

Technology Handbook

Providing Technology-Related Information for Staff,
Faculty, and Instructors of the College of Arts and
Sciences

March 30, 2012

Table of Contents

Introduction	4
University Technology Divisions.....	5
1.0 Policies and Procedures.....	6
1.1 Request for Computer Labs.....	6
1.2 Request for Equipment.....	7
1.3 Request for Rooms	8
1.4 Special Events	9
1.5 Teaching in Rooms/Buildings with Swipe Cards	10
1.6 Wireless Account	11
1.7 Guest Wireless Account	12
1.8 A&S-Owned Computers	13
1.9 Computer Replacements.....	14
1.10 A&S-Owned iPads.....	15
1.11 Information Storage.....	16
2.0 Personnel Action	19
2.1 New Hires	19
2.2 Faculty	20
2.3 FTTIs and PTTIs	21
2.4 Checklist for New Hires	22
2.5 Exiting Employees	23
2.6 Checklist for Exiting Employees	25
3.0 Instructional Technology.....	26
4.0 Additional Information	27
4.1 Share and Home Drives	27
4.2 Virtual Private Network (VPN)	28
5.0 Useful Links	29
6.0 Contacts	30

7.0 Appendix 32
7.1 Appendix A - Zero PA..... 32
7.2 Appendix B – Guest Wireless Policy 33
7.3 Appendix C – Information Storage, College of Arts and Sciences .. 35

Introduction

The College of Arts and Sciences recognizes that faculty and staff need to be provided with a proper work environment so that they can be productive and successful in their positions. One of the main objectives of the College is to be a leader in new pedagogies with respect to technology. For this reason, the Dean of Arts and Sciences established the Office of Educational Technology in 2006 as a service organization for the College. The Office of Educational Technology, or eTech, serves several functions within the College of Arts and Sciences:

- It provides incoming faculty and staff with office computer equipment, and lends assistance to those who have questions about or experience problems with these devices.
- It serves as a centralized source of knowledge for faculty and staff who need technology information or desire technological assistance. eTech also supports faculty and instructors who wish to incorporate technology in their classes and research.
- It assists A&S departments with website creation and maintenance.
- It provides a means for the College to communicate with faculty, staff, alumni, and students through the website and social media.
- It maintains computer labs for faculty who want to use them for teaching and students who use them throughout their academic career at UA.
- Most recently, eTech has helped implement the Dean's iPad initiative by providing logistical, instructional, and tech support for these devices.

This handbook provides A&S departments with a centralized source of information for College technology resources and policies. With all of the technology distributed throughout the College, it is necessary for each department to be aware of these policies and to work with eTech to uphold them. Any questions or concerns should be directed to the eTech main office at 348-4832 or eTech@as.ua.edu.

We at the Office of Educational Technology are here to serve all faculty and staff of the College of Arts and Sciences. Please feel free to contact us with any questions. We are here to help!

University Technology Divisions

The technology divisions within the University have undergone changes recently to accommodate the constant growth of the faculty and staff. The current departments (as of January 2012) are outlined below and a list of contacts is included in Section 6.0.

Office of Informational Technology (OIT)

OIT is the main source of technology support for the University of Alabama. They are responsible for setting up and maintaining faculty and staff office computers and department computer labs, they maintain the University network system, they obtain licenses for most of the software available to faculty and staff (<http://oit.ua.edu/oit/services/software-licensing/>), and they are in charge of technical support through their IT Service Desk (348-5555 or itsd@ua.edu). This department is also in charge of all University email systems and network security.

Center for Instructional Technology (CIT)

CIT can be subdivided into three main categories: Audio/Visual Systems (AVS), Faculty Resource Center (FRC), and Multimedia Services.

AVS is responsible for maintaining and supporting all multimedia equipment and for imaging all non A&S-controlled multimedia rooms. When faculty experience problems with multimedia computers, they can contact AVS by using the phones that are located next to the podiums or by calling 348-6011.

The FRC provides the faculty with regular informational sessions throughout the year on the various teaching technologies available at UA, including Tegrity, eLearning, Blackboard Learn, and clickers. Faculty can also contact the FRC for one-on-one assistance with these technologies or when having technical difficulties. To contact the FRC, call 348-3532 or email them at elarning@ua.edu.

Multimedia Services offers videography capabilities. When department have guest speakers and/or events that they would like professionally recorded, they can contact Rebecca Johnson in eTech (348-4832; rljohnson@as.ua.edu) to request these services.

1.0 Policies and Procedures

1.1 Request for Computer Labs

The College of Arts and Sciences owns and maintains (through eTech) seven computer labs, five of which can be reserved for teaching purposes. Faculty and instructors who have classes that will require extensive use of computers by the students can reserve computer labs for use during normal operating hours (go to <http://as.ua.edu/labs> for lab hours). Reservations must be requested in advance, are granted based on the availability of the rooms, and depend on the needs of the faculty. When making a reservation request for a computer lab, the following points should be kept in mind:

- Faculty who would like to block computer labs for particular courses should submit their requests at least two months prior to the semester in which they are requested.
- Single-date or short-term requests for lab use should be made at least 10 business days in advance. Requests made closer to the desired date may not be able to be granted, based on availability.
- Faculty will not be able to book rooms that have already been reserved.
- Gordon Palmer 152 and Morgan 238 are open computer labs and cannot be reserved without approval from the Dean.
- Although one may make a request for a specific room, actual room assignments will be made based on availability and in accordance with priorities set by the Dean's Office.
- A confirmation email will be sent to the requestor once the request has been granted and a lab assignment has been made.

Computer lab reservations may be requested by going to the eTech website at <http://as.ua.edu/labs> and entering the required information. Please note that completing the form submits a request only. Faculty will receive confirmation from eTech when the rooms are actually reserved.

1.2 Request for Equipment

Faculty, instructors, and staff who need to borrow equipment, such as laptops, projectors, and iPads, for a limited time may do so through eTech's Equipment Loaner program. The standard duration of an equipment loan is two weeks. A few items, such as room projectors, may be checked out for a semester, based on need and availability.

When making a request for loaner equipment, the following should be kept in mind:

- Equipment is loaned out on a first-come, first-served basis and is based on availability, need, and desired duration of loan.
- The duration of the standard loan time (two weeks) may be extended in some cases. However, requests for an extension must be made before the due date and are granted based on availability.
- Faculty and staff who borrow equipment must return all items on or before the due date.
- When returning items, faculty and staff must return all pieces checked out to them. This includes carrying case, all cords, and accessories. Faculty and staff will be charged for any checked-out items that are not returned.
- Equipment that is damaged while checked out must be reported immediately. eTech will assess the damage and take appropriate action. Faculty and staff will be charged the cost for fixing and/or replacing damaged items, as indicated on the check-out form.
- Faculty and staff who fail to return loaned equipment by the due date or damage equipment may be banned from the Equipment Loaner program.
- Faculty and staff can designate someone to pick up the equipment on their behalf. However, the request must still be made under the name of the person loaning the equipment, and that person should be aware that he/she is still responsible for the equipment, even when it is in the possession of their designee.

In order to request equipment, faculty, instructors, and staff should go to the eTech website page at <http://as.ua.edu/etech/equipment/>. Please note that submitting a request does not guarantee an equipment reservation. If a request is approved, then someone from the eTech office will contact the individual to let him or her know when they can pick up the requested equipment.

1.3 Request for Rooms

This section deals with room reservations for events only (i.e. club meetings, workshops, guest speakers, etc.). Each department is responsible for scheduling space for semester courses using the University of Alabama ASTRA system. For more information on how the scheduling process works, feel free to contact your department chair or department main office, or view the UA Registrar tutorial at http://registrar.ua.edu/doc/Scheduling_A_Class.pdf.

When faculty, instructors, or staff want to make event reservations for rooms that are not controlled by their department or for events that include non-UA organizations, they need to make these requests through eTech. When requesting rooms, the following should be kept in mind:

- Room reservations are granted based on availability and on a first-come, first-served basis.
- Equipment, chairs, and tables must be put back exactly as they were arranged when the group arrived.
- If white boards are used, they should be wiped at the close of the meeting.
- Equipment used during the meetings should be turned off at the end of the session.
- Doors to the rooms should be locked after the meeting – especially if the meeting takes place after hours.
- For security reasons, eTech cannot check out keys to individuals. Instead, eTech will arrange for someone to unlock and lock the doors before and after the meeting takes place. Therefore, it is important to make reservations for events that occur after normal business hours or during weekends at least two (2) weeks in advance so that appropriate arrangements can be made.
- It is important for these meetings to begin and end at the prearranged times. If the designated group does not arrive at the room within 30 minutes of the stated reservation time, the room will be relocked and the eTech person will leave the location.
- The individual or group reserving the room is responsible for the room while it is in their possession. Those responsible will be charged for the cost of repairing any damages that may occur during this time.
- Individuals and/or groups that do not follow the room reservation policy risk being denied future use of A&S-controlled rooms.

In order to request use of an A&S-controlled room for an event such as the ones described above, faculty, instructors, and staff should go to the eTech website page at <http://as.ua.edu/etech/reservations>. Please note that submitting a request does not guarantee a room reservation. If a request is approved, then someone from the eTech office will contact the individual to let him or her know.

1.4 Special Events

Departments that have arranged for guest speakers at special events may want to consider making a recording that can be accessed at a later date. For presentations that are primarily PowerPoint-based, a Tegrity recording posted to iTunesU, a department website, or eLearning may be the best method for capturing the event. For speakers that are well-known in their profession and presentations where video of the speaker is desired, departments should contact Rebecca Johnson in eTech at rljohnson@as.ua.edu, or 348-4832. Requests for videographers must be made at least two weeks in advance and are based on availability. The College of Arts and Sciences has also provided each department with a hand-held digital video camera for recording day-to-day classroom events and teaching observations or evaluations. Faculty should contact their department chair or main office to inquire about this option.

Please note that if you are interested in recording or videotaping a guest speaker, you must get their permission first. Speakers who agree to be recorded through Tegrity or video need to sign a release form, which can be obtained through the iTunesU website at itunes.ua.edu under the Contribute Content section. The department will also need to submit additional information on a "metadata" form, which is also found on the iTunesU website in the Contribute Content section. For more information about iTunesU, contact Rebecca Johnson at rljohnson@as.ua.edu, or 348-4832.

1.5 Teaching in Rooms/Buildings with Swipe Cards

In order to provide better security, the University of Alabama has been installing electronic keyless entry systems for buildings and classrooms. This system allows the Security department to automatically unlock and lock all doors at set times during the day. They also provide access for faculty who need to gain entry to the buildings and rooms outside the normal operating hours by swiping their action cards across the activation plates. All new and renovated buildings are being installed with this mechanism and the outside doors of numerous older buildings have been retrofitted with these mechanisms. Ten Hoor was the first older A&S building to have this keyless entry system installed, but it is anticipated that all buildings on campus will use this electronic entry system within the next few years.

Before the start of each semester, departments will be required to send eTech a list of faculty, instructors, and GTAs who will need access to ten Hoor. eTech will send this information to the Security department so that the individuals are able to access the appropriate classrooms at the start of the semester.

For non-A&S controlled classrooms with swipe cards, departments will need to contact the appropriate college to which the classroom belongs in order to request access. For swipe card access to rooms in buildings owned by the Provost, departments need to contact the Building Administrator for the Office of Research at 348-6818. This includes access to Shelby, SEC, and Lloyd.

1.6 Wireless Account

The Office of Informational Technology (OIT) requires that all University students and employees register for the wireless system every academic year. When staff, faculty, and students try to access the internet for the first time using a wireless device, they will be prompted for a login and password. This will be the same login as the person's bama identification and password. If the employees or students have any questions about this process, they can contact the OIT service desk at 348-5555.

1.7 Guest Wireless Account

The Office of Informational Technology (OIT) provides the College of Arts and Sciences with a guest wireless registration every academic year. The purpose of this account is to allow guest speakers and professional visitors to the College to use the University wireless for the duration of their stay. eTech will send notices out to department chairs each year, supplying them with the guest account ID and password effective for that year, along with a list of UA terms and conditions. It is the responsibility of each department chair to understand the terms with which this account should be used and to provide the information to the appropriate individuals. For a copy of the current terms and conditions, and how to access login and password, please see Appendix B on page 22.

1.8 A&S-Owned Computers

The College of Arts and Sciences provides each faculty and staff member with an A&S-owned office computer (with regular replacement) and iPad to be used for the duration of his/her employment. Because of the new Technology Inventory system in place, it is necessary that eTech be knowledgeable of the location and condition of the equipment. If faculty or staff move from one office to another, they or their department must notify the eTech main office. The eTech staff will then make arrangements with the individual to go to the offices and ensure that the technology is properly disconnected and reconnected. The eTech staff will then notate the change in location on the technology database. With the exception of laptops and iPads, faculty should not remove their computers from UA property without permission from the Dean's Office. Also, faculty and staff are not allowed to swap computers. If a department would like for a used faculty computer to be transferred for another use, after a replacement has been given, the department must notify eTech so that the computer can be wiped clean of any sensitive faculty or FERPA information before reinstallation.

If laptops are damaged, the faculty and staff to whom these computers are assigned are responsible for the repairs and associated costs.

1.9 Computer Replacements

In July 2011, eTech launched a Technology Inventory Initiative across the College. The purpose of this initiative is to provide eTech with a comprehensive view of all A&S-owned computers, which will enable eTech to create an automated system for notifying individual faculty and staff when they are eligible for a new computer. This automated system will relieve faculty, staff, and departments of the burden of tracking the age of their computers and will ensure that no equipment posing a risk to the UA network is in use.

When faculty and staff are identified by the system as eligible for new computers, they will receive an email that provides them with a link and an activation code. This information will allow them to log into the automated system and request what type of equipment they prefer (i.e., Mac or Dell). For faculty who require computer equipment that is outside the standard models offered by the College, they will be given the option to request custom computer configurations. In these cases, the College will provide a set amount of money toward the equipment and the faculty or their departments will be responsible for providing the balance. Department approval must be provided for custom computer requests. When the new computer is installed, A&S will retrieve the current computer to be used elsewhere in the College.

All instructors and GTAs are supplied with refurbished computers that will be updated as needed, based on availability. Departments should notify the eTech main office no later than July 31st for refurbished computer requests for the following academic year. This will provide enough time for eTech and OIT to image and install the computers during the Fall semester. Refurbished computer requests that occur later than July 31st must come through the department chair. eTech will determine the needs and priority for the department.

1.10 A&S-Owned iPads

In order to promote academic continuity and communication in the event of an emergency and to enhance both the teaching and research experience in the College, the Dean has issued iPads to all faculty and FTTIs. As with office computers, these iPads are A&S-owned and should be treated as such. When issued an iPad, employees should keep the following in mind:

- For security reasons, all faculty, instructors and staff must activate the Find My iPad feature within iCloud and create a passcode for their iPad. Faculty and staff who do not do this and have an iPad stolen will not be issued a new one.
- eTech has an iPad blog, linked to our website, that addresses issues, helpful tips, instructions, and stories shared by faculty mentors. Faculty and instructors are encouraged to visit the site regularly (<http://as.ua.edu/ipad>) to gather new ideas on how to use their iPads in teaching and research.
- If College employees experience any problems with their iPads, they can contact eTech to get help from an experienced technician.
- iPads are purchased with Wi-Fi and 3G capability. Employees who need assistance with setting up their Wi-Fi access can contact the eTech office. Employees who wish to use the 3G will need to set up an account with the appropriate provider and will be responsible for paying the monthly fee.
- When faculty or instructors leave the College, they must return the iPad to their department main office, which will contact eTech for retrieval.
- iPads that are lost or stolen must be reported immediately to UAPD and eTech, and to the local police department if the theft occurs out of town. These departments will work with the individual to attempt to recover the device or remotely wipe critical information from the device if it cannot be recovered.

1.11 Information Storage

With the increasing demand for and interest from faculty to report student and the requirement to submit course information electronically, it is important that this information be stored and transferred using secure methods. The College of Arts and Sciences' Office of Educational Technology has worked with the Office of Information Technology to establish some guidelines that departments can use to make sure that their information is as safe as possible and that no one inadvertently violates any Family Educational Rights and Privacy Act (FERPA) regulations.

The following includes a list of dos and don't that all faculty should keep in mind when storing and transferring student information. Please be aware that failure to abide by these guidelines could result in legal ramifications for the individual and/or the department. For the original memo, see Appendix C (Section 7.3).

Dos

Store all student information on the University network drives. This includes the share drive and faculty home drives, all of which are contained within the University firewall.

Use the University of Alabama Virtual Private Network (VPN) whenever attempting to access share drives from off-campus. Additional information on when to use the VPN can be found under the FAQs section at the end of this memo. For those who need help accessing the VPN, contact the IT Service Desk at 348-5555.

Faculty and staff should send all correspondence with students and about students through UA email accounts only. Please keep in mind that while non-UA email servers may advertise that they are secure, these providers glean information from your emails for research purposes. Therefore, outside email sources should never be used for sending any student information such as CWIDs or grades.

Faculty are allowed to keep gradebooks (hard copies and electronic) in locations off the network drives, with the assumption that appropriate precautions are taken to make sure that the information is not easily accessible or viewable by other people. When faculty are using external sources (laptops, home computers, physical grade books, iPads, etc.) to record student grades, they should take care to disclose as little information as possible on these records. Student names are acceptable, while last name only (or last name with first initial) would create a higher level of security. Faculty should never record student names with CWIDs in their grade books.

Don'ts

Do not save any CWIDs to unprotected devices, such as a non-compliant server, flash drive, unencrypted laptop, disks, external hard drive, or an unsecured online system such as Dropbox, Evernote, or GoogleDocs. If you are unsure whether the device or system is secure, contact eTech at etech@as.ua.edu or just don't use it.

Never store social security numbers for students, staff, or faculty on any personal devices, external storage devices, or office computers. *There is no reason that departments should ever need or use social security numbers for work or any other purpose.* If departments are using forms that ask for social security numbers, they should remove this category immediately. If the form is from an outside source, the department should instruct the individuals filling out the forms to write "declined" in that section. (If the form is from an outside source within UA, please contact eTech so the staff and OIT security can investigate the matter.) When departments receive documents that contain social security numbers, they should obliterate the numbers with black markers on hard copies and delete the numbers on electronic copies.

Don't collect or store sensitive student information on unsecured electronic devices (this does not include grade books). Sensitive information includes student names when they are combined with CWIDs, birthdates, mothers' maiden names, social security numbers, grades, medical records/data, or entrance exam scores. If any faculty or staff members are collecting this type of information, it should be stored on the share drive or a University-encrypted laptop. Anyone who is storing this information on unsecured external electronic devices should transfer it to the share drive and immediately delete it from the external source. Any hard copy materials with sensitive student information should be shredded.

No A&S department should be using unapproved off network servers to store student information, department emails, share drive folders, etc. Any existing share drives in departments must be cleared through the College of Arts and Sciences and undergo review from OIT security to determine whether they can be used. See following page for more information on servers.

FAQs

What is a server?

A server can be ANY computer regardless of size or location that accepts external connects for services such as Web Sites, FTP, SSH, or any other file sharing services through databases or other software that is made available to external users.

What to do with old grad applications containing social security numbers?

Although the Graduate Office has now discontinued the practice of collecting social security numbers for graduate student applications, many departments are wondering what to do with the information already collected. For those departments who have retention policies for these applications, make sure that the paperwork is always stored in a secure location. When the retention period has expired, hard copies of documents containing these numbers should be shredded. Departments should not be collecting SS numbers as part of an electronic database. If any grad student databases currently contain social security numbers, delete this column immediately. Grad application information is considered sensitive and should be stored on the network drives.

What constitutes FERPA information?

For a complete description of FERPA information, please see the Registrar's website at <http://registrar.ua.edu/academics/privacy-guidelines/ferpa-fact-sheet/>. However, here are some highlights that are pertinent to faculty:

In Order To Avoid FERPA Violations, Faculty Should Not:

- Use the SSN/Student ID/Student Names to post grades.
- Leave graded tests [electronically or in print] for students to sort through.
- Circulate electronically or in print, class list with the Student Name and SSN/Student ID.
- Provide anyone with student schedules.
- Provide anyone with lists of students enrolled in your classes.
- Include confidential information (i.e., grades, #of credits) in a commendation letter without the written consent of the student [Note: If a student provides you a resume with the information, you may disclose whatever is in the resume.]

Faculty or staff with any questions about electronic security issues can contact Ruth Pionke at eTech, OIT, or they can go online to <http://oit.ua.edu/oit/security/>.

2.0 Personnel Action

2.1 New Hires

As soon as departments are aware of new hires (faculty, instructors, and staff) in their area, a number of actions must take place before the new employees start work. A checklist has been provided in Section 2.4. Please note that the chronological order of some of these steps is important for executing a smooth transition.

After an official offer is accepted by the new hire and before any other services can be requested, a member of the department office staff must obtain a CWID for the individual, which is done by creating a Zero PA. (See Appendix A) The CWID will be required to set up any technology-related systems for the new hire as well as many other services around the University.

Once a CWID is established, the office administrator can request an email account and share and home drive space for the new hire. (For more information on drives, see section 5.1) This is done by going to the eTech website at <http://as.ua.edu/etech/email/> and filling out the required information.

For new hires who are located or teaching in buildings that are set up with electronic locks, the department administrator needs to place a request for swipe-card access by sending an email to Dana Terrell at dterrell@uapd.ua.edu (copy eTech at eTech@as.ua.edu), and detailing the buildings and room numbers to which the new employee will need to have access. If the individual will be working in areas that have alarms, please contact Tom Hall at thall@fa.ua.edu (copy eTech at eTech@as.ua.edu) to request alarm-code activation. In order to process this request, the department will need to include the individual's CWID and a personally selected 4-digit alarm code (must not begin with a zero) in the email.

2.2 Faculty

After new faculty accept a position within the College of Arts and Sciences, the Dean's office sends each new hire an acknowledgement letter, which includes directions for how they should request a new office computer. When the computer request form has been completed, an auto-response is generated, allowing new faculty to review their submission and to request software.

Once faculty arrive on campus, they can stop by the eTech office to pick up a College-issued iPad. The individual will be required to bring their action card and to fill out a form with their name, CWID, department, email address, and office location, which is kept on record in the eTech office.

During their first year at UA, new faculty will be required to attend a series of mandatory technology meetings. The purpose of these meetings is to provide new employees with general information regarding educational technology and multimedia. Although the exact dates will vary each year, eTech typically schedules the first introductory meeting between August 15th and the first day of class. Multiple sessions will be offered so the new faculty can pick a day and time that best suits their schedule. Subsequent meetings will be held later in the year and will focus on more specific educational technology and will be conducted by the Director of Instructional Technology and the eTech mentors.

2.3 FTTIs and PTTIs

eTech is aware that the process for hiring non-tenure track instructors can result in some FTTIs and PTTIs being hired close to or even after the beginning of a semester. However, the turnaround time for a computer to be installed after it is requested can be up to four weeks, which creates difficulties for new instructors that are hired at the last minute.

In order to help departments meet their technology needs for FTTIs and PTTIs, eTech has developed a system where the departments will make computer requests based on the number of FTTI and PTTI lines they have been given for the following year. On or before July 15th, departments will send a request to etech@as.ua.edu. This request will include the total number of computers needed (based on the total number of FTTI/PTTI lines), the names of the FTTIs and PTTIs that are currently hired, the offices where the computers will be located, and a contact name, number, and an email address for a person that can be contacted regarding the installation. Please email the eTech office with FTTI/PTTI information as soon as they are hired. **If the total number of FTTI/PTTI lines increases and/or additional computers for these instructors are needed, the departments should contact the eTech office immediately.** These computers will be held with OIT or eTech, and will be delivered when eTech receives notification of new hires. This new system will allow eTech and OIT to reduce the turnaround time from 4 weeks to a few days.

All FTTIs (not PTTIs) will receive College-owned iPads and can pick them up from the eTech main office once they begin work. Only FTTIs who appear on an approved list of department instructors will be issued iPads, so it is important that each department provide a list to eTech and notify the eTech office when changes are made to this list. The individual will be required to bring their action card and to fill out a form with their name, CWID, department, email address, and office location, which is kept on record in the eTech office.

Note: If new faculty or instructors are placed in rooms that have not previously been used as offices or have not been used for a while, the department will need to verify that there are functioning network/internet jacks available. In order to do this, the departments can visually verify whether there are network jacks and can call the IT Service Desk at 348-5555 to request that OIT ensure that they are active.

2.4 Checklist for New Hires

All New Hires (Faculty, Instructors, Staff)

Office Administrator:

- Create Zero PA for CWID.
- Request email, share-drive, and home drive access.
- Request building and classroom swipe-card access and alarm-code activation, if needed.

New Faculty and Instructors

Office Administrator (please complete the following on or before July 15th):

- Place computer requests for newly hired instructors – include names, CWIDs, office locations, and contact information.
- Place request for number of remaining computers needed, based on the remaining open instructor positions available for that year. (Computers will be installed once the departments submit the actual requests with the instructor names, CWIDs, office locations, and contact information.)
- Provide eTech with a list of names of all FTTI instructors for that year, and indicate whether they have 1-year or 3-year appointments.

New Faculty:

- Request computer as soon as provided with entry code from Dean's acknowledgement letter.
- Stop by eTech to pick up the College-issued iPad. (bring action card)
- Contact eTech for Educational Technology mandatory meeting schedule.

FTTIs:

Stop by eTech to pick up College-issued iPad. (bring action card)

2.5 Exiting Employees

When faculty, instructors, and/or staff leave the College of Arts and Sciences, Office Administrators and/or Department Chairs must follow the steps below to make sure that the proper systems are deactivated and that equipment is recovered. It is important that the departments note the status of the employee and why they are leaving (retiring versus leaving), since their cut-off dates for access to various University systems will be dependent on this information. For example, an employee who is fired will immediately lose access to the system while a retiring professor may be allowed access to the system under emeritus status. The following two processes outline some of the differences between the types of exiting employees:

Staff

As soon as departments are notified that staff members are leaving their department, the department administrator should notify the eTech main office. eTech will need to know the full name of the staff person, their CWID, the date that they are leaving, and the reason they are leaving (retired, fired, left, deceased, etc.)

Once the above information is provided, eTech will notify HR, OIT, Security, and the College to make sure that all access to electronic systems, software, buildings, and offices is terminated by the date the employee will be leaving. Unless there are extenuating circumstances that are approved by the Dean's office, all staff access will be terminated by the last day of employment.

Staff who retire are not allowed to come back to work at the University at least two years after they leave. If there is a desire on the behalf of the staff member to return to UA after this time, the department should notify eTech. eTech can then put in the request for OIT to keep the staff member's email address on file for two years so it may be reinstated in the event that the individual is rehired.

Faculty and Instructors

As soon as departments are notified that faculty or instructors are leaving their department, the department administrator should notify the eTech main office. eTech will need to know the full name of the faculty//instructors, their CWID, the date that they are leaving, and the reason they are leaving (retired, fired, left, deceased, etc.)

Once the above information is provided, eTech will notify HR, OIT, Security, and the College to make sure that all access to electronic systems, software, buildings, and offices is terminated by a set date. The following timelines will be used to cut-off access for faculty and instructors:

Employee Status	Reason for Termination	Cut-off Date
Faculty	Fired	Immediate
Faculty	Left	3 months from date of termination
Faculty	Retired, Emeritus	No cut-off until department/Dean's office notification
Faculty	Retired, Left	3 months from date of termination
Faculty	Deceased	Immediate
Instructor	Fired/Left	Immediate
Staff	Fired/Left	Immediate
Staff	Retired	Immediate (email address may be kept on file for 2 yrs)

Access can be removed earlier than is posted above, if the departments notify eTech prior to an employee's last day. For departments that would like for the faculty to have access for longer than is listed, they can send an email request to the eTech office. However, approval from the Dean's office will be required before such extensions can be granted.

2.6 Checklist for Exiting Employees

Please note that this list is time-sensitive and should be completed prior to the employee's last day of work.

- Send an email to the eTech office at eTech@as.ua.edu, providing the name and CWID of the person leaving, their termination date, and their reason for leaving.
- Collect any University-issued keys
- Retrieve the individual's College-issued iPad
- Contact eTech to request that someone pick up the iPad and computer
- Submit a termination PA to A&S Financial Affairs office

3.0 Instructional Technology

The instructional technology division of eTech supports those faculty and instructors who wish to incorporate technology into their teaching and research. Of late, most support has been for incorporating iPads into teaching. eTech provides one-on-one meetings with faculty, department presentations, and support through the A&S iPad blog, found here: <http://as.ua.edu/ipad>. eTech also works cooperatively with the University Faculty Resource Center, which assists faculty with enterprise tools, such as Tegrity, Turning Technologies clickers, Turnitin, and Blackboard. Please see the FRC website for more information on their workshops and other support: www.frc.ua.edu. For a list of eTech and FRC contacts, see Section 6.0.

Just before the beginning of their first semester with the University, all new faculty and instructors participate in a workshop that provides an overview of the most commonly used technology and software in the College. In the past, this workshop has covered the Symposium, iPads, Tegrity, eLearning, and the Turning Technologies clickers. For instructors, this overview is provided during FTTI/PTTI orientation. For faculty, workshops are offered at the beginning of fall semester. Returning faculty are also welcome to attend this session as a refresher course, or they can schedule an appointment with eTech for a one-on-one session.

The eTech Mentors are a group of faculty in the College of Arts and Sciences who have successfully incorporated technology into their teaching. They conduct a multi-session workshop in the spring semester in which they work with participants on how to document the achievement of learning outcomes with technology tools. eTech mentors are available to their fellow faculty who may have questions about enterprise technologies at the University. They also provide regular updates on technology issues through the eTech mentors blog at <http://as.ua.edu/etechmentors/>.

4.0 Additional Information

4.1 Share and Home Drives

Share and home drives are both storage systems contained on the University network and are sometimes referred to as network drives. A share drive is one to which multiple people have access. Each department has their own folder and subfolders contained on the share drive. The department chair can designate which individuals or groups of people (faculty, staff, instructors) within their department have access to the various folders. Every employee has a home drive, which is their own personal network drive that they can use for as long as they are employed with the University.

4.2 Virtual Private Network (VPN)

The virtual private network (VPN) allows faculty and staff to access the UA network while using a public network connection. The following list describes when it is typically necessary to connect to the VPN.

- The VPN is necessary to remotely access data on faculty or staff office systems from off campus using either a desktop or laptop. Remote Desktop Protocol (RDP) is necessary to log into the faculty or staff office computers from another computer either on or off campus.
- When faculty or staff who normally use University laptops are off campus, they must connect to the University Network through the VPN in order to access shared folders/files. No RDP is necessary.
- It is necessary to connect to the VPN when using a computer off campus to access folders/files on an office PC or folders/files on the share drive or home drive. In order to do this, the faculty or staff should first log into VPN, then log into RDP.
- Email can be accessed remotely through webmail at webmail.ua.edu. No VPN connection is necessary for this connection; however, this connection will not provide access to local files or files on the share drive. Webmail is only a web interface to email - not a client interface like Outlook or Entourage.
- Self-Service Banner and Banner INB can both be remotely accessed without using VPN.
- Remote Desktop (RDP) can be used by a faculty or staff to access files on a campus computer from another computer that is also located on campus.

5.0 Useful Links

eTech Website

<http://as.ua.edu/etech>

Equipment Reservations

<http://as.ua.edu/etech/equipment/>

Computer Lab Reservations

<http://as.ua.edu/labs/>

eTech Mentors Blog

<http://as.ua.edu/etechmentors/>

eTech iPad Blog

<http://as.ua.edu/ipad>

Request for Email Account

<http://as.ua.edu/etech/email/>

Classroom Reservations

<http://as.ua.edu/etech/reservations>

A&S Website

www.as.ua.edu

Office of Information Technology

www.oit.ua.edu

HR New Hire Forms

<http://hr.ua.edu/benefits/HRforms.html>

6.0 Contacts

eTech

eTech@as.ua.edu

348-4832

120 Bureau of Mines

IT Service Desk

itsd@ua.edu

348-5555

125 Gordon Palmer Hall

Audio/Visual Solutions

348-6011

117 Lloyd Hall

Faculty Resource Center

elearning@ua.edu

348-3532

A203 Gordon Palmer Hall

Computer lab issues, reservations & general lab info (hours, locations, etc.)

Susan Johnston in eTech: <http://www.as.ua.edu/labs>; 348-4832

iPads for teaching use and applications

Rebecca Johnson in eTech: 348-4832; rljohnson@as.ua.edu

Other technologies in your teaching (wikis, blogs, Second Life, etc.)

Rebecca Johnson in eTech: 348-4832; rljohnson@as.ua.edu

Other technology-related questions

Ruth Pionke in eTech: 348-4832; rlpionke@as.ua.edu

Developing online forms/web applications

John Hawkins in eTech: 348-4832; jhawkins@as.ua.edu

Departmental websites

Amy Garner in eTech: 348-4832; ardowdle@as.ua.edu

Online courses through the College of Continuing Studies

Rebecca Johnson in eTech: 348-4832; rljohnson@as.ua.edu

Faculty and staff office computer questions

IT Service Desk at 348-5555 or eTech at 348-4832

Multimedia classroom questions

Use the Classroom Helpline phone (next to the multimedia podium) if you are in the classroom and need immediate help, or call 348-3453

Software site licenses

<http://oit.ua.edu/oit/services/software-licensing>

Tegrity course capturing

Faculty Resource Center: 348-3532; elearning@ua.edu

Clickers (Turning Technologies)

Faculty Resource Center: 348-3532; elearning@ua.edu

eLearning

Faculty Resource Center: 348-3532; elearning@ua.edu

Developing videos, copying videos, voice recording, etc.

Rebecca Johnson in eTech: 348-4832; rljohnson@as.ua.edu

7.0 Appendix

7.1 Appendix A - Zero PA

2/24/09

New Faculty/Staff Setup - Demographic Information For Prospective Faculty/Staff Not Currently Paid on UA Payroll Request for Authorization to Access Campus Services

Home Organization Number: _____

Biographic / Demographic Information

Social Security Number*: _____ Campus Wide ID _____

Name (First, Middle, Last)*: _____

Current Mailing Address*: Street Address: _____

Address 2: _____

City, State, Zip Code: _____

Phone Number: _____

Birth Date*: _____

Race*: _____

Gender*: _____

US Citizen*: Yes No

Employment Information

Expected Start Date*: _____

Date Employee Will Need Access to Campus Services*: _____

Date Access to Campus Services will end: _____

Person will be*: New Faculty New Staff Adjunct not on Payroll ROTC Retiree not on payroll Other
Graduate Fellow

Explanation of "Other": _____

If the person will be put into a paid status as an Employee, indicate the status of the Employee below:
Regular Full Time Regular Part Time Temporary Full Time Temporary Part Time Contingen/On Call

Has the new employee ever been associated with The University of Alabama as a student or employee? Yes No

Has the new employee been reimbursed by Accounts Payable for travel or other expenses? Yes No

Department Contact Information:

Prepared by*: _____ Date*: 12/20/11

Phone Number*: _____ Email Address*: _____

Approved by*:(Dean, Director, Department Head) _____

Submit this form to Human Resource Input for processing:
Email to: hrintput@fa.ua.edu
Fax to: 348-2737
Campus mail to: HR Input
Box 870128

*Required

ECLS
POSN

7.2 Appendix B – Guest Wireless Policy

To: College of A&S Department Chairs and Administrative Staff
From: Ruth Pionke, Director of Operations, Office of Educational Technology
Date: September 14, 2011
Re: Guest Wireless Information

OIT has provided us with a new password for the A&S guest wireless account this year. (see below) This account should be used for department guest speakers and professional visitors who need wireless while visiting the University. Please read over and become familiar with the policy regarding use of this account. If you have any problems with the connection, please contact the IT Service Desk at 348-5555 or itsd@ua.edu.

Thank you.
Ruth

UA Public Wireless Guest Registration

The UA Public wireless guest registration account below should only be released to visiting professionals/vendors who require Internet access to conduct business affiliated with The University of Alabama. The account will be active for guest registration for one year.

Account ID: as-guest
Password:

By accepting this account information, you are agreeing to the following terms and conditions:

- A. Each account is for the exclusive use of the individual or organization to whom it was assigned and users may not allow or facilitate access, including by a proxy or anonymous remailer, to University computer accounts, equipment, or restricted files or systems by others. Authorized users are faculty or staff who are employed by the University and currently enrolled students, unless their access privileges have been revoked by the University.
- B. The use of the account may not violate any policy of the University.
- C. The use must not overload the University's computing equipment or systems, or otherwise negatively impact the system's performance.
- D. The use must not result in commercial gain or benefit to the users and cannot constitute consulting for a business or running a business. The page or site may not promote commercial activities or display paid advertising.

- E. The use may not violate laws or University policies against discrimination or harassment due to race, sex, religion, disability, age, or other protected status.
- F. The use may not violate state laws or University policies on the use of University equipment, resources, or time for political activities.
- G. The use must not involve sending of soliciting chain letters, nor may it involve sending unsolicited bulk mail messages (e.g., “junk mail” or “spam”).
- H. The use may not imply or state University sponsorship or endorsement, nor use University trademarks without permission of the University’s Licensing Program.
- I. The use may not involve unauthorized passwords or identifying data that attempts to circumvent system security or in any way attempts to gain unauthorized access.
- J. A Web site or page of personal collection of electronic material that is accessible to others must include and display the following disclaimer: “The views, opinions, and conclusions expressed in this page are those of the author or organization and are not necessarily those of The University of Alabama or its officers or trustees. The content of this page has not been reviewed or approved by The University of Alabama, and the author or organization is solely responsible for its content.”
- K. The University may examine personal electronic information stored on or passing over University equipment or networks, for the following purposes: (1) to ensure security and operating performance of its computer systems and networks; (2) to enforce University policies or compliance with state or federal law where (a) examination is approved in advance by a dean, vice president, or the president, and either (b) there is reasonable suspicion that a law or University policy has been violated and examination is appropriate to investigate the apparent violation, or (c) examination is necessary to comply with state or federal law. Computer users should have no expectation of privacy in personal material sent, received, or stored by them on or over University computing systems or networks when conditions of subparagraph (1), or both (2a) and (2b), or both (2a) and (2c) above have been satisfied.
- L. Use that violates the terms of the account agreement, state or federal law, or any University policy may result in referral for action under the appropriate disciplinary procedure and the imposition of sanctions which may include suspension or revocation of access privileges in addition to other sanctions.

If you have any additional questions, please feel free to email ITSD@ua.edu or call 348-5555.

7.3 Appendix C – Information Storage, College of Arts and Sciences

To: College of A&S Department Chairs and Faculty
From: Ruth Pionke, Director of eTech
Ashley Ewing, Information Security Officer
Date: January 19, 2012
Re: Information Storage, College of A&S

With the increasing interest from faculty in reporting student and course information electronically, it is important that this information be stored and transferred using secure methods. The College of Arts and Sciences' Office of Educational Technology has worked with the Office of Information Technology to establish some guidelines that departments can use to make sure that their information is as safe as possible and that no one inadvertently violates any Family Educational Rights and Privacy Act (FERPA) regulations.

This memo includes a list of dos and don't that all faculty should keep in mind when storing and transferring student information. Please be aware that failure to abide by these guidelines could result in legal liability for the individual and/or the department.

Dos

Store all student information on the University network drives. This includes the share drive and faculty home drives, all of which are contained within the University firewall.

Use the University of Alabama Virtual Private Network (VPN) whenever attempting to access share drives from off-campus. Additional information on when to use the VPN can be found under the FAQs section at the end of this memo. For those who need help accessing the VPN, contact the IT Service Desk at 348-5555.

Faculty and staff should send all correspondence with students and about students through UA email accounts only. Please keep in mind that while non-UA email servers may advertise that they are secure, these providers glean information from your emails for research purposes. Therefore, outside email sources should never be used for sending any student information such as CWIDs or grades.

Faculty are allowed to keep gradebooks (hard copies and electronic) in locations off the network drives, with the assumption that appropriate precautions are taken to make sure that the information is not easily accessible or viewable by other people. When faculty are using external sources (laptops, home computers, physical grade books, iPads, etc.) to

record student grades, they should take care to disclose as little information as possible on these records. Student names are acceptable, while last name only (or last name with first initial) would create a higher level of security. Faculty should never record student names with CWIDs in their grade books.

Don'ts

Do not save any CWIDs to unprotected devices, such as a non-compliant server, flash drive, unencrypted laptop, disk, external hard drive, or an unsecured online system such as Dropbox, Evernote, or GoogleDocs. If you are unsure whether the device or system is secure, contact eTech at etech@as.ua.edu or just don't use it.

Never store social security numbers for students, staff, or faculty on any personal devices, external storage devices, or office computers. *There is no reason that departments should ever need or use social security numbers for work or any other purpose.* If departments are using forms that ask for social security numbers, they should remove this category immediately. If the form is from an outside source, the department should instruct the individuals filling out the forms to write "declined" in that section. (If the form is from an outside source within UA, please contact eTech so the staff and OIT security can investigate the matter.) When departments receive documents that contain social security numbers, they should obliterate the numbers with black markers on hard copies and delete the numbers on electronic copies.

Don't collect or store sensitive student information on unsecured electronic devices (this does not include grade books). Sensitive information includes student names when they are combined with CWIDs, birthdates, mothers' maiden names, social security numbers, grades, medical records/data, or entrance exam scores. If any faculty or staff members are collecting this type of information, it should be stored on the share drive or a University-encrypted laptop. Anyone who is storing this information on unsecured external electronic devices should transfer it to the share drive and immediately delete it from the external source. Any hard copy materials with sensitive student information should be shredded.

No A&S department should be using unapproved off-network servers to store student information, department emails, share drive folders, etc. Any existing share drives in departments must be cleared through the College of Arts and Sciences and undergo review from OIT security to determine whether they can be used. See following page for more information on servers.

FAQs

What is a server?

A server can be ANY computer regardless of size or location that accepts external connects for services such as Web Sites, FTP, SSH, or any other file sharing services through databases or other software that is made available to external users.

Virtual Private Network (VPN)

The virtual private network (VPN) allows faculty and staff to access the UA network while using a public network connection. The following list describes when it is typically necessary to connect to the VPN.

- The VPN is necessary to remotely access data on faculty or staff office systems from off campus using either a desktop or laptop. Remote Desktop (RDP) is necessary to log into the faculty or staff office computers from another computer either on or off campus.
- It is necessary to connect to the VPN when using a computer off campus to access folders/files on an office PC or folders/files on the share drive or home drive. In order to do this, the faculty or staff should first log into VPN, then log into RDP.
- When faculty or staff who normally use University laptops are off campus, they must connect to the University Network through the VPN in order to access shared folders/files. No RDP is necessary.
- Email can be accessed remotely through webmail at webmail.ua.edu. No VPN connection is necessary for this connection; however, this connection will not provide access to local files or files on the share drive. Webmail is only a web interface to email - not a client interface like Outlook or Entourage.
- Self-Service Banner and Banner INB can both be remotely accessed without using VPN.

Remote Desktop (RDP) can be used by a faculty or staff to access files on a campus computer from another computer that is also located on campus.

What to do with old graduate applications containing social security numbers?

Although the Graduate Office has now discontinued the practice of collecting social security numbers for graduate student applications, many departments are wondering what to do with the information already collected. For those departments who have retention policies for these applications, make sure that the paperwork is always stored in a secure location. When the retention period has expired, hard copies of documents containing these numbers should be shredded. Departments should not be collecting SS numbers as part of an electronic database. If

any grad student databases currently contain social security numbers, delete this column immediately. Grad application information is considered sensitive and should be stored on the network drives.

What constitutes FERPA information?

For a complete description of FERPA information, please see the Registrar's website at <http://registrar.ua.edu/academics/privacy-guidelines/ferpa-fact-sheet/>. However, here are some highlights that are pertinent to faculty:

In Order To Avoid FERPA Violations, Faculty Should Not:

- Use the SSN/Student ID/Student Names to post grades.
- Leave graded tests [electronically or in print] for students to sort through.
- Circulate electronically or in print, class list with the Student Name and SSN/Student ID.
- Provide anyone with student schedules.
- Provide anyone with lists of students enrolled in your classes.
- Include confidential information (i.e., grades, #of credits) in a commendation letter without the written consent of the student [Note: If a student provides you a resume with the information, you may disclose whatever is in the resume.]

Faculty or staff with any questions about electronic security issues can contact Ruth Pionke at eTech, OIT, or they can go online to <http://oit.ua.edu/oit/security/>.