complete personal tasks.

In fact, many said they would [decline to work at a company with anti-Facebook restrictions](#).

This creates a dilemma on several levels for organizations. There are the implications for productivity, but also the potential security risks that are posed when employees are given free rein to surf the web as they wish.

For Quinlan, the changing tide arrived a few years ago as the iPod craze touched off and he found scores of employees downloading iTunes onto company computers without his consent. Not malicious activity on the part of the employees, he notes, but activity that was messing up his network.

"I had issues with remote users saying 'Oh, I can't connect anymore.' I was trying to chase down the problem and finally discovered some piece of software iTunes was running was knocking out our VPN connection every 15 minutes."

That launched a new realization for Quinlan, and he started using Bit9's Parity Suite, several products that control unauthorized software and malware from running on endpoints, while still allowing workers to have access to a range of web content.

"When we hire folks, they have a session with the network administrator and they sit down and go over what you can do on your computer, what the policies are," he explained.

### **Goal! Keeping workers on task through major sporting events**

With the World Cup kick-off this month, managers around the globe are bracing for what is expected to be an inevitable drain on productivity. In the U.K., which tends to have many more soccer fans than the U.S., productivity losses tied to the World Cup could total approximately \$1.45 billion, according to Chartered Management Institute.

The same story usually gets told every March in the U.S. The annual NCAA tournament rolls around and many offices form betting pools and employees monitor games and statistics from their desks. An annual report from firm Challenger, Gray and Christmas claims employees waste about 20 minutes each workday researching teams online, talking to colleagues about their picks, and watching online and TV broadcasts of the games during work hours.

But it's not the games that concern Michael Counes, Director of Information Technology & Education for the Hanley Center, a non-profit addiction recovery center in Florida, where patient

data privacy is of the utmost importance. Social networks are today's biggest time suck, but he has so far resisted removing access to them.

"We don't want to take that away from them. But we don't want them to spend all day on social media sites. We want them to use it as a tool on their break. If someone is spending all day on Facebook, it's hard to believe the rest of the job is getting done."

### [Also see "Employee monitoring - good for the employee?"](#)

Counes does not block any sites, but uses a product from SpectorSoft called Spector 360 to monitor employee computer activity, which he says can get as granular as logging keystrokes of typing and goes as broad as a general report of a worker's internet visitation for the month. He has seen a 15-17 percent increase in productivity since he began using the product, and employees learned they were being monitored.

"Once you talk to five people in the organization, it's like a virus," he said. "People learn that 'These guys are serious, they really do look at what is going on.'"

Even so, companies find that drawing a hard line isn't as clear-cut as it used to be. Streaming sports video might be verboten, but what about score updates? If those alerts are outlawed from company PCs, can employees check the scores on their mobile phones? Productivity-wise, is that any different than keeping the sports section in the restroom?

### **YouTube, URL shortners, and "gentlemen's" sites**

It's probably obvious to most that surfing for pornography at work isn't OK. Despite ever-more-advanced monitoring capabilities, however, porn viewing on the job is still quite common. Research conducted in March by media-information firm Nielsen Co. found that almost 30 percent of employees have visited an adult site using a computer at work; and 20.6 million Americans visited an adult site from a work computer an average of 8.1 times in a month, according to Nielsen.

Other research also bares out the enormity of inappropriate surfing and downloading at work. According to a survey by the American Management Association and the ePolicy Institute, 60 percent of e-mail users admit to having sent e-mail with adult content at work. A survey commissioned by email management company Proofpoint found out that a third of office workers claimed to have watched inappropriate content on their office computers.

A government report released earlier this year found many Securities and Exchange Commission employees were found to have viewed pornography at work—while the financial crisis was unfolding. One senior attorney at SEC headquarters in Washington spent up to eight hours a day accessing Internet porn, according to the report.

Counes said despite the monitoring he does, he has seen this kind of activity and needed to take action.

"Not everyone believes you have the ability to do what you say you can do. There have been cases where I've intervened in ways of a higher punitive level than a stern talking-to," he said. "But for the most part it's been the exception, not the rule."

Of course, there are many web sites out there that aren't technically pornographic, but feature material that managers may be less than pleased to see if they walk by a desk and catch a glimpse of the computer screen.

Maxim.com, for instance, bills itself as a site for men that features "hot girls, sexy photos & videos." Nude-pictures pioneer Playboy is set to launch TheSmokingJacket.com, a site that will exclusively include content that is "safe for work," according to the advertising.

As for his company, "most managers here feel it's to be left at home in the gray situations and is not part of Hanley Center mission vision and values," said Counes.

Even closer to the mainstream, plenty of music videos on YouTube tiptoe on the lines of propriety. Lady Gaga's videos may be offensive to one employee, but no problem for others—what about slightly less controversial pieces by Beyonce or Miley Cyrus?

Even in the case of obvious pornography, today there is a more realistic chance that an employee might accidentally see questionable images unintentionally. [Shortened URLs in Twitter tweets](#) and elsewhere obscure the actual content of the link. Etiquette on social media sites such as Digg dictates that questionable links and images should be labeled "NSFW", but compliance is less than 100 percent.

It's also possible to happen upon a malicious site that loads porn images, unbeknownst to the user.

"We treat each case individually as an opportunity to educate," said Counes. "There are lines in the sand like anything else, but most are left to managers discretion outside the obvious severe violations."

**Also see CSOnline.com's [Security Tools and Templates](#) page for sample acceptable use policies**

At the end of the day, said Counes, he believes most of what employees do is with good intent. Anything they do wrong is usually the result of a lack of knowledge, as opposed to malicious intent. He believes the monitoring he does serves more as an education tool than a "Big Brother" scare tactic, and employees get that.

"As long as you maintain strong education and advocacy, they understand that the bottom line is to serve the client."