BYOD Strategy
2014

BYOD Strategy Group
Joseph Casabona
Lee DeAngelis
Adam Edwards
Diane Kennedy
Calvin Krzywiec (Chair)
Timothy Meade
Glen Pace
Jason Wimmer

Planning and Information Resources
Q: What will be the governance path/process for this proposal? Will the strategy or any of its components require the creation or alteration of policies?

Recommendation:
BYOD will have significant implications for teaching, research, and service, as well as the faculty work environment. TAG strongly recommends careful review of this proposal by the Faculty Senate, and we further advise that any BYOD/MDM policies go through the full, formal governance process.
Summary

The Bring Your Own Device (BYOD) phenomenon offers a unique challenge to IT departments as more students, staff and faculty bring their personal devices and services to campus. The ease of use and ubiquitous nature of consumer technology has led to an increased demand for access to institutional services and data from non-University devices. Since support for BYOD touches all aspects of technology, the BYOD Strategy Group was formed to develop a three-year, high-level strategy for supporting BYOD as it relates to the mission and the vision of the University.

This document is a collection of strategic objectives for addressing the BYOD phenomenon. This strategy is based upon findings from industry specific research publications and contextual conversation among the members of the group. The group compiled and evaluated industry research recommendations and tailored them to local objectives.

Teaching and Learning

As the population of students and faculty bringing technology to campus continues to rise, this technology can be leveraged as an opportunity to enhance the teaching and learning environment. Students today have high expectations for “anytime anywhere” access to teaching and learning material [3]. Expanding mobile friendly content delivery solutions, such as lecture capture and the LMS, provide students access to lecture resources beyond the walls of the classroom. Additionally, students have a higher demand for the integration of their devices into the classroom [3]. Technology solutions can be leveraged to provide faculty and students untethered access to classroom resources, such as mediation and computing infrastructure.

As we look to incorporate client devices into the classroom, BYOD can be leveraged as an opportunity to eliminate a majority of the traditional computing infrastructure provided within instructional spaces. Given the already successful deployment of virtual desktops into the lab spaces and the fact that the vast majority of students own a laptop or tablet [1], these two technologies could be combined to reduce the physical computing infrastructure deployed to labs. This design would rely on the student’s device to connect to a virtual lab desktop or virtual lab applications rather than deploying a traditional computer or VDI thin client into the classroom. This would have a tangential effect of reducing other classroom infrastructure, such as network cabling and switching requirements.

The financial analysis of this is complicated and requires further study. While this may seem like an opportunity for cost reduction, the capital savings associated with traditional PC hardware or VDI thin clients will likely be offset by licensing fees (specifically, Microsoft VDA licenses). Some remaining dollars will likely need to be redirected to fund the network, server, and storage infrastructure required to provide this service. Financial considerations aside, the service provided is
Q: Which three years? When does IR expect to implement the strategy? What steps will take place in what years?

Note: No further reference is made to the University mission or vision. Perhaps a more explicit explanation/articulation of the relationship between the BYOD strategic objectives and the University mission might be in order?

Q: Were there other publications reviewed that are not included in the list of Works Cited? EDUCAUSE seems to be the sole source consulted.

Recommendation:

Note: TAG members (among many other faculty) are enthusiastic about new lecture capture capabilities and recommend that faculty use of lecture capture be encouraged and supported. At the same time, we remind all parties that (under Appendix VIII: Copyright and Appendix X: Distance Learning) any recording and/or transmission of a professor’s lecture should be done at the discretion of that professor, under whatever conditions s/he imposes on the distribution and use of his/her intellectual property.

Notes:
See also faculty concerns regarding specialized software, consistency across operating systems, online testing, etc raised in TAG’s 2013 faculty technology questionnaire (http://blogs.scranton.edu/tag/files/2014/03/2013FacultySurvey-CompiledResponses1.pdf). Note also several mentions of *improvements* to classroom infrastructure that would be necessary for successful implementation of BYOD: power supply, wireless access, display screens, etc.

Recommendation:
While students may indeed bring their own devices more frequently in the future, current demand for computing resources often exceeds supply. Any plans for phasing out instructional labs should include careful review of current usage of available resources and testing of alternatives prior to implementation. We strongly recommend that faculty be full participants in the planning and piloting process for proposed BYOD spaces. We also suggest the creation/implementation of a dynamic, searchable database displaying the real-time availability (and location) of hardware, software, workstations, etc.

Q: This section seems to include regular mediated classrooms, computer lab classrooms (such as those used for freshman writing), general, non-scheduled computing labs (like the Library’s), departmental/specialized computing labs (like the Physics instrumentation labs), and (possibly?) research labs. Is there any distinction between how these spaces are treated/addressed?

Notes:
Several faculty members expressed concerns about versioning and specific functionality of specialized software licenses. For example, does the virtual, licensed version of X software match the functionality and features of the full desktop version? Will the licensed version of X work on all operating systems? Faculty also expressed concerns about the computing power of virtual desktops. For example, will virtual solutions support several simultaneous analyses of large datasets, as may be conducted in a research methods class?

Recommendation:
IR should working closely with faculty and Library to develop a sustainable portfolio of software licenses that meet teaching and research needs.

Q: This draft of the Strategy seems conflicted on the financial implications of BYOD. Several references are made to significant financial savings, though mention is also made of the costs of supporting related services or infrastructure (software licenses, increased power supply, new furniture, etc). We agree that more analysis is needed in order to better understand the anticipated costs and savings.

Recommendation:
TAG requests further and more detailed analysis of the financial aspects of a move to BYOD, including support for specialized software and recommended improvements to classroom infrastructure.

Q: What are the current software licenses the University holds? How do the costs of virtualized software licenses compare to the desktop installations currently deployed?
invaluable. Students would now have access to lab resources beyond the borders of the classroom (e.g. specialized software), extending educational resources to their residence halls and off campus locations. This service is beneficial to current students and marketable to future students. This may also allow for the elimination of some open computing labs, resulting in further cost reduction. It’s important to note that a complete reduction in lab computing infrastructure is not feasible as virtualization is not currently suitable for some specialized labs. Additionally, some open lab machines will be necessary to address disparities in student computer ownership or provide assistance to users with a failed device [2].

Changing the classroom technology necessitates a change to the classroom and lab workspaces. As future classroom renovations occur, rigid furniture should be replaced with flexible workspaces to accommodate mobile devices. Much of the classroom space on campus is constructed with traditional PCs in mind, with power sources being relatively inaccessible and therefore, limits the use of mobile devices for longer durations. Although specific to smartphones, ECAR research supports this, listing “inadequate battery life” as the top barrier to using such devices as a learning device [3]. Flexible workspaces in general use labs (i.e. open labs) will facilitate increased collaboration among students and help promote the sense of community that is core to our mission. The Library Learning Commons will be an interesting project to monitor and will serve as a litmus test for how students will utilize such an environment.

The increased demand for classroom technology has resulted in the organic growth of lab spaces over the years. This demand continues to grow in contrast to a physical footprint that remains relatively constant. Scheduling complexities occur as the registrar attempts to meet the needs of faculty with the finite lab spaces available. As such, construction projects are leveraged as opportunities for the creation of new lab spaces populated with computing devices to address the demand, which results in an increase in overall operating costs for the lab environments. The combination of virtual labs and mobile-friendly classroom environments will reduce the complexity in classroom scheduling as any classroom could conceivably be converted, on the fly, to a computing lab. This approach should remove the need for the addition of spaces with dedicated lab devices in the future, having an overall positive effect on future operational costs.

As more student devices enter the classroom, some faculty have expressed concerns related to academic integrity, as mobile devices have the potential to allow easier access to outside resources during electronic assessment. This will become more of an issue if BYOD access to lab resources is introduced. As such, additional solutions need to be introduced to address faculty concerns. This group does not have a recommendation on a specific technology to address this concern, but it does recommend that this be investigated further as a prerequisite to BYOD in the lab spaces.
Note: This is consistent with faculty concerns as expressed in TAG’s 2013 faculty technology questionnaire (http://blogs.scranton.edu/tag/files/2014/03/2013FacultySurvey-CompiledResponses1.pdf).

Note: This is consistent with faculty concerns expressed in 2013 TAG faculty technology questionnaire (http://blogs.scranton.edu/tag/files/2014/03/2013FacultySurvey-CompiledResponses1.pdf). Faculty from the Nursing and Mathematics departments are especially interested in working on robust solutions for electronic assessment.
Thus far, we've introduced a number of technology changes both inside and outside of the classroom. As these and future solutions are implemented, support models should be enhanced to accommodate training and support for the students and faculty that will incorporate these solutions into their teaching and learning toolbox. Success of BYOD in this area is tied closely to the institution’s ability to proactively support and train their faculty in the integration of this technology into their classroom [4]. As such, this group recommends partnering with the CTLE to develop a model of proactive support for faculty on the use of the proposed technology. Additionally, engaging faculty in the implementation of BYOD has shown to be an effective strategy at other institutions for gaining acceptance for the use of these technologies in the classroom environment.

**Strategic Objectives:**

- Increase student and faculty interaction with technology in the classroom
  - Investigate and implement untethered teaching / learning solutions
  - Focus classroom upgrades on providing collaborative, flexible workspaces
  - Leverage virtual desktop / application technologies and client devices to reduce reliance on physical lab infrastructure
  - Investigate and implement secure electronic assessment solutions
- Extend access to classroom resources to anytime / anywhere
  - Leverage virtual desktop / application technologies to provide ubiquitous access to lab software resources
  - Expand lecture capture to additional locations
  - Leverage the LMS to provide mobile access to course material
- Partner with the CTLE to provide a proactive approach to classroom technology solutions, including technology support and training

**Staff and Faculty**

The core issue associated with BYOD for faculty and staff is how to best provide access to campus services from non-corporate assets, while maintaining the security of institutional data and the integrity of campus software licenses. At this point in time, staff is more likely to use BYOD as a supplement to institutionally provided devices for “routine” access to institutional services and data, such as email and documents. In addition, staff is more likely to use their own devices for remote access to institutional services. Faculty will also fall into this model. However, given that faculty have historically required greater flexibility in technology choices to facilitate their teaching and research, they are also more likely to utilize their own devices in place of standard institutionally provided devices. These predictions are mostly based on anecdotal evidence, but ECAR research supports this in terms of the growth of devices accessing institutional networks by population [5]. That said, embracing BYOD for faculty and staff would rely on the same set of technology solutions and security controls.
Recommendation:
IR should include faculty as full participants in planning and piloting BYOD solutions and strategies. TAG is willing to identify and recommend to the Faculty Senate individual faculty members interested in particular BYOD-related issues (such as electronic assessment).

Q: What is the estimated/planned timeline for implementation of these objectives? What are the next steps?

Q: What are "non-corporate assets"?

Note: Appendix VIII (Copyright) of the Faculty Handbook (http://www.scranton.edu/academics/provost/FAC/fac_handbook.shtml) establishes faculty ownership of most works created while fulfilling regular duties (teaching, research, service, etc). Faculty retain ownership of their documents and research data.

Q: What are the “institutional services” (later “campus services”) invoked? (e.g., email, RoyalDrive, my.scranton, LMS, Banner, network, wireless, authentication...?)

Note: Several faculty members disputed this generalization. TAG has anecdotally observed many faculty members using both personal and institutional devices, and we suggest that a formal survey of faculty be conducted if specific evidence on this point is needed.

Note: At the 2014-05-07 TAG meeting, Jim Franceschelli and presenter Calvin Kryzwy described the BYOD Strategy proposal as “mostly intended for staff.” This language, however, suggests that the proposal would apply equally to faculty and staff.
As faculty and staff bring their devices to campus, they will want to interact with campus services. Classifying and isolating corporate versus non-corporate devices on the network provides for the ability to selectively allow access to campus services from non-corporate devices through the use of technical controls, such as firewalls. For example, a staff member working from their personally owned machine can access common intranet resources, such as printing services, but cannot connect to the ERP.

When access to restricted resources is required, faculty and staff can leverage virtualization technologies to access the resource. This solution allows the employee to interact with the service they need (in this case, the ERP), without the risk of data loss. Virtual desktops and applications have the added benefit for allowing faculty or staff to utilize University licensed software from their personal devices, without violating the license agreement. For example, a faculty member brings their personal laptop to campus and interacts with common software from their own device, such as a Microsoft Office or the LMS. When the faculty member needs to utilize University licensed software (such as SPSS), they can utilize a [virtual application] to do so without violating the terms of the license. Should more faculty and staff bring their own primary computing devices, this technology would give them access to a University desktop and applications from their own device at a fraction of the cost of a traditional University issued device. This same approach can be utilized for remote access to restricted services, accomplishing the same goals with users’ home machines.

As BYOD grows and users begin to utilize their own primary computing devices in lieu of an institutionally provided device, reimbursements models will need to be developed. There is currently no clear industry model for this. Reports from other institutions vary widely by amount, employee type, technology and duration [5]. This is likely due to the fact that this model of BYO primary computing device is not widespread. As this grows, considerations for equipment and software reimbursements should be considered.

While the above technical solutions work well for access to intranet and restricted services from personally owned devices, there is still a risk of data loss from public services. Email and other data storage on mobile devices make them likely sources for a data breach as these devices are frequently lost or stolen. Additionally, as more employees are linking University email accounts to their personal phone, data loss can occur on employee separation, as there is currently no mechanism to ensure that institutional data has been removed from the personal device. Investing in a comprehensive mobile device management (MDM) program can help mitigate data loss by ensuring that the appropriate controls are in place and that corporate data can be wiped from devices when necessary.

In a higher education environment, the same MDM controls are not appropriate for everyone. The following three-tiered approach is recommended:
Faculty members are very interested in remote access to specialized software. As mentioned above, however, careful evaluation of software functionality should be conducted to confirm that the licensed version will fulfill teaching/research needs.

Faculty members seem open to discussion on this point, though we note that some faculty contracts include specific mention of computing resources. Faculty and Academic Affairs should be active participants in any shift to the existing paradigm.

TAG may suggest to the Faculty Senate the establishment of an ad hoc committee to study and compare models for the provision of computing resources (desktops, laptops, etc) to faculty.

Q: What are “public services”? Are all services considered to bear equal risk of loss of confidential or restricted data?

Q: Have existing policies addressing data management (Information Classification & Protection Policy, Information Access Policy, Records Management and Retention Policy) been successfully implemented? Are they currently being enforced?

The Information Classification & Protection Policy describes (in Appendix C) appropriate controls for information classification. Systems and services that are acceptable for public data storage and transmission (e.g., email) should be treated differently than systems and services designed to support controls for confidential or restricted data (e.g., Banner).

Q: Assuming the successful implementation of regular Identity Finder scans, and given the many IR policies regarding information and records management, what is the current likelihood of faculty email holding confidential or restricted information? How does this level of risk compare to other possible data breaches?

Recommendations:
Services involving confidential or restricted data (e.g., ERP) should be isolated as much as possible from everyday services such as email, following the controls described in the Information Classification & Protection Policy.

Recommendation:
Information Security should offer guidelines and training for the secure management of confidential and restricted data, particularly with reference to encryption and use of University file storage systems (currently Royal Drive). For example, the 2012 Remote Access Guidelines could be updated and expanded.

Reference:
Information Classification & Protection Policy, last updated 2013-10-22
https://royaldrive.scranton.edu/Groups/Planningandinformationsystems/PAIRO/Governance/Policies/Information%20Classification/Info%20Classification%20Policy%20Revised%20Final%20Oct%202013.pdf?ticket=t_hzRGsmFL
Remote Access Guidelines (2012-12)
https://royaldrive.scranton.edu/xythoswfs/webui/_xy-31489842_1-t_kbOLGBB

Q: The unqualified term “data loss” implies a conflation of all types of “University information”, regardless of classification. The Information Classification & Protection Policy itself, however, describes different levels of control for restricted and confidential information in comparison to public information. Does the MDM solution proposed differentiate at all between these classifications?

Reference: Information Classification & Protection Policy, last updated 2013-10-22
https://royaldrive.scranton.edu/Groups/Planningandinformationsystems/PAIRO/Governance/Policies/Information%20Classification/Info%20Classification%20Policy%20Revised%20Final%20Oct%202013.pdf?ticket=t_hzRGsmFL

Q: What are the current procedures for employee separation? Do these procedures apply equally to faculty and staff?

Note: Faculty separation can take many forms - for example, phased separation, terminal sabbatical, emeritus status, leave of absence, etc. Since faculty own the intellectual property rights for much of our work, upon separation we expect to be able to take our data with us, including email (at least a copy of the archived content, if permanent or lingering access to an active scranton.edu email account is not possible).

Note: TAG reviewed a draft of employee separation procedures, prepared by IR, in December 2012. I asked Kate Yerkes about the status of that document, and she responded: “The review of the draft employee separation procedures developed over in IT led to a larger discussion about
As faculty and staff bring their devices to campus, they will want to interact with campus services. Classifying and isolating corporate versus non-corporate devices on the network provides for the ability to selectively allow access to campus services from non-corporate devices through the use of technical controls, such as firewalls. For example, a staff member working from their personally owned machine can access common intranet resources, such as printing services, but cannot connect to the ERP.

When access to restricted resources is required, faculty and staff can leverage virtualization technologies to access the resource. This solution allows the employee to interact with the service they need (in this case, the ERP), without the risk of data loss. Virtual desktops and applications have the added benefit for allowing faculty or staff to utilize University licensed software from their personal devices, without violating the license agreement. For example, a faculty member brings their personal laptop to campus and interacts with common software from their own device, such as a Microsoft Office or the LMS. When the faculty member needs to utilize University licensed software (such as SPSS), they can utilize a virtual application to do so without violating the terms of the license. Should more faculty and staff bring their own primary computing devices, this technology would give them access to a University desktop and applications from their own device at a fraction of the cost of a traditional University issued device. This same approach can be utilized for remote access to restricted services, accomplishing the same goals with users’ home machines.

As BYOD grows and users begin to utilize their own primary computing devices in lieu of an institutionally provided device, reimbursements models will need to be developed. There is currently no clear industry model for this. Reports from other institutions vary widely by amount, employee type, technology and duration [5]. This is likely due to the fact that this model of BYO primary computing device is not widespread. As this grows, considerations for equipment and software reimbursements should be considered.

While the above technical solutions work well for access to intranet and restricted services from personally owned devices, there is still a risk of data loss from public services. Email and other data storage on mobile devices make them likely sources for a data breach as these devices are frequently lost or stolen. Additionally, as more employees are linking University email accounts to their personal phone, data loss can occur on employee separation, as there is currently no mechanism to ensure that institutional data has been removed from the personal device. Investing in a comprehensive mobile device management (MDM) program can help mitigate data loss by ensuring that the appropriate controls are in place and that corporate data can be wiped from devices when necessary.

In a higher education environment, the same MDM controls are not appropriate for everyone. The following three-tiered approach is recommended:
employee separation, given that IT is only one area that would need to have support processes on that topic. HR has assumed leadership for that discussion, and I believe Clay would be your main point of contact there. As the larger policy is developed, support procedures for various units, including IT, would then be solidified.” I will contact Clay Nottelmann in HR for additional information.

Note: The 2014-03 revision of the Information Access Policy refers to “Employee Separation Procedures: Information Resources” as a related document. I was not able to find a final version of this document on the University website or in my TAG notes.

Number: 7    Author: yarmeyk2  Subject: Comment on Text    Date: 5/20/2014 2:00:03 PM
Repeated Q: How does IR define “institutional data”, “corporate data”?

Note: As noted above, data for which faculty hold intellectual property rights (as defined in Appendix VIII of the Faculty Handbook) should not be considered “institutional data” and should not be subject to interference or deletion by IR staff, most especially when stored on a personal device.

Number: 8    Author: yarmeyk2  Subject: Comment on Text    Date: 5/14/2014 10:29:31 AM
Q: What circumstances would necessitate wiping of data? Who determines when data may be deleted from a personal device? What procedures would be followed? Would the user be notified of the intent to delete the data?

Number: 9    Author: yarmeyk2  Subject: Comment on Text    Date: 5/21/2014 9:51:13 AM
Note:
We agree that MDM controls are not appropriate for everyone. MDM constitutes an intrusion to user privacy, which should only be justified in cases of high risk.

“Although security and liability concerns may result in legitimate constraints being placed on usage, in general no conditions or restrictions should be imposed on access to and use of electronic-communications technologies more stringent than limits that have been found acceptable for the use of traditional campus channels of communication.”

Recommendations:
TAG suggests establishing a tier between Optional and Exempt for faculty, whose primary use of University services (email, LMS) is less likely to involve transmission of confidential or restricted data than many staffing areas (e.g., those that frequently interact with Banner). Faculty should be provided with training and best practices for the appropriate use and protected storage of confidential and restricted data (especially student information).
• **Mandatory:** This tier applies to all University issued devices and requires an enrollment in a MDM system that enforces the implementation of technical controls on the device, such as lock code, lock when idle, remote wipe capabilities, device encryption, and potentially even location tracking for locating a lost device.

• **Optional:** This tier applies to all non-corporate owned staff, faculty, and affiliate devices connecting to University systems, including email. Enrollment in the MDM solution is optional but the expectations of minimal technical controls and the requirement to notify PIR of a lost/stolen device are defined in institutional policy. Employees must agree to allow the University to wipe the device when it is lost/stolen or the employee separates from the institution.

• **Exempt:** This tier applies to student devices. This tier has no requirements but offers guidance to students on how to secure their devices.

The tiered system offers a balance between security controls and end user privacy on their personal devices. Users may object to a full wipe of their device on separation in which case, enrollment in the MDM solution is attractive so as to facilitate a partial wipe of the device, removing only corporate data.

One of the more crucial components of an MDM program will be the policy it's based on. An MDM policy should clearly describe the institution’s authority and expectations. In addition, and perhaps more importantly to the success of a MDM program, the policy should be transparent as to what the capabilities the MDM solution provides the University, the data it collects and why it collects it. This will help dispel some of the “big brother” feeling that MDM is sometimes associated with. Stanford University has an excellent example of this on their MDM website\(^1\). Other policies, such as the *Acceptable Use of Computing Resources Policy* and the *Planning and Information Resources Privacy and Confidentiality Statement* may also need updating to incorporate MDM and other BYOD concerns.

The group identified two important services that should be enhanced to provide seamless integration of BYOD into the work environment. Failure to do so will likely inhibit the growth of faculty and staff BYOD on campus. The first service is one of the most common, routine resources utilized by users: a printer. While our current infrastructure works well for corporate laptops and PCs, we lack a solution for printing from mobile and non-corporate devices. Most printers on campus require special drivers that aren’t compatible with mobile devices and introduce security risks for non-corporate workstations. As more of these devices enter our environment, the printing infrastructure needs to be updated to provide a secure and scalable solution.

\(^1\) [https://itservices.stanford.edu/service/mobiledevice/management](https://itservices.stanford.edu/service/mobiledevice/management)
Q: Would "all University issued devices" include faculty desktops, laptops, and tablets?

Note: Enforced activation of location-tracking features raises significant privacy concerns.

Q: Would this apply to other external devices, being used temporarily? For example, would a faculty member visiting family (or another institution) be required to install MDM software on their host's computer in order to be able to check their email?

Repeat Q: What would be the procedures and processes for data deletion? Who would make this decision?

Note: This is highly problematic for faculty. A faculty member should retain control over his/her data on a personal device, even upon separation from the University.

Q: What would be the procedures for objecting to a full wipe? Would the user be notified with sufficient time and information to register an objection prior to data deletion?

Note: The AAUP’s report on Academic Freedom and Electronic Communications states:

"Access to campus computing facilities, and through them to the Internet, represents a vital component of faculty status for most scholars and teachers... While it would be naive to suggest that circumstances might never warrant withdrawal or suspension of digital access, such access may be denied or limited only for the most serious of reasons (for example, creating and unleashing a destructive virus) and only after the filing of formal charges and compliance with rigorous disciplinary procedures that guarantee the protections of academic due process to the accused individual, even where the transgression may not be so grave as to warrant dismissal or suspension.

"A university’s policies must specify the infractions that might warrant such a sanction, recognizing only conduct that jeopardizes the system and the access of others. The policy should also prescribe the procedures to be followed in such a case. In exigent circumstances, a faculty member’s computer access might be summarily and briefly suspended during an investigation of serious charges of abuse or misuse. Any such suspension should, however, be no longer than necessary to conduct the investigation and should be subject to prior internal faculty review."

Note: The Planning & Information Resources Privacy and Confidentiality Statement (revised 2013-06) states that:

"No member of the Information Resources staff outside of the Computer Security Incident Response Team (CSIRT) is authorized to access individual data stores without first obtaining the explicit permission of the account owner. Inspection of data by CSIRT members will be guided by the principles stated above, and is restricted in scope to what is required by the investigative procedures published in the CSIRT Operational Standards manual.

"Exceptions to this inspection policy may be granted when required by extenuating circumstances provided that requests for exceptions are formally documented, submitted to the Information Security Office, and approved by the Chief Information Officer in consultation with the appropriate Vice Presidents and Deans."

Q: Would this be a newly developed policy? If so, what would be its path through University governance?

Note: The Computer Security Incident Response Team (CSIRT) Manual currently posted on IR’s Computing Policies website was last updated 2009-01-27. Its Incident Investigation Process (Section 11.0) includes (in 11.1) the requirement to “communicate with parties that need to be aware of the investigation.” There is no specific mention of communication with the user. The CSIRT Manual also refers to the Information Security Advisory Group (ISAG), which I believe may be defunct. The only mention of it on the University website is a membership list (http://www.scranton.edu/resources/committee_irc.html) that includes several people no longer employed by the University.

Note: Again, this clause is also problematic for faculty, who retain ownership of their work under most circumstances (per Appendix VIII of the Faculty Handbook). A “partial wipe” of only “corporate data” would require very careful technical distinctions, which seems both impractical and unlikely.

Q: Would this be a newly developed policy? If so, what would be its path through University governance?

Note: The AAUP’s report on Academic Freedom and Electronic Communications (updated 2014, http://www.aaup.org/report/academic-freedom-and-
• **Mandatory:** This tier applies to all University issued devices and requires an enrollment in a MDM system that enforces the implementation of technical controls on the device, such as lock code, lock when idle, remote wipe capabilities, device encryption, and potentially even location tracking for locating a lost device.

• **Optional:** This tier applies to all non-corporate owned staff, faculty, and affiliate devices connecting to University systems, including email. Enrollment in the MDM solution is optional but the expectations of minimal technical controls and the requirement to notify PIR of a lost/stolen device are defined in institutional policy. Employees must agree to allow the University to wipe the device when it is lost/stolen or the employee separates from the institution.

• **Exempt:** This tier applies to student devices. This tier has no requirements but offers guidance to students on how to secure their devices.

The tiered system offers a balance between security controls and end user privacy on their personal devices. Users may object to a full wipe of their device on separation in which case, enrollment in the MDM solution is attractive so as to facilitate a partial wipe of the device, removing only corporate data.

One of the more crucial components of an MDM program will be the policy it’s based on. An MDM policy should clearly describe the institution’s authority and expectations. In addition, and perhaps more importantly to the success of a MDM program, the policy should be transparent as to what the capabilities the MDM solution provides the University, the data it collects and why it collects it. This will help dispel some of the “big brother” feeling that MDM is sometimes associated with. Stanford University has an excellent example of this on their MDM website. Other policies, such as the Acceptable Use of Computing Resources Policy and the Planning and Information Resources Privacy and Confidentiality Statement may also need updating to incorporate MDM and other BYOD concerns.

The group identified two important services that should be enhanced to provide seamless integration of BYOD into the work environment.Failure to do so will likely inhibit the growth of faculty and staff BYOD on campus. The first service is one of the most common, routine resources utilized by users: a printer. While our current infrastructure works well for corporate laptops and PCs, we lack a solution for printing from mobile and non-corporate devices. Most printers on campus require special drivers that aren’t compatible with mobile devices and introduce security risks for non-corporate workstations. As more of these devices enter our environment, the printing infrastructure needs to be updated to provide a secure and scalable solution.

---

1 [https://itservices.stanford.edu/service/mobiledevice/management](https://itservices.stanford.edu/service/mobiledevice/management)
electronic-communications-2014) provides 6 recommendations on the development of policies relating to electronic communications:

1. Policies and practices regarding information technology should be within the purview of a representative faculty committee. Any new policy or major revision of an existing policy should be subject to approval by a broader faculty body such as a faculty senate.
2. The faculty committee may be drawn from the faculty senate or elected as an ad hoc committee by the faculty; its members should not be appointed by the administration.
3. Faculty members participating in the committee should be familiar with and informed about relevant developments in communications technology, so that they are able to recognize potential conflicts with principles of academic freedom.
4. The members of the faculty committee should be provided with all relevant contracts and technical materials necessary to make informed decisions about policies governing electronic communications.
5. Whenever policies are proposed or administrative actions taken with respect to information technology that may directly or indirectly implicate academic freedom, faculty members must be consulted.
6. In those institutions with collective bargaining, faculty unions should seek to include in their collective bargaining agreements protections for academic freedom in electronic communications as described in this report.

As a subcommittee to the Faculty Senate Academic Support Committee, TAG serves as a representative faculty committee as described in 1-4. We agree with the AAUP's recommendation, however, that "any new policy or major revision of an existing policy should be subject to approval by a broader faculty body" - in our case, the Faculty Senate as a whole.

Note: While TAG strongly agrees with IR's intentions for transparency, an MDM program as described here would neither dispel a "big brother" feeling nor foster the trust and openness present in a healthy academic environment.

Note: We expect new policies to be consistent with the guiding principles expressed in the Privacy and Confidentiality Policy (2012-05-17), which include:
"Disclosure: Individuals will be notified if their personally identifiable information is being collected and informed of their rights."

Note: The AAUP report on Academic Freedom and Electronic Communications (updated in 2014, http://www.aaup.org/report/academic-freedom-and-electronic-communications-2014) provides recommendations regarding BYOD and other electronic communications policies. These include:

"1. The policy should recognize the value of privacy as a condition for academic freedom and the benefits that privacy and autonomy bring to the individual, to groups, and to the culture of an institution. The institution should recognize that faculty members have a reasonable expectation of privacy in their electronic communications and traffic data.
2. The policy should clearly state that the university does not examine or disclose the contents of electronic communications and traffic data without the consent of the individual participating in the communication except in rare and clearly defined cases. Calls to examine electronic communications or transactional information should consider the special nature of the academy, weigh whether the examination would have disproportionately chilling effects on other individuals or the institution generally, and contemplate alternative or less invasive approaches to preserve privacy in communications...

... 4. Faculty members should be involved in the setting of institutional policies surrounding the monitoring of and access to content and traffic data in electronic communications."
The second important service is file storage. The current file storage solution, RoyalDrive, lacks important features needed in a BYOD world. First, access from mobile devices is restricted to read-only and the solutions that exist are awkward to use and rarely render the content correctly. Second, when working with files from non-mobile devices, users must either download the file from the web interface or form a persistent connection to RoyalDrive to interact with files. This is a security concern as files containing sensitive data have the potential to be accidentally stored locally on the user’s device, which could lead to a data breach as a result of malware or theft of the device. Many free, clouded storage solutions exist today, almost all of them providing mobile-ready features, such as a mobile application and in-browser editing. Lacking a local comparable solution, users are likely to utilize these foreign solutions for their functionality and convenience, resulting in the loss of control over institutional data. This is evident by the fact that IdentityFinder scans have already detected restricted data in some of these products installed on institutionally owned machines. Many of the consumer services offer corporate solutions as well. These solutions provide the same features of the consumer versions, but also allow administrators to set parameters as to how and where data is stored.

While many technical controls and solutions are recommended, end user behavior will pose the greatest risk to data loss in a BYOD world. Developing a comprehensive Information Security training program to build end-user awareness of the risks and benefits of BYOD is recommended. Mandatory security awareness training at other institutions focuses primarily on staff and faculty knowledge workers [5]. Training should focus on building awareness to data exposure risks and how to use corporate solutions to secure and isolate institutional data from personal data.

Strategic Objectives:
- Implement virtual desktop / application technologies to facilitate ubiquitous access to services
- Deploy new network configurations to facilitate connections from non-corporate devices
- Investigate and implement a mobile device management (MDM) solution utilizing a tiered approach
  - Develop transparent MDM policy
  - Update existing policies as needed
- Develop solutions that allow for secure interaction with the corporate environment from non-corporate devices
  - Mobile printing
  - File storage
- Develop a comprehensive Information Security education program to raise end-user awareness of BYOD risks and controls
- Investigate BYOD reimbursement/stipend models
Recommendation:
IR should invite faculty participation in a File Storage work group. TAG is willing to identify and recommend to the Faculty Senate faculty members with specific needs or interest related to this topic.

Note:
Anecdotally speaking, Royal Drive and its permissions provisioning have proved highly problematic in several Library projects.

Note:
End users receive what seem to be mixed messages from IR regarding the appropriate use of Royal Drive. We are instructed to store our University documents on Royal Drive (see for example the 2012 Remote Access Guidelines), and our desktop computers are set up to maintain a persistent connection to Royal Drive, but then we are told that those documents are not secure.

Note: TAG anticipates that IR attempts to require restrictive software on personal devices will push faculty to use third party services such as Gmail, Google Drive, Dropbox, etc for email and file storage. Restrictions on email access may further encourage faculty to simply stop checking their institutional email account. Thus the practical result of a restrictive MDM program may include decreased security and increased difficulty in campus communication.

Q/Note:
Several faculty have reported that a large majority of the hits in their Identity Finder scan results are false positives, and the scan results also include personal documents stored in services that are mapped to a local drive (e.g., Dropbox, Google Drive) -- in other words, information that is PII but personal, not University-related. Has IR confirmed that these scan results included *University data* classified as either confidential or restricted? If so, how did was this confirmed? According the email announcement about Identity Finder from former CIO Jerry DeSanto, "Identity Finder does not allow Information Security staff to read files that are scanned. It only identifies strings of numbers or characters that match potentially restricted data and notes the location of that data."

Furthermore, Identity Finder scans were described to TAG as a way to mitigate security risks (e.g., encouraging the user to either delete or encrypt any unprotected data). It seems disingenuous to then use Identity Finder scan results as a justification for even tighter access controls.

Q: Which administrators would make this decision?

Note:
The Information Classification & Protection Policy lists appropriate controls for access, transmission, and storage of confidential and restricted information. Controls for public information are included but are not explicit (e.g., Storage "As required.")

Recommendation:
TAG supports user education and suggests exploration of effective ways to increase awareness about appropriate data management among faculty and staff.

Q: What/who are considered "staff and faculty knowledge workers"?

Repeated Q: What would be the planned timeline or expected rollout for these objectives?
**Infrastructure Implications**

Much of the technology solutions discussed are reliant on a high performance, reliable infrastructure. The wireless network is the conduit for access to all BYOD services and a dense wireless deployment is required to handle the number of client devices coming onto campus. Our recent investments in a campus-wide wireless upgrade have put us in an excellent position to meet the BYOD demand. That said, as the recommended lab strategy is implemented, wireless client density in classrooms will grow. These areas need to be monitored for saturation and small investments may be needed to increase the number of wireless access points and maintain proper wireless density ratios.

Much of the recommended solutions are based on virtualization technologies, which are highly dependent on infrastructure services. As these solutions grow, a reliable data center network, storage, and server infrastructure will be required. Continual investments in this area will be required to enhance the redundancy and scalability of the infrastructure.

**Strategic Objectives:**
- Monitor wireless access point density ratios and deploy additional access points as necessary
- Continue to invest in data center infrastructure
  - Increase redundancy and scalability of network, storage and server infrastructure
  - Expand virtualization infrastructure

**Support Implications**

Traditional support models focused on supporting devices. As BYOD grows, these support models will evolve to focus on supporting the service rather than the device itself. Many consumers are familiar with the “self help” model so developing “self help” modules or DIY tutorials will likely reduce the BYOD load on support staff. While the number of different devices that users are bringing to campus is vast, the underlying operating systems (Windows, OSX, Android, iOS) are not. Support staff should be familiar with the major operating systems that consumer devices are using in order to better support the services being utilized from these devices.

**Strategic Objectives:**
- Develop “self help” models for services
- Develop support staff skills across the major BYOD operating systems
This page contains no comments
1. Institutional Research Office, ECAR Undergraduate Student Technology Survey, The University of Scranton, September 2013
2. EDUCAUSE: What Does BYOE Mean for IT?, May 2013
   http://www.educause.edu/library/resources/what-does-byoe-mean-it-it-leader-roundtable
3. EDUCAUSE: ECAR Study of Undergraduate Students and Technology, 2013
   http://www.educause.edu/library/resources/ecar-study-undergraduate-students-and-information-technology-2013
   http://www.educause.edu/library/resources/formal-planning-optimizes-byoe-opportunities-university-florida

University of Scranton Information Technology Policies:

Information Access Policy (last revised 2014-03-18? revisions include the removal of procedures - Section IX)
https://royaldrive.scranton.edu/xythoswfs/webui/_xy-55819895_1-t_pJ82zJ7l

Information Classification & Protection Policy (last revised 2013-10-22)
https://royaldrive.scranton.edu/Groups/Planningandinformationsystems/PAIRO/Governance/Policy%20Analysis/Technology%20Policies/Policies/Information%20Classification/Info%20Classification%20Policy%20Revised%20Final%20Oct%202013.pdf?ticket=t_hzRGsmFL

Computer Security Incident Response Team Operational Standards (dated 2009-01-27)
https://royaldrive.scranton.edu/xythoswfs/webui/_xy-28627674_1-t_OndUIFYB

Employee Separation Procedures: Information Resources
Note: I was unable to locate the latest version of this document on the University website.

University Privacy and Confidentiality Policy (2012-05-17)
https://royaldrive.scranton.edu/xythoswfs/webui/_xy-21807668_1-t_hC9B4uyL

Planning & Information Resources Privacy and Confidentiality Statement (revised 2013-06)
https://royaldrive.scranton.edu/xythoswfs/webui/_xy-39612802_1-t_GoH7tPIV

Records Management and Retention Policy (last revised 2011-09)
https://royaldrive.scranton.edu/xythoswfs/webui/_xy-8488481_1-t_kKOUDPg

Remote Access Guidelines (2012-12-12)
https://royaldrive.scranton.edu/xythoswfs/webui/_xy-31489842_1-t_kBoLBGB8