



# 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 the faculty, staff and students at the University of Maryland School of Dentistry. This Support Guide provides links and information to better assist you. Many of these links navigate to UMB's [Center for Information Technology Services \(CITS\)](#).

Getting Started.....	3
Welcome to the School of Dentistry.....	3
UMID.....	3
Duo.....	3
UM Directory Authentication.....	3
UMB Alerts.....	3
Wireless Internet Connection.....	4
Campus Wireless Connection.....	4
Wireless Setup on Specific Devices.....	4
Email.....	4
Google@Umaryland Mail.....	4
myUMB Mail office 365/OneDrive.....	4
Encryption.....	7
Phishing Emails.....	7
Spam Quarantine.....	9
IronPort.....	9
Accellion.....	9
Printing.....	10
Campus Phone.....	11
Remote Access (VPN).....	11
Information Storage.....	12
Personal Storage.....	12
Self Service Applications.....	12

myUMB Portal Page .....	12
COEUS .....	13
Effort Reporting System (ERS).....	13
EHS Training Registration System .....	13
ORD Research Data Warehouse .....	14
Clinical Applications .....	14
Axium .....	14
Romexis.....	15
Instructional Technology Applications and Equipment .....	15
Questionmark .....	15
Blackboard .....	15
Lesson Builder .....	16
Mediasite .....	16
GoogleApps@UMaryland .....	16
Audio/Visual Equipment Loan Request .....	17
Loaner Laptop Requests.....	18
Troubleshooting HELP! .....	19
Get HELP! .....	19

## Getting Started

### Welcome to the School of Dentistry

The Office of Information Technology (OIT) is your information technology resource at the School of Dentistry. We strive to provide you with high-quality service and support. This Support Guide answers many common IT-related questions and provides links and instructions for relevant information. To resolve any issues you are experiencing, please consult this guide first. If you are unable to resolve your issue, see [Troubleshooting HELP!](#) to create a support request with OIT.

In this section, you'll find essential services for getting started at the School of Dentistry.

### UMID

Your UMID and password are 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 campus email.

For instructions on how to create a UMID and password, visit:

<https://www.umaryland.edu/helpdesk/umb-account/creating-a-umid-and-password/>

### Duo

Duo is the University of Maryland's solution for multi-factor authentication. Duo uses your smart phone to provide another layer of security when logging into some services while at home or outside of the UMB computer network. Instructions for enrolling in Duo and installing the mobile application may be found here:

<https://www.umaryland.edu/cits/services/duo/enrollment/>

For frequently asked questions about Duo, visit:

<http://www.umaryland.edu/cits/services/duo/faq/>

### UM Directory Authentication

The UMID system 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 FAQs. <https://www.umaryland.edu/cits/services/umid-login-reference/>

### UMB Alerts

UMB Alerts is the system used by the **Emergency Management Team** to send text messages about campus emergencies. The system is also used to announce campus closings or delayed openings. You can register personal devices, such as cell phones or tablets 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 here: <http://www.umaryland.edu/alerts/access-umb-alerts/>

## Wireless Internet Connection

### Campus Wireless Connection

The School of Dentistry, in conjunction with the campus (CITS), maintains Eduroam, the secure, world-wide roaming access service developed for the international research and education community. Eduroam is a wireless network that allows students, faculty and staff from participating institutions to connect to the Internet on campus and at other participating institutions using their local login credentials (UMID). 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 Eduroam. For specific directions, please visit:

<http://www.umaryland.edu/cits/services/eduroam>

## Email

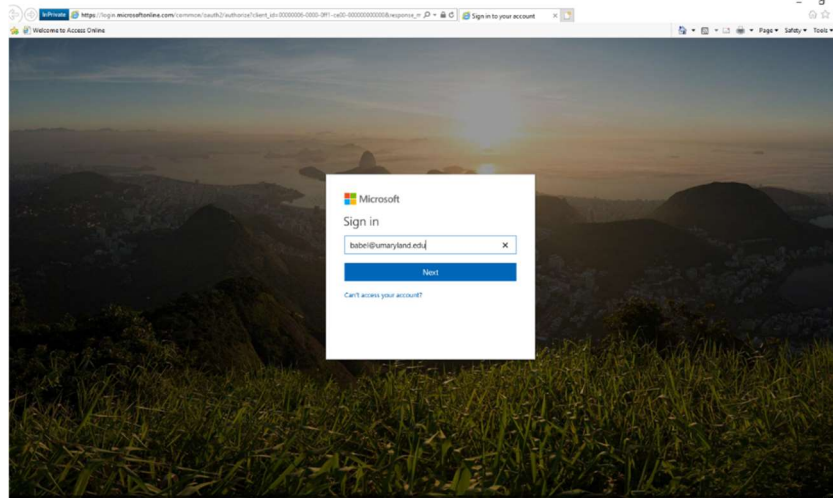
### Google@Umaryland Mail

GoogleApps@UMaryland (or Google Apps for Education (GAE)) is a communication and collaboration tool for students and residents. Students share ideas quickly and get things done more 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 is no hardware or software to install. Everything is delivered through a standard web browser. For more information about GoogleApps@UMaryland, visit: <https://www.umaryland.edu/cits/services/googleappsumaryland/>

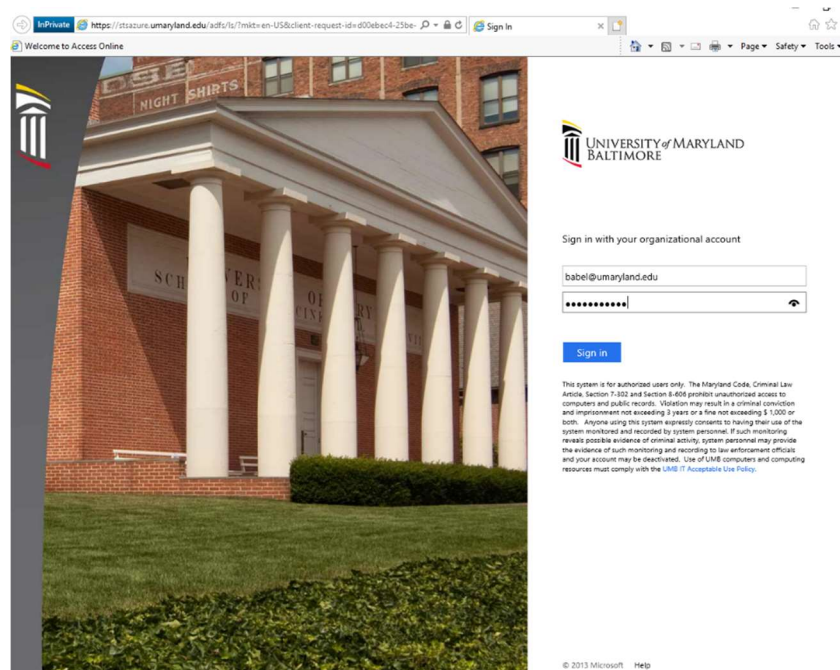
### myUMB Mail Office 365/OneDrive

UMSOD provides Microsoft Exchange email and calendar for faculty, staff, affiliates and students. Microsoft exchange may be accessed with the Outlook app on any school PC, or offsite using a web browser on Windows or MacOS.

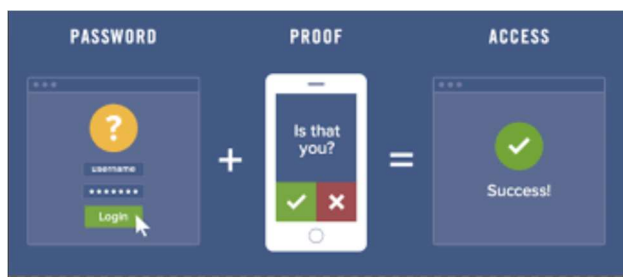
UMSOD also provides access to Microsoft Office 365, which includes the complete Microsoft Office Suite, OneDrive and Sharepoint. Users can access Office 365 by visiting <portal.office365.com>.



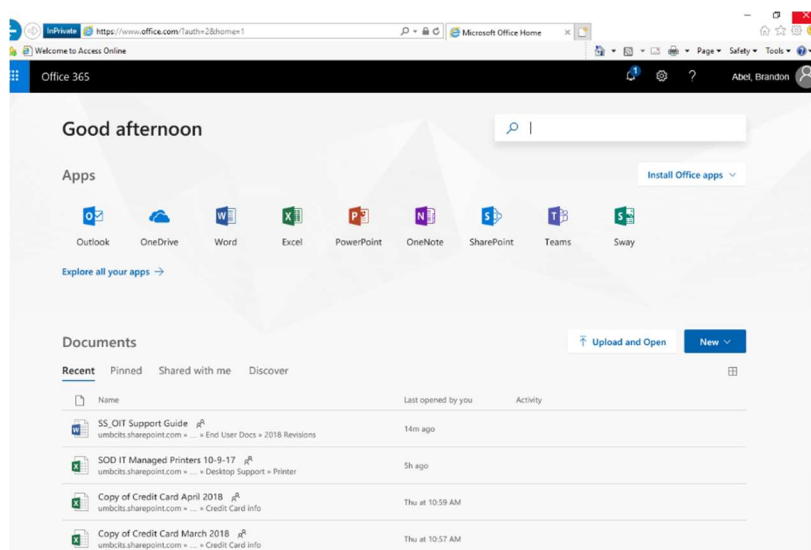
Enter your UMSOD email address (typically your UMID followed by '@umaryland.edu'). You will then be prompted for your password.



After clicking the Sign In button, you will receive a DUO notification on your mobile device which must be approved before continuing.



You will then be directed to the Office 365 home page, containing the entire Microsoft Office suite as well as OneDrive and SharePoint.



OneDrive allows you to access your files from any web browser or mobile device. OneDrive replaces network shared/personal drives, which are normally 20 gigabytes, with 1terabyte of storage space.

To access email on your mobile device, visit the App/Play Store and download two apps: Outlook and Duo Mobile. Once installed, you will be prompted to enter your UMSOD email address and password. After entering credentials, you will receive a confirmation message from Duo. Once you verify this confirmation, Outlook will begin to load emails. This process may take a few minutes to complete, depending upon the number of emails.

For additional information on the Outlook Web App and email, visit:

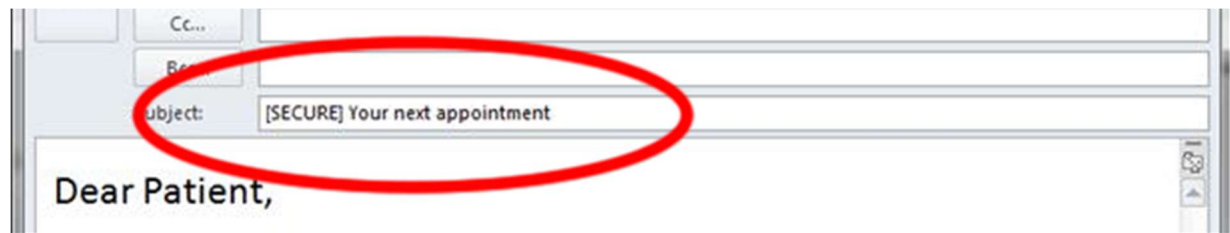
<https://www.umaryland.edu/cits/services/campus-exchange-email-system/outlook-web-app/>

## Encryption

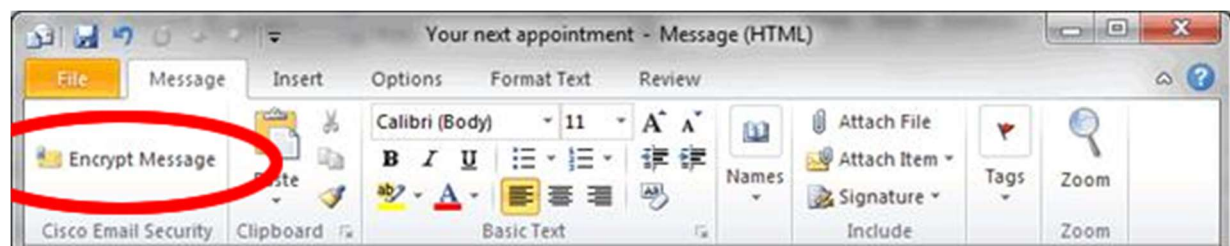
All electronic communication must be from a School of Dentistry issued email account. The secure messaging system must be used for all email communications with or about patients, from any and all School of Dentistry employees, students or affiliates.

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><b>If you ....</b></i>	<i><b>Then you need to...</b></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 <a href="mailto:sodhelp@umaryland.edu">sodhelp@umaryland.edu</a> . Do not respond to the message itself.

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

1. **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. **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>

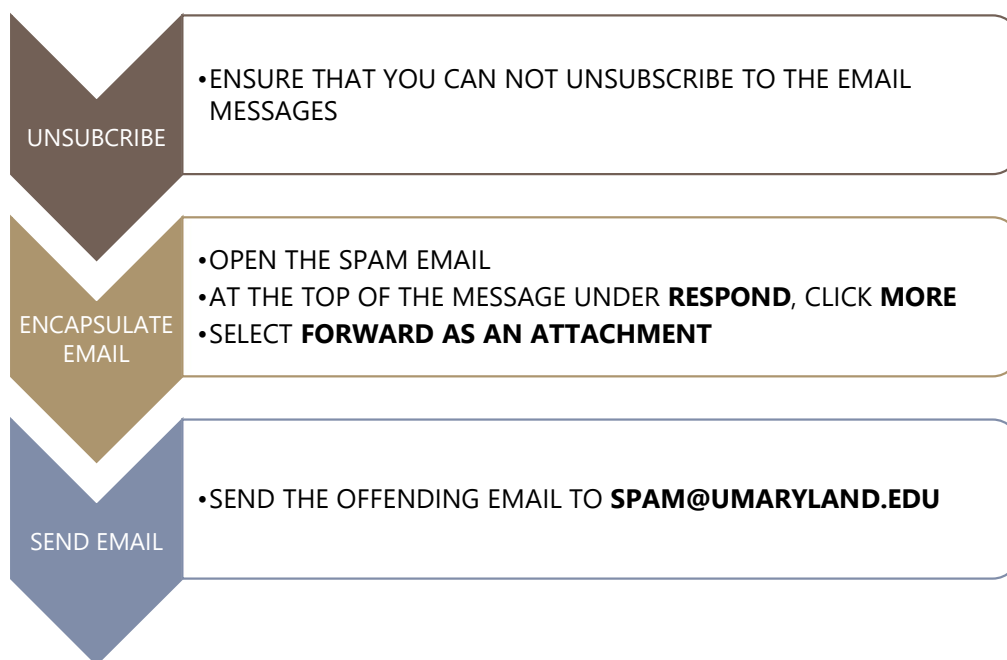
DO NOT resolve a username and password issue in another forum. DO NOT give your username and password to another website.

For 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 CANNOT 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, visit:

<https://www.umaryland.edu/cits/services/ironport/>

## 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 UMID. Check

<http://www.umaryland.edu/cits/services/accellion/> 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 from any printer simply by swiping their UMOne Card. PaperCut is available for all users except those on the clinic floor printing from Axium (this is a direct printing process that does not need the UMOne Card to be swiped).

To get started, first enroll in the PaperCut system by following the instructions here:

<http://sodhelp.umaryland.edu/papercutjobaid.pdf>

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. For more information, watch a short video presentation on Mediasite:

<https://mediasite.umaryland.edu/Mediasite/Play/0861c0b72fc740408f14b65ee48f58e01d>

If no printer is listed for your area, please contact the Help Desk ([sodhelp@umaryland.edu](mailto: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/it](http://www.dental.umaryland.edu/it) by selecting **Purchasing Requests**.

## Campus Phone

The School of Dentistry uses campus-provided Cisco VoIP (Voice over IP) handsets. For more information about how to use this handset and the campus voicemail system by visiting:

<https://www.umaryland.edu/cits/services/campus-telephone-service/> and see the Quick Links 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, visit: <https://www.umaryland.edu/cits/forms/unified-messaging-request-form/>

## 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 UMID credentials for signing on.

To install a VPN client, please visit one of the following links and follow the instructions:

- Windows: <https://www.umaryland.edu/media/umb/cits/vpn/Palo-GlobalProtect-VPN-Windows-Installation.pdf>
- MacOS: <https://www.dental.umaryland.edu/media/sod/information-technology/PaloGlobalProtect-VPN-Mac-Installation.pdf>

For additional information, please visit the CITS VPN page: <https://www.umaryland.edu/cits/service-catalog/vpn/>

### What you need before connecting

1. Only connect to the VPN using a system with an Operating System still supported by the vendor.
2. Ensure your system is patched and is running a current and updated anti-virus software.
3. Know your UMID and password.
4. Get your VPN group name from your supervisor.
5. Log in to <https://cf.umaryland.edu/vpn> and select the link **Completing VPN Group access request for myself**
  - a. Check the box next to **Member**
  - b. Select the **VPN Group Name** provided by your supervisor.
  - c. Click **Submit**
6. **(You will only need to perform this step with your first connection on a device that doesn't already have the Palo Alto GlobalProtect VPN Client!)**
  - a. Open your browser and go to <https://umbvpn.umaryland.edu>
  - b. Enter your UMID and Password and click **Login**

- c. Download and install the Palo Alto GlobalProtect VPN client for your operating system.

**Other requirements:**

- An active internet connection.
- Ability to install the software on the workstation – Local Admin rights required for installation.
- A valid UMID account name and password for authentication.
  - If you need assistance with your UMID account, email the [IT Help Desk](#) or 6-HELP.

## 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. If the local drive fails, the data is lost. 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

### myUMB Portal Page

Users can access the myUMB Portal at <http://myumb.umaryland.edu/>. The myUMB Portal is an online gateway to campus information and resources. The portal provides you with news, activities, and campus information specific to your school. Some of the systems accessible through the myUMB 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 myUMB Portal.

For Frequently Asked Questions, visit:

<https://www.umaryland.edu/cits/services/myum-portal/>

### ***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 myUMB Portal. For additional information, visit:

<https://www.umaryland.edu/eumb/training/eumb-hrms---payroll-training/>

### ***eUM Financials***

eUM Financials is the current financial administrative system for the University of Maryland. For additional information, visit:

<https://www.umaryland.edu/eumb/training/eumb-financials-training/>

### ***eUM Raven***

The eUM RAVEN system is used to gather financial data from the eUM Financials system. eUM RAVEN is accessed through the myUMB Portal. For additional information, visit:

<https://www.umaryland.edu/kualicoeus/raven-reports/>

### **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, visit:

<https://www.umaryland.edu/kualicoeus/>

### **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, visit:

<https://www.umaryland.edu/cost/effort-reporting/>

### **EHS Training Registration System**

For access to the Environmental Health & Safety (EHS) Training Registration System, visit:

<https://afcf.umaryland.edu/ehs/sec/myehs/>

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, visit:

<http://www.umaryland.edu/ord/>

## Clinical Applications

### Axium

Axium is the School of Dentistry's comprehensive clinic management software. It was designed exclusively for use in dental schools. 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 can access. 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 UMID 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 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 Axiom 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.

### **Blackboard**

Blackboard is the learning management system that is used for web-enhanced and web-based courses for all the educational programs such as DDS, DH, Ph.D, and Post graduate. In addition, the School of Dentistry utilizes Blackboard to house important training material for mandatory clinical training, such as HIPAA, OSHA, and Bloodborne.

### *Blackboard Collaborate*



Blackboard (Bb) Collaborate is an online learning solution. It provides various types of instructional delivery, including mobile learning, virtual classrooms, and online office hours. Bb Collaborate also offers recording options, interactive whiteboarding, application sharing, and screen sharing.

Faculty and students have access to Bb Collaborate through their Blackboard courses. To learn more about Bb Collaborate, visit:

<http://www.umaryland.edu/blackboard/collaborate/>

### Lesson Builder

Lesson Builder enables users to create interactive and engaging lessons for the web efficiently and effectively. 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 Chrome, Internet Explorer, Firefox, and Safari. The lessons are SCORM compliant, can be embedded in Blackboard courses.

For more information about Lesson Builder including installation and license information please contact Sarita Sanjoy at X 65808, by email at [ssanjoy@umaryland.edu](mailto:ssanjoy@umaryland.edu).

### Mediasite

Sonic Foundry's Mediasite Video Platform is the industry leader for lecture capture and online training. Lectures are captured, live streamed and archived to provide playback on demand on a variety of platforms.



### 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/cits/services/googleappsumaryland/>

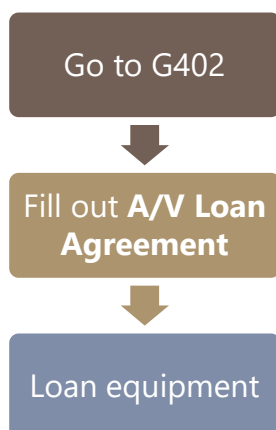
### Audio/Visual Equipment Loan Request

Requests for equipment or services can be made by visiting G402, by calling (410) 706-2084, or by completing equipment requests by email at [equipment@umaryland.edu](mailto:equipment@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](mailto:dbrotherton@umaryland.edu). Please notify us, as soon as possible, if you need to cancel a submitted request.

To loan equipment, follow the 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 that 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:

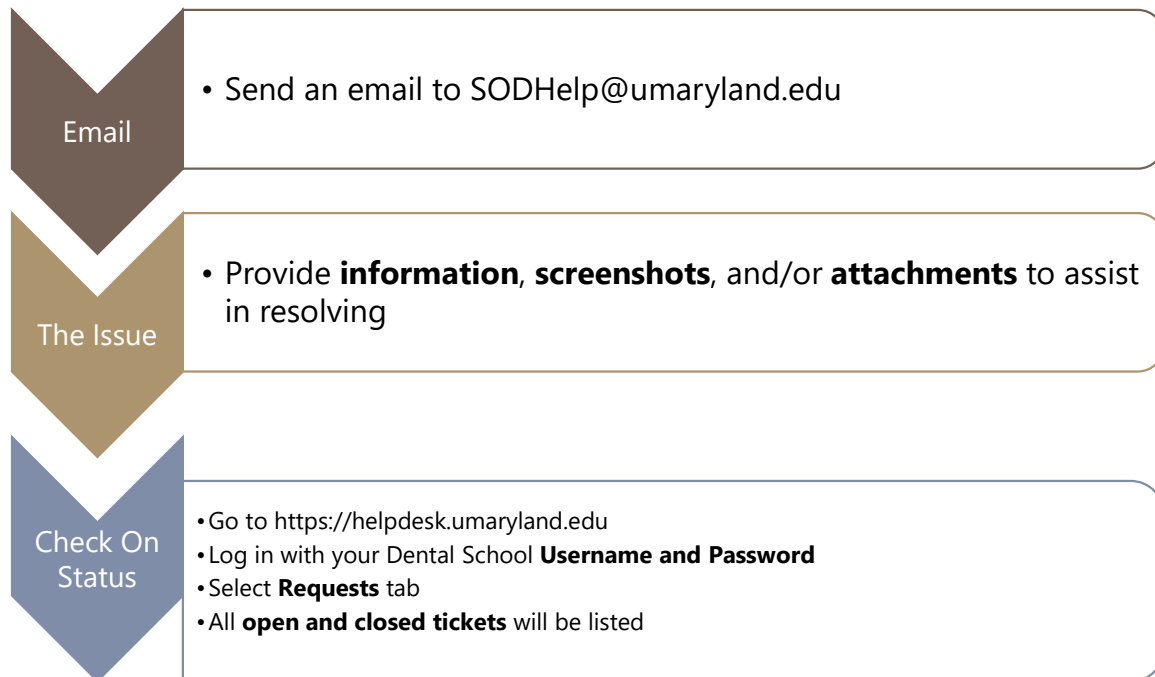
1. OIT also makes loaners available to faculty and staff as needed for presentations and projects.
  - **All faculty/staff loaner requests must be made through email to [equipment@umaryland.edu](mailto:equipment@umaryland.edu).**
  - The email must include the following:
    - The name of the requester
    - 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

If you're stuck and need OIT help, submit a ticket by following the steps below:



Or give us a call at 410-706-2084 or email us at [SODHelp@umaryland.edu](mailto:SODHelp@umaryland.edu).