



Office of Information Technology Support Guide

Office of Information Technology

SODHelp@umaryland.edu
410-706-2084

Support Guide

The Office of Information Technology strives to provide the best possible service to our faculty, staff, and students of the University of Maryland, School of Dentistry. To better serve you, below are links to assist and support you. Many of these links navigate to the central information technology organization for the University, also known as Center for Information Technology Services (CITS) www.umaryland.edu/cits.

Wireless Internet Connection	3
Campus Wireless Connection.....	3
Wireless Setup on Specific Devices.....	3
Email.....	3
Google@Umaryland Mail	3
myUM Mail.....	3
UM Mail Lists	5
Encryption.....	5
Phishing Emails	6
Spam Quarantine	7
IronPort.....	7
Accellion	7
Printing.....	8
Campus Phone	9
Remote Access (VPN)	9
Information Storage.....	10
Self Service Applications	11
MyUM ID	11
UM Directory Authentication	11
UM Alerts	11
myUM Portal Page.....	11
Novell Vibe	12
COEUS	12
OIT Support Guide	1

Effort Reporting System (ERS).....	13
EHS Training Registration System	13
ORD Research Data Warehouse.....	13
Clinical Applications	13
Axium.....	13
Romexis	14
Instructional Technology Applications and Equipment.....	15
Questionmark.....	15
Blackboard.....	16
Turning Point.....	17
Lesson Builder	17
Mediasite.....	17
GoogleApps@UMaryland.....	17
Audio/Visual Equipment Loan Request.....	18
Loaner Laptop Requests.....	19
Troubleshooting HELP!	20
Get HELP!	20

Wireless Internet Connection

Campus Wireless Connection

The School of Dentistry, in conjunction with the campus (CITS), maintains wireless network Eduroam, the secure, world-wide roaming access service developed for the international research and education community. Eduroam allows students, faculty and staff from participating institutions to obtain Internet connectivity across campus and when visiting other participating institutions by utilizing their local login credentials (myUM ID) on their laptop or Smartphone. Eduroam also gives the faculty, staff, and students the ability to connect to any wireless system in the University regardless of the building you are in.

Wireless Setup on Specific Devices

For users of laptops, smartphones, tablets, or other wireless-capable devices, wireless access can be obtained by connecting to the wireless network, Eduroam. For specific directions, please visit <http://www.umaryland.edu/cits/communications/eduroam>

Email

Google@Umaryland Mail

GoogleApps@UMaryland (or Google Apps For Education (GAE) is a communication and collaboration tool for students and residents that was implemented in Summer 2011. Students share ideas quickly and get things done effectively when they have access to the same powerful communication and sharing tool. GoogleApps@UMaryland contains E-mail, Calendar, Docs, Groups, Sites, Talk, and Mobile Apps. There's no hardware or software to install. Everything is delivered through a standard web browser. Access is anytime, from anyplace! For more information about GoogleApps@UMaryland, click below.

<http://www.umaryland.edu/helpdesk/systems/gae/index.html>

myUM Mail

Faculty, staff, and affiliates each have a dental.umaryland.edu account. This is an enterprise email system run by the campus IT (CITS) staff and managed by dental IT (OIT) staff. The mail system is currently Microsoft's Exchange 2007 and can be accessed via Outlook clients that run on Windows, Mac OS X as well as a web browser.

User mailboxes can grow to a maximum of 2 gigabytes (GB).

The procedure for connecting an Outlook client (PC and Mac clients are available or many smartphones or tablets) involves providing basic account information to an AutoDiscovery wizard that retrieves published configuration information without you needing to know or supply it. One key point to remember is that the mail server, the system that receives, stores, and transmits your email is running Microsoft Exchange; using POP or IMAP settings will generally not produce the best results. Figure 1 shows you a typical page where you need to provide your email address in the form <Dental ID>@dental.umaryland.edu and the password is your Dental ID password.

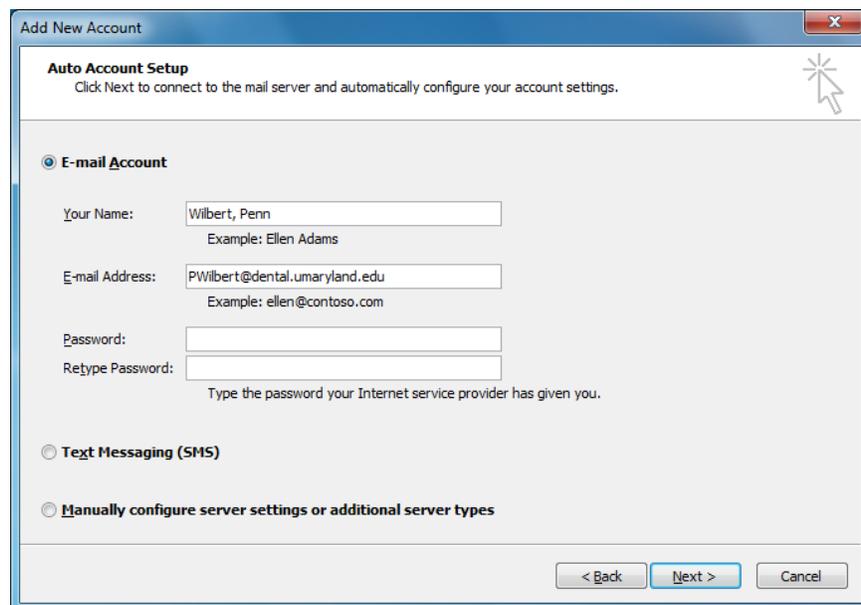


Figure 1: Outlook Account Info for AutoDiscovery

Email may be accessed from a web browser using Outlook Web Access (OWA). Connect to <http://umail.umaryland.edu> and use your Dental ID credentials. For example, in the section shown in Figure 2 you can type in the Domain\User name section <Dental ID>@dental.umaryland.edu and the password is your Dental ID password. Just remember again this is using your Dental ID information, not your myUM ID information.

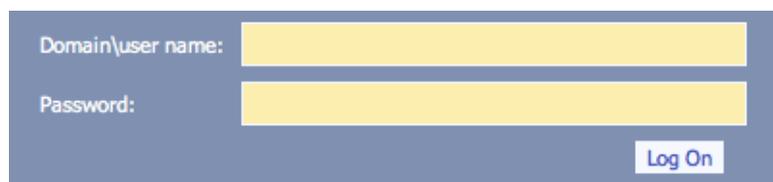


Figure 2: OWA Login Section

For additional information on myUM Mail, click below.

http://www.umaryland.edu/helpdesk/getting_started/UM_mail.html

UM Mail Lists

A UM Mailing List is used to send email messages to a group of email addresses. Once created, owners of the UM Mailing List have the ability to maintain their list through the UM Mailing List interface. They can add or remove subscribers and configure the sending and receiving options on their list. For more information and directions on UM mailing lists, click on the link below.

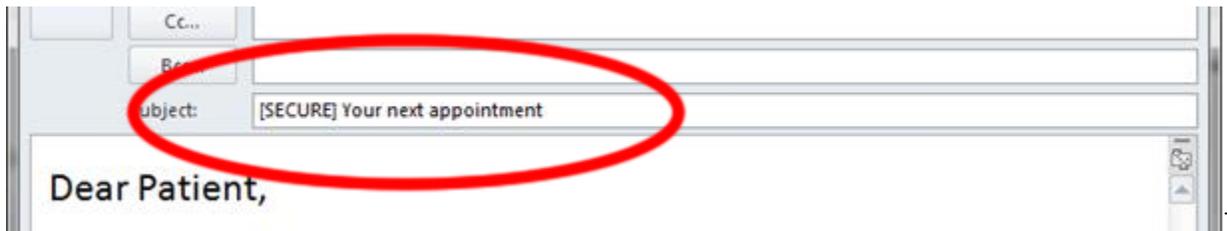
<http://www.umaryland.edu/helpdesk/systems/umbmailinglists/index.html>

Encryption

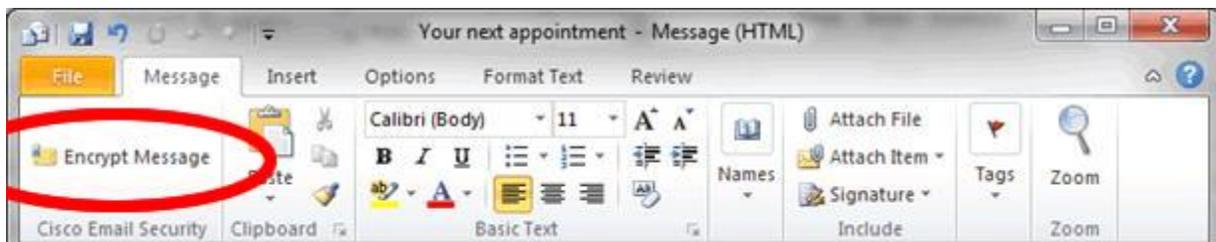
All electronic communication must be from a School of Dentistry issued email account. The secure messaging system must be used for all email communications with or about patients, from any and all School of Dentistry employees, students or affiliates.

Send an encrypted email one of two ways:

- (1) Add the term “[SECURE]” at the beginning of the subject line within the email. The word “secure” is non-case sensitive;



- (2) If using Microsoft Office Outlook, open a new email and then click on the “Encrypt Message” button under the Message tab.



Text messaging is not an acceptable form on electronic communication because we do not have a secure encrypted text messaging system.

Phishing Emails

Have you ever received an email claiming to be from the IT group asking for your email user name and password? *Do not respond to it!* What you have just received is a 'Phishing Email.' It is not a legitimate email message.

<i>If you</i>	<i>Then you need to...</i>
Responded to a phishing email	Immediately change your password
Responded to a phishing email and now you can't log into your email	After the system administrators receive notification about a new phishing email attack they try to identify any users that have responded to the email. Call OIT or submit a ticket.
Are unsure if the email message is legitimate	Forward the message to sodhelp@umaryland.edu . Do not respond to the message itself.

Here are some of the tips and tricks to identify spam from a legitimate email:

1. Most importantly! If the link that the email message wants you to copy and paste into your browser is not from the umaryland.edu domain, then it is probably SPAM. The spam email may direct you to go to a website with a domain name of atwebpages.com.
2. Do not trust who the email is from. The below email states that it is from helpdesk@umaryland.edu; the name looks correct, but it is actually not. When email was designed as a form of communication, checks and balances as to the official sender were never included in the technology. If the grammar on the email is very poor, then it is probably SPAM. Usually when an email is being sent with the intent to inform large amounts of people about a change, the grammar and spelling are checked for errors.
3. 4. If you are ever in doubt about your username and password, please go to one of two places in order to resolve this:

a. <http://myumb.umaryland.edu>

b. <http://umail.umaryland.edu>

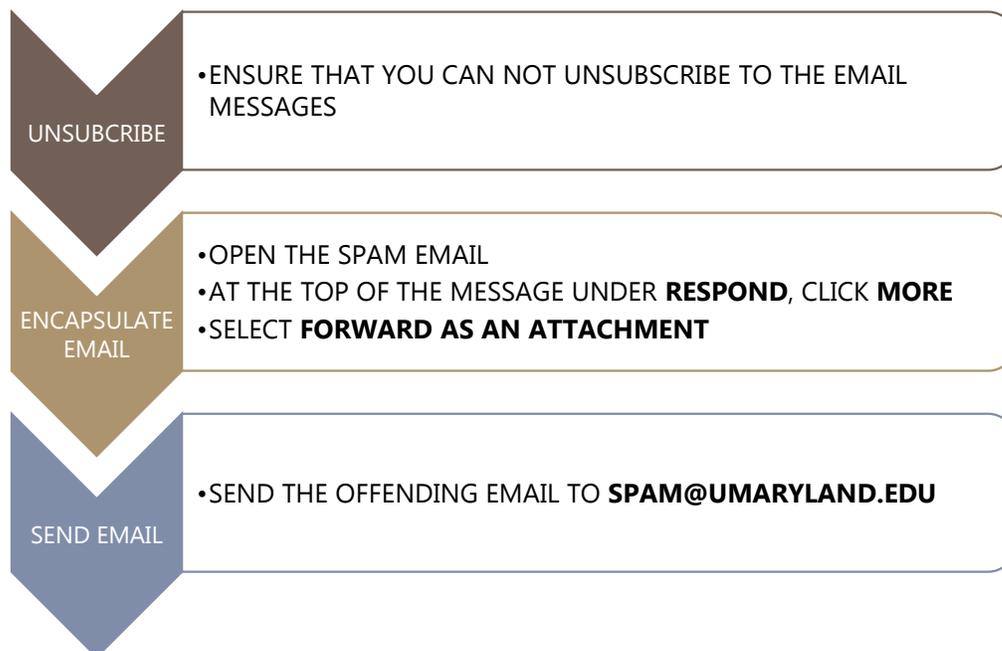
DO NOT resolve a username and password issue in another forum. DO NOT give your username and password to another website.

If you want more information on how to identify a spam message, please see the link below from Microsoft about some other tricks that spammers will try:

<http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx>

Spam Quarantine

If you receive an email that you CAN NOT unsubscribe to, follow this procedure to avoid receiving these emails:



IronPort

IronPort is the campus' email security and SPAM quarantine solution. For more information on quarantine notification emails, SPAM email, and other IronPort capabilities, click on the link below.

<http://www.umaryland.edu/helpdesk/systems/ironport/index.html>

Accellion

The campus (CITS) operates a file transfer system that allows for the secure, encrypted transfer of large files. Email attachments are limited to 30 megabytes (MB) and may or not be encrypted during transfer depending upon the recipient's mail server.

The Accellion system allows the internal user to invite external users to upload files and transfer files back and forth. Additionally, an email notification may be generated when the recipient downloads the file you've sent. File size can be up to 2 gigabytes (GB) and be sure to use your

myUM ID. Check <http://www.umaryland.edu/helpdesk/systems/accellion/index.html> for details and instructions.

Important Tips to Note

- The encryption being discussed above only covers the transfer of the information. Once the information arrives, there is no encryption in place unless you encrypted the information before you sent it. Consider Electronic Patient Health Information (ePHI).
- This device should not be used for storage. Files you transfer using it only remain for two weeks and there is no warning when they are removed.

Printing

For faculty, staff, and affiliates, each department has a designated multi-function printer (MFP) that is automatically installed on your computer during the creation of your account. This printer has a designation of room number, location, and/or printer model in its name to help determine the machines' location.

We utilize a print system called PaperCut to provide a secure mechanism that enables users to print documents to any printer simply by swiping their UMOOne Card. PaperCut is implemented to all users except those on the clinic floor printing from Axiom (this is a direct printing process that does not need the UMOOne Card to be swiped).

To get started, users must first enroll themselves in the PaperCut system. You will only need to complete this process once. However, you will be unable to print and retrieve documents until you have completed the enrollment process. To get registered with PaperCut, please follow these simple steps outlined here: <http://sodhelp.umaryland.edu/papercutjobaid.pdf> or watch a short video presentation on Mediasite:

<http://mediasite.umaryland.edu/Mediasite/Play/20448cef16b8445ca89aa4be76a4527d1d> .

If there is not a printer listed for your area, please contact the Help Desk (sodhelp@umaryland.edu) and provide:

1. Your username
2. Your room number
3. Your department
4. The room number the printer is near that you would like to be connected to

We also have a large format printer to use for posters and canvas printing. The services of the large format printer can be requested through the OIT department website www.dental.umaryland.edu/oit by selecting **Purchasing Requests**.

Campus Phone

The School of Dentistry uses campus provided Cisco VoIP (Voice over IP) handsets. You can find out more information about how to use this handset and the campus voicemail system by visiting: http://www.umaryland.edu/cits/services/network_telecom.html and see the Phone Manuals & Information section which includes a video tutorial of the phone features.

If applicable, you may request to receive a copy of voicemails in your email box. To request activation, go here http://www.umaryland.edu/CITS/FORMS/UNIFIED_MESSAGING.HTML

Remote Access (VPN)

A VPN (Virtual Private Network) is a technology that allows for safely connecting to the UM Campus network over the public internet. The VPN encrypts data while it being transferred to or from the campus and also allows for limiting outside access to resources by making them only available via VPN.

The campus VPN appliance is managed by the campus (CITS) and supports Windows, Mac and Linux clients. VPN access is managed by the OIT Helpdesk and is provided by request. You will need to use your myUM ID credentials for signing on.

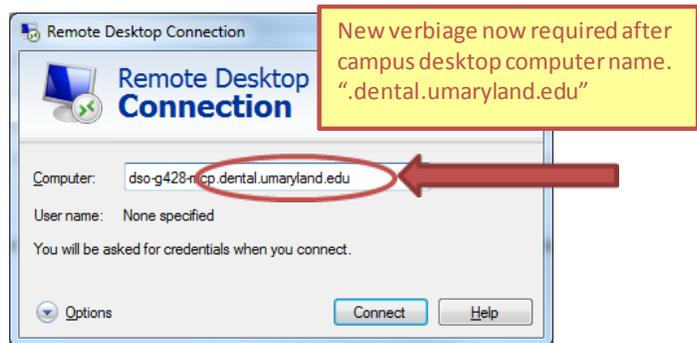
You can install the client, which requires Java, by visiting <https://vpn.umaryland.edu>.

For more specific instructions on how to download VPN and check to ensure your system meets requirements, go to <http://www.umaryland.edu/cits/vpn/>. For more specific directions on how to download VPN, go to http://dshelp.umaryland.edu/manual/index.php/Remote_Desktop/VPN_Faculty.

Once the VPN install is complete on your non-campus computer, reboot your computer. When your computer is back up, run the VPN program, press Connect. A login box will appear, simply login the same way you do for e-mail dental\username and press ok. After a few seconds the window should go away and you will now see a lock icon in the bottom right corner, notice that the lock is locked, that means you are connected to the dental school network.

Now you can use Remote Desktop to login to your office PC. Remote Desktop Connection is integrated in Windows XP, Vista, and Windows 7; and is found under Programs - Accessories. Simply run it and enter in the name of your office PC, this is found by double clicking on the LANDesk Remote Control icon found in the bottom right corner. Highlighted in blue is your office PC's computer name.

Log on normally as you would if you were in your office; you now have access to anything you have access to if you were in your office.



Information Storage

For faculty, staff, and affiliates, file storage is provided for both personal and shared arrangements.

Personal Storage

Personal storage is allocated to users for storing documents and data. The information is backed up nightly and periodically moved offsite. Faculty and staff are initially allocated 5 gigabytes of space. This will be listed as your Z: drive.

Local storage of important information and documents is strongly discouraged.

Local storage of information and documents means storing information on your local computer's hard drive (your C: drive, for example) or a USB flash drive unless you are making sure the information is regularly backed up or copied elsewhere. Please be extremely careful storing information here. To ensure the information is copied and backed-up, it is recommended to store information on the Z drive or shared storage place.

Self Service Applications

MyUM ID

Your myUM ID and password is used to log into many resources provided by the University of Maryland such as eUMB, the myUMB Portal, Blackboard, Mediasite, COEUS, Effort Reporting, SURFS, GoogleApps@UMaryland and myUM Mail.

For how to create a myUM ID and password, click on the link below.

http://www.umaryland.edu/helpdesk/getting_started/FirstTimeUser.pdf

For additional resources and information on myUM ID, click on the link below.

http://www.umaryland.edu/helpdesk/getting_started/UMValues.pdf

UM Directory Authentication

The myUM ID is a crucial part of moving towards a single-sign-on system which will reduce the number of passwords and logins each user must remember and maintain. For additional information, click below for FAQ's. <http://www.umaryland.edu/helpdesk/accounts/faq.html>

UM Alerts

UM Alerts is the system used by the **Emergency Management Team** to send text messages about campus emergencies to the University community. The system will also be used for campus closing or delayed opening announcements. You can register personal devices, such as cell phones, smartphones or pagers that are capable of receiving SMS text messages.

To add your personal device, email account or home number to the emergency message list, follow the directions explained at the link below.

<http://www.umaryland.edu/helpdesk/systems/umalerts/index.html>

myUM Portal Page

Users can access the myUM Portal from the following web address:

<https://myumb.umaryland.edu>. The myUM Portal is an online gateway to campus information and resources. The myUM Portal will provide you with news, activities, and campus information specific to your school. Some of the systems accessible through the myUM Portal Authentication include:

- eUM HRMS
- eUM Financials
- eUM RAVEN
- COEUS
- Effort Reporting System
- Electronic Timesheet

Users can also update their campus contact information after logging into the myUM Portal.

For FAQ's, click on the link below.

<http://www.umaryland.edu/helpdesk/systems/myumportal/index.html>

Novell Vibe

Vibe is an online collaboration tool. It offers various functionalities including secure document management and project management. Additionally, it allows users to create personal workspaces and build a team by creating team workspaces for organization and effective communication. Vibe also offers guests to interact with Vibe teams and individuals by granting guest access.

Students, Faculty, and staff can access Vibe through a web browser by navigating to <http://vibe.umaryland.edu>. myUM account holders can use their myUM username and password to log in. Training materials for Vibe can be accessed by clicking the link below.

<http://www.umaryland.edu/vibe/training.html>

eUM HRMS

eUM HRMS is the current HR, payroll, and payroll distribution system for the University of Maryland. The eUM HRMS system is accessed through the myUM Portal. For additional information, click on the link below:

http://www.umaryland.edu/helpdesk/systems/eum_hrms/index.html

eUM Financials

eUM Financials is the current financial administrative system for the University of Maryland. For additional information, click on the link below:

http://www.umaryland.edu/helpdesk/systems/eum_financials/index.html

eUM Raven

The eUM RAVEN system is used to gather financial data from the eUM Financials system. eUM RAVEN is accessed through the myUM Portal. For additional information, click on the link below:

http://www.umaryland.edu/helpdesk/systems/eum_raven/index.html

COEUS

COES is the software solution that allows the electronic creation and route grant proposals for sponsored research project grants to external sponsors. For additional information, click on the link: <http://www.umaryland.edu/helpdesk/systems/coeus/index.html>

Effort Reporting System (ERS)

The purpose of the web based Effort Reporting System (ERS) is to provide a means for the institution to distribute paperless effort forms via the web to its employees who are required to certify their effort in accordance with institutional and federal policies. For additional information and access to ERS, click on the link below.

<http://www.umaryland.edu/helpdesk/systems/ers/index.html>

EHS Training Registration System

For access to the Environmental Health & Safety (EHS) Training Registration System, click on the link: https://www.act.umaryland.edu/webprd/ehs/tms?event=LOGIN_FORM

Note: Users will need to use one of the following values: UM employee ID, UM affiliate ID, OneCard customer number, Social Security Number.

ORD Research Data Warehouse

The Research Data Warehouse captures demographic and financial information about all proposals submitted to external agencies and awards received. For more information, click on the link: http://www.ord.umaryland.edu/admin_updates_issues/mis.html

Clinical Applications

Axium

Axium is the School of Dentistry's comprehensive clinic management software. It was designed exclusively for use in dental schools and its functions include appointment scheduling, patient billing, instrument tracking, student grading, and treatment charting.

Each Axium user is assigned to a particular "User Level" (or group), and given a unique login id and password. The "rights" or "permissions" granted to a User Level determine what functions and program areas the user has access to, and which ones are off-limits. In this way, each user is given access only to those functions necessary to perform their job or role within the school. For example, as members of the "DS Student" User Level, dental students are allowed to enter and edit patient treatment, but for security reasons are restricted from entering or editing anything related to treatment fees or patient billing.

Cheat Sheets, Training Documents and PowerPoint Presentations can be accessed from within Axium by clicking "Links" on the toolbar at the top of the screen.

Dentalapps Access

Axium may be accessed off campus by using DentalApps Access.

NOTE: Axium may also be accessed through a UM SOD issued computer.

First, *ensure you have an internet connection*. To access the Dental School's Virtual Private Network (VPN) off campus, follow the steps below:

1. Go to <http://vpn.umaryland.edu>
2. Select group SOD
3. Enter your myUM ID and password
4. Accept to install a Java or ActiveX app.
5. Connected to the VPN and <http://dentalapps.umaryland.edu>

Troubleshooting DentalApps Web Access

If the "Connect" button is not highlighted, follow the directions below to add this site as a Trusted Site:

1. Ensure your browser is Internet Explorer
2. Select "**Tools**" at the top of the browser
3. Select "**Internet Options**"
4. Select "**Security**" tab Double click on "**Trusted Sites**"
5. Click the "**Sites**" button
6. Click the "**Add**" button
7. Click the "**OK**" button

Romexis

Romexis is the digital radiographic imaging software. The combination of Romexis software with Planmeca digital imaging equipment has completely replaced traditional "film" radiography. Radiographic images are stored on a centralized server and can be viewed from any clinic workstation or faculty office.

Each Romexis user is assigned to a "User Group". The User Group settings determine what functions, permissions and privileges are assigned to the user. For example, certain users, including undergraduate dental and hygiene students, are not permitted to make radiographic exposures without faculty approval. This restriction is controlled by the User Group settings.

Romexis Cheat Sheets, Training Documents and PowerPoint Presentations can be accessed from within Axium by clicking "Links" on the toolbar at the top of the screen.

Instructional Technology Applications and Equipment

Questionmark

Questionmark is the electronic system for the delivery of assessments (exams, quizzes, and surveys) to the dental and dental hygiene program. There are over twenty different question types available for use in the assessment of student performance including the provision for images and motion sequences. The assessments can be run in a secure mode, with a restricted timer, and surveys can be run anonymously. Following assessments, the faculty member receives a full set of reports to identify questions that were problematic or to assist in developing a higher level of questions enabling the control of item difficulty or discrimination.

Internet Explorer 9 and 10 are not supported by Questionmark. It is not possible to take exams on Questionmark if Internet Explorer 9 or 10 is installed on your computer. To uninstall Internet Explorer 9 or 10 on Windows 7 PCs, follow the steps below:

1. Click the **Windows Start** button, and click **Control Panel**.
2. Click on **Programs**.
3. Click on **Programs and Features**.
4. In the top left of the window, click **View Installed Updates**.
5. Wait for the green progress bar across the window title to complete.
6. Click on **Windows Internet Explorer 9** listed under the **Microsoft Windows** heading.
7. Click on the **Uninstall** button and follow the prompts to uninstall.

NOTE: The uninstall process will cause your computer to reboot twice. When it is finished, the computer will be reverted back to Internet Explorer 8, which will work properly with Questionmark.

To ensure that Internet Explorer 9 or 10 is not reinstalled again by Windows Update, follow the steps below for Windows to hide the update and not prompt for it:

1. Click the **Windows Start** button, and click **Control Panel**.
2. Click on **Windows Update**.
3. Click on the message showing some number of "**important updates**" available.
4. Find **Windows Internet Explorer 9 or 10** and **right click it**.
5. Click on **Hide Update** in the menu that appears.
6. Ensure that Internet Explorer 9 or 10 is **UNCHECKED** and **UNSELECTED**.

NOTE: Removing Internet Explorer 10 will revert the computer to Internet Explorer 9.

Blackboard

Blackboard is the courseware management system that is used for web-enhanced and web-based courses. The School of Dentistry utilizes Blackboard to house important training material, such as HIPAA training. Faculty and staff may gain access to Blackboard by completing a Blackboard request form found here

<http://www.umaryland.edu/helpdesk/systems/myummail/doc/emailregistrationform.pdf> and submitting it to CITS. To become acclimated with the system, click the link below.

<http://www.umaryland.edu/blackboard/instructors/index.html>

Blackboard Collaborate

Blackboard (Bb) Collaborate is an audio, video and web conferencing application used to deliver online instruction and meetings throughout UM. The technology is proven to make online collaboration and delivery of instruction a more exciting experience ensuring student engagement; regardless of geographical location, by featuring various types of instructional delivery including **mobile learning** as well as allowing instructors to create their own virtual classroom and office hours. Furthermore, Bb Collaborate offers **recording options**, works with the Interactive Whiteboard, as well as allows **application sharing** (users can work with word or other documents without having to install the specific program on their computers), and **screen sharing**.

Faculty and students have access to Bb Collaborate via their Blackboard courses. To learn more about Bb Collaborate, we encourage you to visit the campus tutorial site,

<http://www.umaryland.edu/cits/collaborate/training.html>.

Turning Point

TurningPoint is a student response system (SRS) used to conduct interactive polls in face-to-face or distance education classes. Students can participate in lectures by submitting responses to interactive questions using their smart phones or laptops. With Turning Technologies instructors are able to quickly gather information about students' understanding (or lack thereof) of course content. Results are transferred in real-time through data plans to response software. BlackBerry smartphone and Apple iPhone users can even download ResponseWare applications that take advantage of device functionality.

For more information about TurningPoint and to schedule one-on-one tutorial please contact Sarita Sanjoy at X 65808, ssanjoy@umaryland.edu .

Lesson Builder

Lesson Builder software enable users to create engaging lessons for the web in an efficient and effective way. Faculty can style their lesson for a professional look and/or add various tools and activities for making instruction more engaging and interactive for students. Lesson Builder runs on both Windows and Macintosh computers. Students can view lessons using any standard web browser such as Internet Explorer, Firefox and Safari.

For more information about Lesson Builder including installation and license information please contact Sarita Sanjoy at X 65808, ssanjoy@umaryland.edu

Mediasite

Mediasite is used to distribute class lectures and content. To become acclimated with the system, click the link: <http://www.umaryland.edu/helpdesk/systems/mediasite/index.html>

GoogleApps@UMaryland

GoogleApps@UMaryland is a communication and collaboration tool that allows students to share ideas quickly and get things done effectively when they have access to the same powerful communication and sharing tool. For information on how to utilize GoogleApps@UMaryland, click the link: <http://www.umaryland.edu/helpdesk/systems/googledocs/index.html>

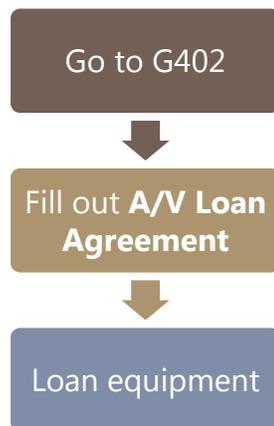
Audio/Visual Equipment Loan Request

Requests for equipment or services can be made by visiting G402, by calling (410) 706-2084, or by completing equipment requests by e-mail at equipment@dental.umaryland.edu. The following audio/visual equipment is available for loan:

- Video Conferencing
- Tele Conferencing
- Laptops
- Computer Display Adapters
- PA System – Microphone & Speaker
- Mobile Projection System
- Portable Projection Screen
- Document Camera
- Digital Voice Recorders
- Overhead/Transparency Projector
- Slide Projector

Requests should be made as far in advance as possible. Equipment is scheduled on a “First come, first served” basis and availability is not guaranteed. Faculty members may arrange to pick up and return equipment themselves. For those who need assistance in using the equipment, we ask that you contact Doug Brotherton X 61324 or dbrotherton@umaryland.edu. Please notify us, as soon as possible, if you need to cancel a submitted request.

To loan equipment, follow the easy steps below:



NOTE: Students may NOT loan equipment; a Faculty or Staff member must sponsor the loan.

To preserve the quality and ensure the security of our equipment, please follow the guidelines below:

1. The equipment must be kept in a secure location at all times when not in use. The user may be liable for replacing all equipment that is missing (regardless of whether it was lost or stolen).
2. The user is responsible for the safety of the equipment and must take steps to prevent any damage from occurring. The user may be liable for replacing equipment which was broken or damaged while in their possession and they agree to report immediately any damage that has occurred (regardless of whether or not the equipment was damaged due to accident or by a third party).
3. Upon receiving the equipment it is advised that the user inspect/operate the equipment to verify that it is in working order. If damage is found, or parts missing, they must report immediately any problems that they have encountered to avoid being liable.

Loaner Laptop Requests

OIT provides Faculty and Staff loaner laptops on two separate occasions:

1. OIT also makes loaners available to faculty and staff as needed for presentations and projects.
 - *All faculty/staff loaner requests must be made through email to equipment@umaryland.edu.*
 - The email must include the following:
 - The name of the requester
 - Who will be using the loaner (if different from the requester)
 - Purpose of the loaner(s)
 - Number of loaners required
 - Date(s) required
 - Any other information requested by OIT
 - OIT will confirm the request with the requester and advise if it is able to fulfill it. OIT is not obligated to provide a loaner at any time, and does not guarantee availability of loaners.
 - *For short-term loans (one day or less), three days' advance notice is expected. For longer-term loaners (more than one day), seven days' advance notice is expected.*

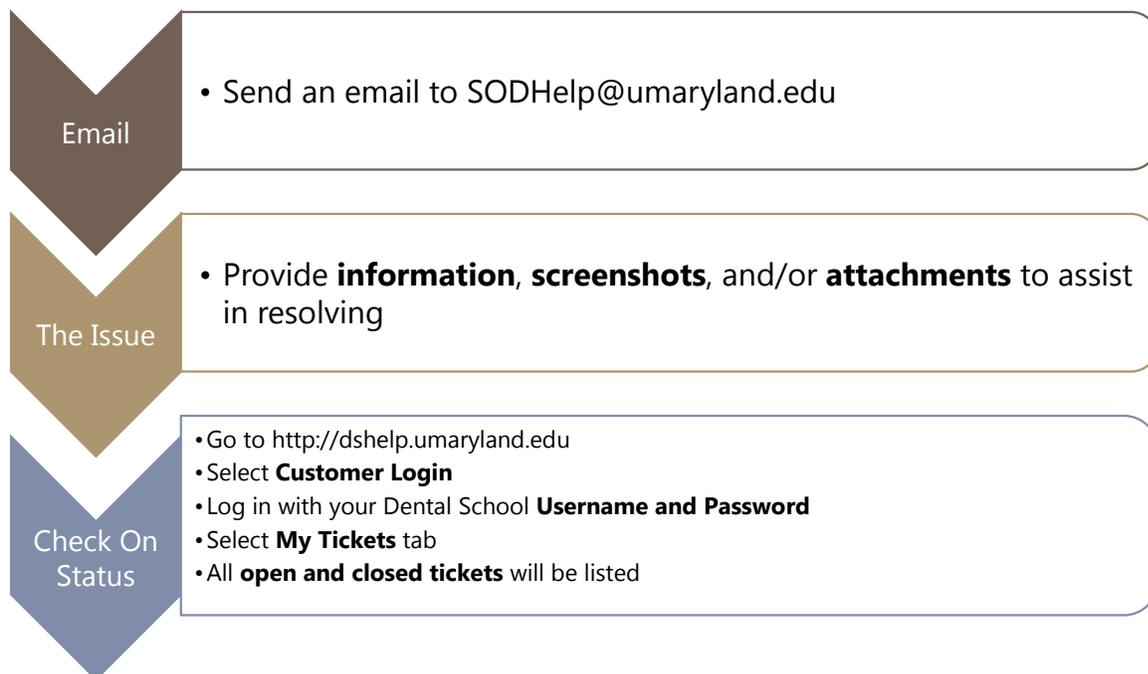
- If someone other than the requester will be using the loaner(s), the requester accepts all responsibility for the loaner(s). Students desiring a laptop reservation for faculty/staff work must have their sponsoring faculty request on their behalf.
2. OIT maintains a limited supply of UM-owned laptops to assist when repair, maintenance, and/or troubleshooting of computers. Batteries or other accessories are not available for loan.

Availability of Loaners is not guaranteed. OIT is not responsible for any data on loaners at any time. This Loaner process also applies to malfunctioning or broken AC adapters.

Troubleshooting HELP!

Get HELP!

We all get there at times. If you're stuck and need OIT HELP, submit a ticket by following the steps below.



Or you can give us a call at 410-706-2084 or email us at SODHelp@umaryland.edu.