DRAFT Review of PG-55 Update -- April 16th, 2024

Faculty Welfare & Concerns Committee

This is a compilation of questions and concerns from individual faculty, the Faculty Senate Executive Council, and the membership of the Faculty Welfare & Concerns standing committee.

General Issues:

Has this draft been reviewed yet by University Counsel? Some things seem to be dubious in a legal sense and problematical from an enforcement perspective.

Many references are made to "sensitive data" or "sensitive information" throughout all of the documents. The following additional elements are necessary.

- definitions for "sensitive data" and "sensitive information"
- a set of criteria for identifying something as "sensitive"
- who gets to designate something as sensitive
- when public documents are treated as "sensitive" a written explanation of how they could be misused is required to be made public in place of having them available to the public.
- a procedure for periodic review of the categories of information/data designated sensitive so public debate can influence whether a type of information remains "sensitive"

Specific Issues:

Line 66 --"obtain additional resources beyond those allocated"

What does this mean?

Line 81 -- "Personnel should not intentionally access, create, store, or transmit material which Morehead State University may deem to be offensive, indecent, or obscene."

Who will be the arbiter for this?

Line 89 -- "All remote access connections made to internal Morehead State University networks and/or environments must be made through approved, and Morehead State University-provided, virtual private networks (VPNs)."

Does this mean that we cannot access MSU things from our homes?

Line 96 – "Personnel must not share their Morehead State University authentication information, including: o Account passwords, o Personal Identification Numbers"

Some university business (filling out travel requests, contacting payroll, getting help with IT issues) require personnel to share their MSU ID #. This IT policy, though, says we are *never* to share that ID #.

Line 162 -- "Any personal use of Morehead State University provided email should not: Be associated with any political entity, excluding the Morehead State University sponsored PAC."

Enforcement seems problematical. Who will be the arbiter?
Hypotheticals that are all apparently violations of this regulation:

- A staff sponsor of the College Republicans student group sends out an email announcing an ice-cream social.
- A faculty member monitors the KY General Assembly during one of its sessions and reports what they learn from this in an e-mail to colleagues.
- A union organizer on staff sends announcements to campus e-mail addresses.
- The College Democrats want to get the vote out and use campus e-mail to known supporters.

Line 173 -- "Personnel should use discretion in disclosing confidential or internal information in Out of Office or other automated responses, such as employment data, internal telephone numbers, location information or other sensitive data."

When the policies talk about not disclosing "internal telephone numbers" does this mean we aren't supposed to give people our office phone numbers?

Line 186 -- "The Internet must not be used to communicate Morehead State University confidential or internal information, unless the confidentiality and integrity of the information is ensured, and the identity of the recipient(s) is established"

A definition for "confidential information" and "internal information" and a set of criteria for identifying it and who gets to designate something as such are needed. [SEE General Issues]

Line 190 – "Use of the Internet with Morehead State University networking or computing resources must only be used for business-related activities."

"Business-related activities" does not automatically allow for academic freedom in teaching and research. If I connect to the Internet using MSU resources looking for

adaptations of Jane Austen novels, that's not a "business-related activity." It is though a teaching related activity as I prepare for my fall classes.

Line 213 - 225

- "Morehead State University OIT Leadership may choose to execute "remote wipe" capabilities for mobile devices without warning.
- If there is a suspected incident or breach associated with a mobile device, it may be necessary to remove the device from the personnel's possession as part of a formal investigation.
- All mobile device usage in relation to Morehead State University Information Resources may be monitored, at the discretion of Morehead State University OIT Leadership.
- Morehead State University OIT Support for personally owned mobile devices is limited to assistance in complying with this policy. Morehead State University OIT Support may not assist in troubleshooting device usability issues.
- Use of personally owned devices must follow all other Morehead State University policies.
- Morehead State University reserves the right to revoke personally owned mobile device use privileges if personnel do not abide by the requirements set forth in this policy."

Will we need to install special software onto our devices simply to access the network?

Is there going to be a guest network for our personal devices?

If we cannot use our cell phones to monitor emails it will become difficult for those of us teaching online classes. Will the university provide us with a cell phone in addition to our computers for university use?

How will the administration respond when students complain about their professors being inaccessible, as a result of us not being permitted to use personal devices to access the internet or even our MSU devices off campus?

What are departmental social media managers supposed to do when our devices are no longer permitted to be used for MSU purposes (most social accounts are only fully accessible from mobile devices)?

Does this mean that if we use our personal cell phone to access MSU systems (such as e-mail or Blackboard or the LiveSafe App), then MSU could choose to delete everything on our personal cell phone (including all photos and videos, and all names and phone numbers in the Contacts list) at any time, without any advance notice to us?

Is this only if the mobile device is suspected of being used to cause the incident or breach, or does it include situations where the mobile device was simply affected by an incident or breach that was caused by someone else?

Student privacy. If IT can access information on any device connected to its network, what privacy do students have? They can't do their work without a personal device, and their tuition helps pay for the network. Now, after we require them to use personal devices to access a network even when we're in something like a computer lab, we're leaving them open to Big Brother surveillance?

- Scenario: a young female student is in Starbucks, completing homework for her class on her laptop. She's connected to MSU secure and working in the BlackBoard system. While she is working, she gets a text from her friend which pops up on her laptop. This personal text involves an aspect of her reproductive health. She responds to this text using the MSU secure system. What's to stop MSU from getting or handing over that personal text to a zealous Attorney General who is seeking records related to all miscarriages or anything that could be construed as "gender affirming care"?

Remote wiping. The policy doesn't differentiate between mobile devices owned by MSU and those that people bring in. So we're seriously saying that IT is prepared to (and capable of) remotely wiping person devices if people violate IT polices?

- How does IT have control of the operating systems of personal devices?
- Why does IT have control of the operating system of personal devices?
- What gives IT the right to destroy personal property?
- How is this not a violation of rights, especially the rights of students?

Civil asset forfeiture: "If there is a suspected incident or breach associated with a mobile device, it may be necessary to remove the device from the personnel's possession as part of a formal investigation." So IT is now the police? On what authority? And what's will the passive voice here?

Line 227 – "Photographic, video, audio, or other recording equipment, such as cameras in mobile devices, is not allowed in secure areas."

How are "secure areas" defined?

Line 276 --

> "As a convenience to Morehead State University personnel, incidental use of Information Resources is permitted. The following restrictions apply:
>
> - No files or documents may be sent or received that may cause legal action against, or embarrassment to, Morehead State University or its customers."

Who are Morehead State University's "customers"? This is an odd word to use at a not-for-profit educational institution.

How can anybody accurately predict litigation or "embarrassment"?

Is reporting a crime a violation of university policy?

References to institutional “reputation” and “embarrassment” are overly broad and tend toward censorship. Who or what determines a “potential” toward the harm of a reputation?