

# CURSOR

**Carnegie Mellon**  
**COMPUTING SERVICES**

[www.cmu.edu/computing/](http://www.cmu.edu/computing/)

The newsletter of Carnegie Mellon's Computing Services Division

## **The Gates and Hillman Centers: A New Media-Rich Environment**

Over the past several months, the Computing Services MediaTech group developed 26 new media-rich facilities within the Gates and Hillman Centers. Of the 26 new facilities, eight have been designated as Enrollment controlled teaching spaces with the remaining 18 being developed for specific School of Computer Science (SCS) applications. Through a collaborative initiative between MediaTech and SCS, the 18 SCS facilities have been jointly designed and were installed and managed as a team effort.

**This collaborative approach has integrated specific SCS faculty user requirements with MediaTech's campus-wide standards for media-rich facilities.**

This collaborative approach has integrated specific SCS faculty user requirements with MediaTech's campus-wide standards for media-rich facilities. As a result, this approach will simplify the transition for faculty members into the Gates and Hillman Centers by providing continuity with other campus-wide classrooms.

The new classrooms feature lecterns containing a touch-screen control system, DVD/CD player and ports for laptops and other auxiliary devices. These rooms also feature a document camera, which can project transparencies, pages from a book or images of objects. Enrollment controlled auditoriums throughout campus, including the Gates & Hillman Centers, now feature Dell computers and the iClicker classroom response system (see "Clickers Classroom Response System").

Computing Services Cluster Services also partnered with SCS to develop three new Clusters in the Gates and Hillman Centers, including two teaching Clusters (5201, 5205) and a collaborative workspace (3000). To ensure consistency with other Computing Services Clusters across campus, the new clusters will feature Red Hat Enterprise Linux.

The official opening of the Gates and Hillman Center is scheduled for September 22, 2009.

## **Clickers Classroom Response System**

Computing Services is pleased to announce that the i>clicker Classroom Response System (CRS) is now part of the technology in all large Enrollment controlled (Registrar) classrooms and auditoriums and is ready for use. The Clicker service is jointly supported by the Office of Technology for Education (OTE), the Eberly Center for Teaching Excellence and Media Technology Services.

The i>clicker classroom response technology will be installed in the small Enrollment controlled classrooms throughout the summer 2010 semester. Until then, faculty members who are scheduled to teach in small Enrollment controlled classrooms and would like to use Clickers sooner should contact MediaTech to arrange installation by emailing [mediatech@cmu.edu](mailto:mediatech@cmu.edu).

Instructor kits are still available for faculty members to use in their offices as they prepare course lecture materials. Each kit is comprised of a receiver, flash drive with software (Windows and Mac OS), one student remote and an instructor remote. Please contact MediaTech at 412-268-8855 or send email to [mediatech@cmu.edu](mailto:mediatech@cmu.edu) to reserve a kit.

*continued on page 2*

## **September 2009**

**The Gates and Hillman Centers: A new Media-Rich Environment**

**Clickers Classroom Response System**

**New Microsoft Campus Agreement**

**Cluster Updates**

**Security Tip: Avoiding Malware**

**New Look for the Web Portal**

**C@CM: New Hybrid Required Course for First Year Students**

**Help Center Service Changes**

“Clickers Classroom Response System” continued from page 1

For a complete list of small and large classrooms, see [www.cmu.edu/computing/mediatech/classrooms/](http://www.cmu.edu/computing/mediatech/classrooms/). To view the availability of these rooms, please visit Space Quest at <https://enr-apps.as.cmu.edu/r25webapp/r25webapp>.

Please visit [www.cmu.edu/teaching/clickers/](http://www.cmu.edu/teaching/clickers/) for information on best practices, as well as Clicker documentation for equipment set-up and use.

## New Microsoft Campus Agreement

Carnegie Mellon’s Microsoft Campus Agreement, a campus-wide software licensing contract, was renewed on June 1, 2009. The new agreement includes Microsoft Campus Desktop, which is comprised of Office Professional, Windows Update, and Core Client Access Licenses. It also includes a student option and work-at-home rights: the student option gives students the right to run Microsoft desktop software on personal or university-owned equipment while their enrollment at the university is current. Members of the faculty and staff may install and use one copy of the software at work, as well as one copy on a home machine.

Media can be purchased at the University Store; product keys are distributed with the media. The Campus Desktop package includes the following:

### Office Windows Enterprise Edition & Mac Professional Edition

- Windows: Access, Outlook, Excel, PowerPoint, Publisher, Word, Communicator, Groove, InfoPath, OneNote
- Mac: Entourage, Excel, PowerPoint, Word, Virtual PC

### Windows Upgrade

- 32-bit or 64-bit Windows Vista Business, Enterprise, & Ultimate Edition

### Core CALS (Client Access License)

- Windows Server, Exchange Server, SharePoint Portal Server, and System Manager Server

## Cluster Updates

In a continuing effort to enhance the teaching and learning experience for faculty and students, Cluster Services completed a number of improvements over the summer months; the highlights are as follows:

- Red Hat Enterprise Linux 5 replaced Andrew Linux in all Computing Services Clusters across campus. Red Hat Linux is a more modern operating system featuring an updated application set, as well as the GNOME and KDE desktops.
- Software that enables popup printing to public Cluster and library printers was upgraded. This upgrade greatly simplifies the printer installation process on personal Windows computers; it also resolves previous issues with personal printing from Mac Leopard. Along with the software upgrades, new print release stations were installed.
- A number of Cluster software applications were updated; the most notable are Mathematica v7, the Adobe CS4 product line (including InDesign, Dreamweaver, Photoshop and more), iLife 09, Maya 2009 and others. For more information, refer to our software page at [www.cmu.edu/computing/clusters/software/](http://www.cmu.edu/computing/clusters/software/).
- Over seventy new Windows computers have been installed in Baker 140C, CFA 317, Cyert and West Wing Clusters. West Wing also received new Linux hardware.
- Baker 140E & F received new ergonomic “Think” chairs and the West Wing Cluster furniture was rearranged to create a more open space for collaboration.
- New video cameras are available through the College of Fine Arts (CFA) lending collection. The lending request form continues to be available online and items are loaned using your Carnegie Mellon ID card; see [www.cmu.edu/computing/clusters/lending.html](http://www.cmu.edu/computing/clusters/lending.html).
- A new HP color laser printer was installed at the CFA cluster.

Additionally, Clusters partnered with the School of Computer Science to develop three Clusters in the Gates and Hillman Centers (see “The Gates Hillman Centers” on page 1). For more details on Cluster hardware and software, visit [www.cmu.edu/computing/clusters/](http://www.cmu.edu/computing/clusters/).

## Security Tip: Avoiding Malware

A program that is installed on your computer without your knowledge, via websites, pop-ups or free software downloads, is referred to as “malware.” Spyware is a form of malware that sends information from your computer to a third party without your consent. Spyware/malware programs can steal your identity information, connect to botnets and post your password and other personal data to a botnet repository.

### Facebook, YouTube Sites Pose Higher Security Risk

The Information Security Office (ISO) has seen a recent increase in the number of exploits related to malware embedded in web site frames, movies or pictures. These are downloaded by users as they casually browse the Internet, especially on social networking sites. Sometimes the user is prompted to download an “update” of Adobe’s Flash software, but the file that’s downloaded is actually a Trojan horse or malware. Some recent examples are the Koobface Trojan or the rogue application “Personal Defender 2009.” These programs have infected computers via Facebook, YouTube and other media sites. Users should be aware that these sites carry a higher risk of compromise and should be careful about following links sent to them by friends in email.

Although removal tools often work to remove varying types of malware, the computer’s operating system will sometimes need to be reinstalled in order to completely remove the threat. In most cases, this results in some amount of computer downtime.

Practice safe computing! Reduce the likelihood of an infection by following these security measures:

- Don’t click on links within pop-up windows—instead of removing malware, these pop-ups often install it!
  - Choose “no” when asked unexpected questions, such as whether to run a program or task.
  - Be wary of free downloadable software.
  - Don’t follow email links claiming to offer anti-spyware software.
  - Adjust your browser preferences to limit pop-up windows.
- Frequently update all Adobe software directly from the Adobe site. Adobe recently issued a major upgrade for all of its software products which should be downloaded. For Adobe product upgrades, visit [www.adobe.com/downloads/updates/](http://www.adobe.com/downloads/updates/).
  - Patch your operating system and virus signatures by scheduling automated upgrades and updates; for help refer to our security documentation at [www.cmu.edu/computing/doc/security/](http://www.cmu.edu/computing/doc/security/).
  - If you use Mozilla Firefox for casual browsing, use it with the Netcraft anti-phishing toolbar. This toolbar will warn you about sites that are known to belong to phishers. Another recommended solution is to install Firefox’s NoScript add-on. This add-on preemptively blocks javascript in all sites except for the ones you specify in a whitelist.

### Computer Compromised?

If you suspect your computer has been compromised via malware, STOP! Take the following steps immediately:

- Disconnect from the network—turn off wireless or unplug the wired network cable.
- Discontinue use of the machine but DO NOT turn the power off.
- Refer to security documents listed at [www.cmu.edu/computing/security/](http://www.cmu.edu/computing/security/), or contact the Help Center at 412-268-HELP (4357) or [advisor@andrew.cmu.edu](mailto:advisor@andrew.cmu.edu) or your DSP consultant or departmental computing administrator for further instructions.

For more information on the process for responding to compromised computers, visit [www.cmu.edu/iso/governance/procedures/compromised-computer.html](http://www.cmu.edu/iso/governance/procedures/compromised-computer.html). For help with cleaning an infected Windows computer, visit [www.cmu.edu/computing/doc/security/clean-win/](http://www.cmu.edu/computing/doc/security/clean-win/).

### New Look for the Web Portal

The Carnegie Mellon Web Portal has been redesigned. Visit the portal and see for yourself!

<https://my.cmu.edu/>

## C@CM: New Hybrid Required Course for First-Year Students

During the fall 2009 term, Computing Services, in partnership with the Open Learning Initiative (OLI), will pilot the first phase of a new hybrid course model for the Computing@Carnegie Mellon (C@CM) undergraduate course. The hybrid course will be delivered through a combination of live, hands-on classroom instruction and the OLI's online course environment. The first phase will focus on file storage and sharing, where students will learn strategies for choosing options that are efficient, dependable and secure. Students will learn how to apply these strategies to the specific file storage and sharing options they are afforded as members of the Carnegie Mellon community, along with the university-specific tools they will use to store and share their work.

C@CM is a 3-unit, pass/fail course that is required for graduation for all undergraduate students. The course is aimed at providing new students with a quick introduction to the skills that will allow them to navigate the local computing environment. Since its inception in 1989, C@CM has continued to support the university's teaching and learning needs by providing educational programs on relevant technologies and commonly used tools. Students are taught how to make safe and responsible decisions in their use of technology, as well as strategies and conceptual skills that can be translated across electronic resources and emerging technologies.

The OLI offers intelligent tutoring systems, virtual laboratories and simulations that provide frequent opportunities for assessment and feedback. The OLI courses are intended to enact dynamic, flexible and responsive instruction that fosters learning. All of the instructional activities have embedded assessment tools that collect real-time interaction level data of students' use. These powerful feedback loops provide opportunity for continuous evaluation and improvement for not only the students, but instructors as well. The C@CM teaching assistant staff will use the assessment data to inform and target their instruction to the skills and concepts students have yet to master.

Future phases of the hybrid course will be developed in collaboration with the C@CM Advisory Committee. Send email to [c-cm@andrew.cmu.edu](mailto:c-cm@andrew.cmu.edu) for additional information.

## Help Center Services Change

In a continuing effort to provide high quality, cost-effective computer troubleshooting service when "hands-on" assistance is necessary, the Computing Services Help Center has enlisted SARCOM, a third party vendor. Previously, the Help Center provided hands-on troubleshooting, but on a best-effort basis only. Effective August 3, SARCOM assumed this work as part of their comprehensive menu of fee-based services.

For the past year, SARCOM has managed a computer hardware repair service on campus through the University Store. This service has been expanded to include software repairs such as the diagnosis and removal of viruses and spyware as well as the diagnosis and repair for operating systems. The Computing Services Help Center will offer users brief triage and will make appropriate referrals to SARCOM or to self-service documentation for software repair.

Although SARCOM's service is extensive, it is also fee-based. To avoid the need for computer software repair that results from misuse or malware, we encourage all campus affiliates to take the following steps:

- Always shut down personal computers properly.
- Update software on a regular basis through Microsoft, Apple and anti-virus updates.
- Remove any file sharing programs (e.g., Kazaa, Limewire) or disable file sharing on these programs.
- Exercise care in opening email attachments or attachments received through personal networking sites (see "Security Tip: Avoiding Malware" on page 3).
- Don't share personal computers; keep them physically secure.

Overall, follow steps outlined in the online Security documentation at [www.cmu.edu/computing/security/](http://www.cmu.edu/computing/security/).

For a detailed list of software and services supported through the Help Center, visit [www.cmu.edu/computing/help-center.html](http://www.cmu.edu/computing/help-center.html). SARCOM's price list is available through the Computer Sales Web site at [www.cmu.edu/stores/computer/ComputerRepair/](http://www.cmu.edu/stores/computer/ComputerRepair/).