THE UNIVERSITY OF MEMPHIS
Information Technology Services

CENTER FOR TEACHING AND LEARNING NEWSLETTER

Volume 7 Issue 8, December 2020

IN THIS ISSUE: FALL REVIEW AND SPRING UP!

SPRING 2021 FACULTY CHECKLIST

Are your Spring 2021 courses ready? Here's a handy checklist:

- ☐ Locate Spring '21 Courses in eCourseware
- ☐ Upload/Create Course Syllabus and Content
- ☐ Add an Instructor's Welcome Message
- ☐ Setup Course Gradebook
- ☐ Create Assignments (Dropbox,Quizzes, Discussions)
- ☐ Connect Publisher Widgets/Links to Course
- ☐ Ensure Your Students are Listed on the Classlist
- ☐ Add TA/GA to Course (If Needed)
- ☐ Submit a Course Combine Request (If Needed)
- ☐ Submit a Course Copy Request (If Needed)

DELL DISCOUNT STORE (STUDENTS)

Students that are enrolled at the University of Memphis can receive a discount on laptops. Moving largely to remote learning has taught us that a good laptop is essential to a good course experience. The discount store for students will provide deals and recommendations on reliable, fast, and secure laptops for students.

For more information about the Dell discount store, visit the Dell Discount Store for Students. Also, visit the Center for Teaching and Learning webpage on Remote Teaching Options, including hardware recommendations for instructors, students and staff.

Extended Course Access

There are times when students need access to the course beyond the course end date. Often, this occurs when students have incomplete work in the course due to extraordinary circumstances. If this is the case, you can grant extended access to your course in eCourseware for the student by placing an Extended Course Access service request. Please keep in mind, for the students to submit assignments, complete quizzes and access the content in the course, you must ensure the end dates for those assignments, quizzes, and content is extended as well. While the CTL team can provide the student(s) extended access upon your request, the system does not have an automated way to remove the extended course access. Therefore, you will need to enter a separate request to have the student's extended access to the course removed, once the student(s) have completed their work.

ECOURSEWARE INTEGRATIONS – COURSE LEVEL OR ORGANIZATION LEVEL?

If you have ever investigated a new integration to add to eCourseware, such as a web tool or textbook e-text, you already know about all the different variables that go into choosing the right one. When you speak to a sales or customer service representative about a prospective eCourseware integration, along with considerations of accessibility, cost, and ease of use, it is a best practice to ask another question: Does this integrate at the course or the organization level?

On the surface, that may seem like a technical question, but, in the end, it could make or break the ability to get the new tool adopted into eCourseware. When a tool integrates at the organization level, it is fairly simple to copy that tool from course to course or add it to new courses without issue. Our widely used integrations, such as MyLabs or Cengage, do just that. Often, anyone who wants or needs to use it in their course can just request it and have it added, once it has been added to our repertoire. However, course level integrations are often much more difficult. They may require the tool to be added and tuned for each course, individually. The tools may not work when copied from course to course or semester to semester, and you may have to redo work that you thought was already complete. This is why we recommend that, when you're looking into new integrations to make your classes more interactive or easier, you ask the question above and take special note of the answer.

Keep Our Data Safe

The University of Memphis is committed to protecting the security and confidentiality of the information entrusted to us. Protecting the University's infrastructure and data is a shared responsibility involving policies, procedures, guidelines, technology, and employees.

University Policy IT6007 formalizes the University's Information Security Program and defines additional policies designed to protect institutional infrastructure and data. Employees are required to review the Information Security policies annually. In addition to the University Information Security policies, employees are reminded to review and follow the Guidelines for Storage of University Electronic Data and Classifications of University Data.

Important Reminders

Social Security Numbers (SSNs) should not be transmitted or stored in email, OneDrive, NAS space, UMWiki, or other electronic media regardless of the data classification or intended use.

Similarly, PCI credit card data may not be stored in any University system, server, personal computer, e-mail account, portable electronic device (laptop, flash drive, CD/DVD, PDA, cell-phone, tablet, portable hard-drive, etc.) or on paper document.

Information Technology Services has implemented several technologies to support the Information Security Program. Specifically, technologies have been deployed to enhance security for email, networking, desktop security, and authentication in addition to supporting the IT Security Awareness Training efforts. Please contact your Local Service Provider or ITS Service Desk for more information on technology available to secure desktops, email security, Duo authentication, or other questions about the Information Security Program.

Employees are required to complete IT Security Awareness Training annually to develop an understanding of basic principles designed to protect and enhance the University's data security. If you have not completed this year's IT Security Awareness Training, please visit the training portal to access and complete the course.

BEST PRACTICES FOR CYBERSECURITY

UofM has several ways to protect digital activities and accounts related to the University. All these best practices can be adopted in your personal digital life as well.

Your passwords are the keys to your digital kingdom.
Protect them as you would the keys to your house or auto.

- Don't share your passwords with anyone. ITS will never ask for your password in assisting you with an issue.
- Use a different password for each website.
- Long = strong. Create a passphrase rather than a password:

    1. String together 3 or 4 random words.
    2. Add a couple of numbers and special characters.
    3. Add a couple of characters to remind you what website it is for.

MULTI FACTOR AUTHENTICATION (MFA)

MFA is your best friend in keeping your accounts secure. At UofM we use Duo for MFA. It provides an extra layer of security on an account in case your password is stolen or guessed. MFA requires an additional means of identifying yourself, like a token with a passcode or use of an app on a cell phone. If your password is cracked, a hacker still cannot access your account unless he/she also has your phone or token to authenticate the log-in.