*From Faculty Council Discussion, 12/17/2010:*
Faculty responses to the general question: What issues and concerns would you like to have addressed at the next meeting regarding IT?

- Security on flash drives and laptops of student grades. What special security do we need to have in place on these devices?

Student grades are covered by FERPA and should be protected as sensitive information. Per campus policy Sensitive information that is stored on mobile devices must be encrypted. PGP is the recommended approach for laptop encryption.

Policy summary:
http://help.unc.edu/CCM3_020433

Campus Information Security Homepage:
http://its.unc.edu/InfoSecurity/itssecuity/index.htm

PGP Overview:
http://help.unc.edu/CCM3_021069

Questions can be directed to security@unc.edu, by calling the help desk at 962-HELP, or by reaching out to your department's Information Security Liaison.

- We are told that sensitive info should only be on a univ-owned computer, especially in re mobile devices – security policy seems to be primarily an issue of mobile devices. But if I bought my own personal mobile device, what do I do? What is the reason it must be "university owned"? Also issues of using devices like this with wireless access points; there is a concern about this – how to use, how to assure? VPN client was said to be the solution, but on a trip, I couldn't use my VPN, which was being blocked by the hotel where I was staying. And, when I get on my Outlook email, I see the lock … is it secure without the VPN?

It is not recommended to use a personally owned computer to store sensitive information. This is due to the risk personal use of a computer can introduce to the security of the device along with the inability of the University to ensure effective management of the computer. Policy stipulates that sensitive information only be stored on University owned or managed computers. "University Managed" means using University administered encryption, sensitive client antivirus, and being scanned with the Qualys vulnerability scanning platform.

In light of the University's recent cell phone stipend policy, we strongly recommend that only mobile devices that support full encryption be purchased for personal use if there's any chance that sensitive data may be on the device.

You can use your Outlook client remotely with reasonable assurance of security as the connection between your laptop and the campus server is encrypted with or without VPN. VPN is, of course the preferred method because it secures all communications directed to campus computers that are occurring.

Use VPN when connecting to public wireless to protect UNC-CH transmitted data. Be aware of the risks of hacker exposures such as key stroke logging when using public computers (such as hotel or airport kiosks)

VPN FAQ:
http://help.unc.edu/2502

- Connect Carolina – you can no longer see all the students pictures at the same time, as you could in Faculty Central before. Now you have to go thru each name separately; disconnects students from faculty. Also, large number of clicks required every time you go to Connect Carolina, which is different from Faculty Central .

This is being worked on. The plan is to increase the number of student pictures per "page" from 4 to 40 by the end of Spring semester.

- Email retention/records management. [Thorp says we do have a policy; we can bring.]

A proposed e-mail policy is being finalized by the Office of University Counsel, but is not yet official.

- People in School of Medicine still don't have clarity on what it makes for "your data to be safe." Your databases. Faculty want someone else to tell them their data is safe.

It's difficult to do that right now as we don't know that is true. ITS is working with the School as well as the rest of campus to put additional programs in place which will help improve the safety of campus data. One of the best ways to ensure your data is secure is to make sure you have adequate support by a competent systems administrator. Things that need to occur include appropriate configuration, regular patching, vulnerability scanning, and appropriate access control. For further information, you should check with the School's IT support unit.

- Office of Sponsored Research now requires signing on to data storage plans for research, but this requirement seems to add bureaucracy without adding actual protection/additional clarity to guarantee that I am doing things right.

We need to do more than is being presently addressed on the data storage plans for research. As noted above, ITS is working with campus units to put additional programs in place which will help improve the safety of campus data plus we are working with the Office of Research and Economic Development to better define research data policies.

- Huge issue in a class where my students have submitted final projects as email attachments to me and my doctoral students, and we have divided them up, developed a rubric for grading. And we are discussing it via email – how to grade, students by name – in three different cities – CH, Durham, Cary. Doctoral students don't have univ-owned laptops – how many rules we might be breaking? Yet to find another efficient way to do this work is highly problematic. Our goal right now is to be fair to the students.

Policy would require the personal systems in this case to be scanned, that they run the sensitive client version of antivirus protection software, and the laptops be encrypted as well as using encrypted email to meet policy expectations.

Guideline for securing sensitive information:
http://help.unc.edu/6446

- Number of major changes in IT that have occurred in short time; learning costs for faculty in navigating these all at once – people are feeling that the IT tail wags the dog, they work for IT rather than IT working for them.

Well, obviously that's not the way it should be. It is certainly true there are a number of changes to the campus IT environment underway or in planning . As CIO, I will take the blame for pressing the move to Microsoft Exchange for e-mail and calendaring, although the old Oracle Calendar was at end of life and had to be replaced one way or the other, and we needed a solution with better support for mobile computing devices. However, the other changes are being driven by other forces, not "mandates from IT." For example, ConnectCarolina is being driven by the need to replace the old Student system, which was also at end of life, and the need to modernize Financial and HR/Payroll systems for things like Carolina Counts (Bain). Changes to improve information security are being driven by the need to better protect the systems and data here at Carolina. Changes for Carolina Counts are being mandated by the Board of Trustees and budget pressures due to State mandated budget cuts. The move from Blackboard to Sakai as a learning management system was put forward by the Instructional Computing Coordinating Committee and approved by the IT Executive Steering Committee as a strategically important upgrade for the campus. The existing research computing cluster (Topsail) is at end of life and must be upgraded to allow our researchers to remain competitive for grants. The campus network core was at 1 Gb and needed upgrading to 10 Gb to support leading-edge research needs. And so it goes. Frankly, the overall Carolina IT environment had become "trailing edge" in many ways and in need of fundamental upgrade, which is what we're working through now. We're working to ensure faculty have current IT infrastructure to support their teaching and research needs.

- Connect Carolina – I cannot print out my class rosters! I can't receive attachments via Gmail; it seemed to coincide with Connect Carolina. I see no advantage to CC; no one likes it.

Neither of these seem right. Please contact me, so we can have the right person follow-up.

- Trying to email my students from Connect Carolina at beginning of semester, emails went to the parents!

Perhaps this had something to do with the new proxy capability? At any rate, this doesn't seem right either, so please contact me and we'll have the right person follow-up.

- Students with email addresses other than UNC; how do you verify that the Gmail accounts really are the person they say they are? Would be nice to force all students to use UNC accounts. IT would have to fix it? Students get to say what email they would like to receive. School of Nursing uses Blackboard to email students – students can change the emails that are there thru the univ system. Many don't use the UNC email at all. We take what's in BB as "official" and send emails through this.

We plan to be moving official student e-mail accounts to Microsoft Live@edu by start of fall semester. Students will continue to be able to forward to other accounts, but the UNC e-mail address will be the official contact mechanism and official communications to students should utilize UNC e-mail addresses.

- Issues related to our collaborations with foreign universities when our students are enrolled there; implications for our study abroad programs – security questions.

We have to be responsive to the requirements of the European Union Privacy Directive.

However, we can largely satisfy these concerns by meeting existing campus policy expectations.

Guideline for securing sensitive information:
http://help.unc.edu/6446

- Policies usually talk about “sensitive information” as if all info is “equally sensitive”; I would like to hear some discussion of different degrees of security and have a policy that recognizes that so we don’t have to treat all info we have as equally sensitive.

Sensitive information is largely made up of groups of data that are protected by law, statute, or regulations. The provisions typically mandate that the data must be protected. The protections that are specified in existing campus policy meet the expectations of the laws, statutes, and regulations.

Help page for definition of Sensitive data:
http://help.unc.edu/6475

Guideline for securing sensitive information:
http://help.unc.edu/6446

- Re having this meeting (December Faculty Council) while we are grading . . . we had no information about how to enter the grades into the system until the week that we would have to put that in. We had a very short time to figure it out. Learning on this at the very same moment that people were doing. We needed those workshops 2-3 weeks prior to when we needed to use it.

I will pass on concerns over the timing of the training workshops to the University Registrar.

- Sudden onset of the universal course evaluation system; no notice. I felt a loss of autonomy in my classroom; this felt invasive, I didn’t know who was doing it, not sure who has the data or where it is. We had no role in the questions.

I will pass on concerns over the course evaluation system to the Provost’s Office.

- Instructors didn’t get the email about these that the students got; didn’t get to see the form. Also, FERPA info may not be as sensitive as credit cards, etc. Also, anti-viral protection. How to keep updated? Especially on older computers.

FERPA does not have formal notification requirement but the information must still be protected from inappropriate disclosure. In that respect, it is as sensitive as credit card data. Antivirus is available from the UNC share ware site. The anti-virus client will automatically connect to servers to keep itself updated.

- General anxiety among faculty that tech processes are introduced without sufficient input from faculty in the process; this seems to be accumulating. Faculty are having to spend time to correct issues that could be anticipated. What is the process for faculty input whenever a new process is introduced?

The Faculty Council Executive Committee is discussing the idea of reforming an IT committee which provides advice to the VC for IT and CIO as a way to improve faculty input on key activities and plans.

- If students refuse to use a UNC email address, or faculty do, will they no longer be able to receive our emails?  Do we have to compel all colleagues onto this system?

As mentioned, student e-mail will be outsourced to Microsoft Live@edu over the coming months.  The coming e-mail policy will address options for faculty e-mail.  Alternatives will be allowed, but certain requirements for retention and access will be defined.