Internet Content Filtering

Statement and Purpose

Seattle Pacific University policy defines a number of categories of content that are contrary to University lifestyle expectations and inappropriate within our campus environment. Such content is not allowed to be sent or stored on University resources and includes material sent or viewed on the Internet, via email, file transfer or any other electronic means. See the University's **Computer Acceptable Use** for more information.

There are two categories of web-based content that is blocked from access on the SPU network. The first category is pornographic or sexually explicit web sites. The second category are web sites that promote, distribute various types of malicious software code, worms, viruses, keystroke loggers, spyware; or facilitate phishing attacks, fraud, identity theft, botnet command and control, and other cyber crime.

Download Policy as PDF

Content filtering is provided by FortiGuard.

Version: 1.1

Effective Date: *May 15, 2000*
Last Updated (minor revisions): *November 15, 2016*

Approved by:
President's Cabinet (Senior Leadership Team)
Responsible Office:
Computer & Information Systems
Responsible Executive:
AVP of Technology Services/CIO

Category One: Pornography

You may not fully agree with some facets of the University's behavioral expectations, but by enrolling as a student, or working as an employee of Seattle Pacific you have agreed to live according to the expectations outlined here.

This policy was put in place in May 2000 after extensive review and discussion by SPU student government, SPU faculty and administration, and ultimately approved by the President. It is acknowledged that the technology used to filter this material is not perfect, but the moral position being advocated with these tools support the lifestyle expectations of the SPU community.

Frequently Asked Questions

- **How are sites deemed "pornographic"? Who decides?**
  The content filtering company offers many categories of sites that clients may block, from pornographic to gambling. SPU has asked to have two types blocked: pornography sites, and sexual material. FortiGuard uses a search engine as well as human reviewers to constantly update the selection.
- **Isn't this an abridgment to my right of privacy and free speech?**
  When you signed up for a computer account at SPU, you agreed to a use policy that states in part: "Computing and network resources, and user accounts are owned by the University and are to be used for university-related activities only. Computer equipment and accounts at Seattle Pacific University should be used for legitimate instructional, research, administrative, or other approved purposes." While you may own your computer, the network resource is owned by SPU and paid for by all members of our community. Any inappropriate use not only may damage our relationships, but also is a misuse of a valuable resource. It is true that there may be other uses not in keeping with our campus computer use policy, but the university has determined that pornographic sites present particular issues in terms of addiction potential, shame and guilt, and harm to relationship between men and women.
- **Wouldn't it be better to allow people to make their own choices and learn by mistakes? Aren't we encouraged to engage the culture?**
  Engaging the culture may begin best with a statement about who we are as a community. The Office of Student Life (OSL) and CIS felt there is a difference between assisting people to make choices and sponsoring or facilitating over our campus system activities that are in direct conflict with our values that uphold the dignity of every human being, made in the image of God. We also note that the scale of the misuse means that following up on every violation would make a demand on our residence life, CIS, and counseling resources that could overwhelm our system, taking time and attention away from other pressing needs on our campus.
- **Won't there by any follow up to this policy to assist people who are struggling to resist accessing pornography via the Internet?**
  The OSL-CIS recommendation calls for the creation of a committee to review the problem on our campus and determine what resources we can offer that would be appropriate to each person who might want help. We recognize that all sectors of society are dealing with cyberspace pornography.
- **Is this "Big Brother Is Watching You" on our campus?**
  We hope everyone in our community will note that this recommendation has been very difficult for all of us who have researched the issue. President Eaton, in his response to our recommendation, affirmed that we must not approach this step in a judgmental or punitive manner, but in a way that reinforces what we stand for as a community. Our hearts go out to all people who are struggling with this issue, whether it is within their relationships or in the loneliness of one person and one computer screen. We affirm that sexuality is a gift from God that helps define us as human beings. We hope that if you struggle with the problem of pornographic web sites, you will remember that the blocking message you may get is not one of judgment and censorship, but a reminder that you have a community of people who value you, who think you are worth more than that web site suggests, and who need you.

Category Two: Security Risks

The second category are web sites that promote, distribute various types of malicious software code, worms, viruses, keystroke loggers, spyware; or facilitate phishing attacks, fraud, identity theft, botnet command and control, and other cyber crime.

These are the category definitions:

- **Malicious Websites**
  Sites that host software that is covertly downloaded to a user's machine to collect information and monitor user activity, and sites that are infected with destructive or malicious software, specifically designed to damage, disrupt, attack or manipulate computer systems without the user's consent, such as virus or trojan horse.
- **Phishing**
  Counterfeit web pages that duplicate legitimate business web pages for the purpose of eliciting financial, personal or other private information from the users.
- **Spam URLs**
  Websites or webpages whose URLs are found in spam emails. These webpages often advertise sex sites, fraudulent wares, and other potentially offensive materials.

CIS will regularly review and update these categories as the various computer threats and exposure change. The intent is to provide a layer of protection for all campus users to maintain a healthy and effective computing and network environment.

SPU Related Policies and Procedures:

Computer Acceptable Use