



Classroom Technology Support

The installation of instructional technology in the classrooms is now complete. All generally scheduled classrooms have been equipped with ceiling-mounted projectors and tech desks including computers, DVD/VHS players and a control panel to simplify operation of the equipment.

Support for this new classroom technology will be managed by Kathleen Weidner, as a part of User Support. For assistance with instructional equipment, call the Helpdesk at x5555, and press "1" for classroom support. Your call will immediately be directed to Classroom Technology Support where you will receive the level of service to which you've grown accustomed.

The Classroom Technology Support (CTS) unit consists of manager, Kathleen Weidner, Classroom Tech Assistant, Jessie Onderdonk, and a Classroom Tech Consultant (currently being searched). Helpdesk staff will be cross-trained on the equipment in order to provide additional assistance as needed. The CTS unit provides support for classroom instruction only. Non-instructional requests whether internal or external, will be handled by Media Support (as seen below).

All existing mobile equipment will be reallocated to Media Support, maintained in Classroom Tech Support for quick swaps, or permanently distributed for departmental use.

Media Support

Media Support provides consultation and services related to traditional audiovisual, digital media, and presentation technology. Areas of support include:

Event support – Audiovisual support of live events ranging from a single microphone at a podium to complex multimedia presentations for large groups.

Videoconferencing – Technical support of the two-way interactive video conferencing facilities and equipment.

Media systems design - Design and integration of presentation technology systems on campus. Recent projects include the SAC AV technology, the instructors station in the Informatics lab, and the classroom technology desks.

Media production - Design and production of analog and digital audio and video programs related to instruction and other university functions, to include duplication, format conversion, and digitization.

Media consultation - Consultation with faculty regarding audiovisual and media equipment and systems, ranging from departmental purchases of cameras to advice on the technical component of grant applications.

Restart for clean start

PCs in the labs as well as instructor stations in classrooms have been configured to return to their original pristine state after a restart. This keeps them from accumulating bothersome software and pop-ups installed by previous users. To ensure the best operation, IT encourages users to restart the computer before using. It only takes a few seconds, and could prevent problems in your session.

Making IT Happen!

Indiana University students, staff, and faculty can "Get with IT" to learn about information technology resources, innovations and support tools at *Making IT Happen!* – an annual information technology fair held on IU campuses statewide. Those who attend can see demonstrations, student showcases, and get information on tech-related opportunities, products, and services.

Refreshments and giveaways cap off the fun-filled event – making it a place where techies and the confessed technologically challenged can come together to learn something new.

Tuesday, March 22, 2005
10am—3pm
Student Activity Center
Rooms 221, 223, 225

Have you signed up for spam filtering?

If you haven't taken advantage of the spam filtering provided with your IU email, please consider registering for it now. This service quarantines those pesky email messages and gives you a list to review if you choose. To learn more about this service and register, visit the IT web page, www.iusb.edu/~sbit and follow the links for e-mail and spam filtering.

IT Helpdesk

DW1245

Hours:

8:00 am—8:30 pm, Mon-Thurs.

8:00 am—5:00 pm, Friday

www.iusb.edu/~sbit

Phone: 574-520-5555

E-mail: helpdesk@iusb.edu

Protect Yourself!

On campus.....

- **Create a secure password.** Do not write it down. Create a password that is easy for you to remember, but impossible for someone to guess. For suggestions, visit kb.iu.edu and search on "password".
- **Never share your password with anyone.** You are held responsible for anything done under your username.
- **Restart the computer when you finish in the lab, or when you leave your office for the day.** A good practice is to restart the computer rather than just logging off. (Select Shut Down, then select Restart.)
- **Lock your screen when you leave your computer momentarily** by pressing the Windows key and "L", or set a passworded screen saver to automatically lock your screen after 10-15 minutes inactivity. In both instances your password is required to start using your computer again.

At home.....

- **Turn on the Windows firewall.** (In Windows XP, select Control Panel, select Windows Firewall, then select the "ON" option.)
- **Install Symantec Anti-virus.** Schedule a daily scan of your computer. Perform a Live Update once a day to acquire new virus definitions.
- **Install Spybot and configure to immunize your computer.** Check for updates weekly.
- **Check Microsoft Windows Update weekly for patches.** Or better yet, set your computer to automatically download and install critical patches as they are made available.

Storing and Transporting Data

Zip drives began to be eliminated on campus last fall in computer labs, classrooms and employee offices. Beginning this spring new computers ordered for employees will no longer include floppy drives as these become obsolete in view of the more current technology. Computer labs will begin eliminating floppy drives in summer 2006.

IT discourages users from storing data on the local C:drive of office computers, whether Mac or PC. This can prolong downtime during upgrades, and increases the risk of data loss. In the labs, anything stored on the C:drive will be deleted when the computer is restarted.

*So, where **should** you put your data files for storage and transport?*

- ◆ **Network drives** are available to faculty and staff with varying levels of security. The files on these drives are backed up each evening, as well as maintained on monthly and yearly tapes. Just remember HOW:
 - H:** is for departmental data, which is accessible to everyone in your department. Subdirectories with further restrictions can be created for administrators or secretaries for all departmental-related files.
 - O:** is your private directory. No other user has access to it. This is for information that would not be needed if you were to leave the university.
 - W:** is a campus-wide shared directory. This drive is for sharing files with faculty and staff.
- ◆ **Network drive** space is available for students via their M:drive.
- ◆ **USB drives**, also known as flash drives are very easy to use and can plug into the USB port of any current computer so are great for transporting files.
- ◆ **CDs** can be burned from all lab and office computers and are an economical way to store files for backup or transport.

Beware of Phishing

Beware of e-mails that are "phishing" for information. These emails appear to be from legitimate banks or institutions and frequently allude to security issues with your account, and ask you to confirm information.

Do not use any links that are in this email. Check directly with the institution directly if you think they might be real, but most institutions will not send requests for such information through e-mail.

Infected Dialup Users Will Lose Access

Users connecting to the internet through IU South Bend's dialups will be disconnected if their computers are found to be infected by a malicious virus. IT scans the dialup lines for virus-type activity which could be harmful to other computers connected through dialup as well as to the campus network. When an infected computer is identified, the user's access for dialup is discontinued until the computer is cleaned and updated with the latest anti-virus software.

All IU students and employees are encouraged to use Symantec Anti-Virus software on their home computer. It is provided on the IUware CD which is sold in the bookstore for \$5. The software provides for an easy live update for the latest virus patterns, and should be updated every day.

Also, visit the windows update web site, windowsupdate.microsoft.com to check for and apply the latest critical patches. When Internet Explorer is launched, you can also click on "tools" and "windows update" to take you automatically to the update site.

Wednesday Nights

Remember to leave your office computers powered ON, but logged OFF when you leave on Wednesday. IT uses this night to centrally push patches and system upgrades, in order to minimize interruption for you during the day.

We appreciate your cooperation in keeping our campus computers updated and secure.

*Information Technologies
It Update - March 2005
Beverly Church, Editor*