EMAIL from Andy Goodenow: SUMMARY OF CHANGES TO FACULTY EMAIL

I wanted to pass on a few updated drafts of email related policy changes. Beth Chancellor, UM System VP of IT, I believe is going to meet with Faculty Senate leadership and others (faculty council/senate, staff council, alumni associations, etc.) to brief also but I wanted to pass on to you directly. The two attached documents have some additional changes highlighted in red. The exact go live dates are still in flux but most of the changes would go in effect mid-December through mid-January.

I would summarize the actions as the following:

- Students – mid to late December after finals, enforcement of a PIN being in use on student phones in order to check email. All faculty/staff already have this requirement currently in place. Communications to students to be sent before Thanksgiving.
- Consistency in approach to all email accounts (employees, students, volunteers, consultants, emeriti, retirees and others acting for or on behalf of the University) – tentatively January 1, size of mailboxes (15GB max), auto deletion policies (3 or 5 years for items in base inbox, sent items or deleted items – still under review by Records Management, Legal and Risk Management on exact length), consistent policies on removing accounts after users separate from the university
- Movement away from email for life with options for certain groups to continue to have sponsored affiliation by individual departments/academic units – tentatively January 1
- All email accounts will be moved from on premise email servers in Columbia to cloud hosted emails at Microsoft – tentatively completed by January 21
    - Most PC users are not affected by the move at all
    - MAC users may have some reconfiguration steps
- UM System IT upgraded to a new Microsoft licensing level called A5. This provides the UM System new security tools supporting Digital Loss Prevention (DLP). Over the next six months, new policies will be put in place which scan email for DCL4 level data. (https://www.umsystem.edu/ums/is/infosec/classification-definitions#dcl4) If that type of data is found, for example a social security number in an email, the user would be presented with a warning email asking them to confirm they intend to send the message or some type of undefined remediation process.

Thanks

Andy Goodenow
Chief Information Officer
University of Missouri-Kansas City