

Professional Concerns Committee Agenda for January 18, 2018

SU 109
3:15 pm

1. Call to Order, Adoption of Agenda
2. Approval of Minutes from PCC Meeting of December 7, 2017
3. Chair's Report and Announcements
4. Old Business
 - Voting Item: Health Insurance Benefits for Short-Term Non-Tenure-Track Temporary Faculty Members (1 attachment)
 - Voting Item: Withdrawal of Application for Promotion During RPT Process (1 attachment)
 - Voting Item: Acceptable Use Policy (3 attachments)
5. New Business
 - Discussion Item: Shortened Semester Length (1 attachment)
6. Adjournment

Professional Concerns Committee
Minutes for January 18, 2018
SU 109, 3:15 pm

Members in Attendance: S. Alexander, K. Ankem, D. Childs for P. Bills, T. Bonner, T. Bowers, J. Farrar, S. Finke, K. Fuegen, N. Grant, J. Hammons, K. Katkin, A. Miller, G. Newell, S. Nordheim, S. Weiss for T. Songer, M. Torres, M. Washington, L. Wermeling, K. Schwarz for M. Whitson, J. Wroughton.

Guests in Attendance: Sue Ott Rowlands

Members Not in Attendance: A. Al-Bahrani, J. Clarkin, I. Encarnacion, E. Fenton, B. Karrick, M. Kirk, B. Mittal, B. Zembrodt.

1. Call to Order, Adoption of Agenda
 - a. The Meeting was called to order, and the agenda was adopted unanimously.
2. Approval of Minutes from PCC Meeting of December 7, 2017.
 - a. The minutes were approved.
3. Chair's Report and Announcements
 - a. Faculty Senate elections occur before the meeting this month. All faculty may participate at 2:45pm on January 29, 2018.
 - b. Faculty Regent Rick Boyce is not standing for re-election, but that voting is separate from Faculty Senate.
 - c. Faculty Senate Executive Committee discussed the shortened semester, a proposal from SGA for a joint committee on teaching issues.
 - d. President elect Vaidya will be at an open forum for faculty on January 24 in the Otto Budig Theatre. It will be recorded. This is the only faculty role in the presidential transition.
4. Old Business, voting item: Health Insurance Benefits for short-term non-tenure track temporary faculty. The Faculty Senate asked for edits to the language in the PCC proposal. Particularly, concerns were expressed that the proposed Faculty Handbook language was ambiguous about the effect on full-year non-tenure-track faculty members if the ACA is repealed. To clarify that the new language would apply only to temporary non-tenure-track faculty members who work at NKU for less than one year, T. Bonner moved to add the following sentence to current NKU Faculty Handbook Section 1.4: "If the appointment is full time for less than one complete academic year, health insurance is provided by the University to comply with local, state, or federal laws or regulations." Second by T. Bowers. The motion passed without dissent. PCC therefore recommendation that NKU Faculty Handbook Section 1.4, fourth paragraph) should be amended to read as follows:

Non-tenure-track, temporary faculty are provided with Social Security contributions by the University. In addition, health insurance is provided by the University if the appointment is full-time for the complete academic year. If the appointment is full-time for less than one complete academic year, health insurance is provided by the University as needed to comply with local, state, or federal laws or regulations.

K. Katkin will forward this recommendation to Faculty Senate for further action.

5. Old Business, voting Item: Withdrawal of Application for Promotion during the RPT process. Based on discussion at the previous meeting, K. Katkin brought language that would disallow the withdrawal of application. However, committee sentiment at this meeting was much more mixed. Several members expressed the desire to take this to their departments for discussion. G. Newell moved, J. Wroughton seconded a motion to postpone the vote for one month. The motion passed without dissent.
6. Old Business: Acceptable Use Policy. K. Katkin presented a document with comments from PCC. Several additional comments were recommended. S. Finke made a motion to adopt the comments with additions. M. Torres seconded and the motion passed without dissent. K. Katkin said he would make the additions, and then file the amended document with NKU Chief Information Officer Tim Ferguson. The amended documents was subsequently filed with Tim Ferguson, and is attached to these Minutes as filed.
7. New Business: Discussion of shortened semester length
 - a. The committee is divided on this topic with much concern. The proposal will shorten the semester but maintain the minutes of instruction. The proposal will benefit the winter term by not overlapping holidays, and this term has been profitable for NKU.
 - b. Concerns raised were for lab classes because they would almost certainly lose content—number of meeting days matter as much as minutes, scheduling with Fall Break and Thanksgiving during second bi-term courses, and content driven courses requiring longer class periods with shorter student attention spans. Concerns were also raised about the impact of a compressed timeline on visual arts courses and on some traditional classroom courses. There was also a question about the effect on pay schedules.
 - c. A committee member suggested a MW and TR class schedule may also be a possibility.
 - d. There seems to be interest in the proposal amidst the concerns. There is no complete proposal to evaluate at this time.
8. The meeting was adjourned by K. Katkin.

Submitted,
John Farrar

MEMORANDUM

To: Tim Ferguson, Chief Information Officer, NKU

From: Ken Katkin, Chair, Faculty Senate Professional Concerns Committee (PCC)

Re: PCC Comments in Response to NKU's "Acceptable Use Policy" Proposal

Date: Jan 23, 2018

I am the Chair of the Professional Concerns Committee (PCC) of the NKU Faculty Senate. At its meetings of December 7, 2017 and January 18, 2018, the PCC discussed the proposed revisions to NKU's "Acceptable Use Policy" that have been released for public comment. On behalf of the PCC, I hereby offer the following comments on the draft Policy proposal entitled "Acceptable Use Policy."

(1) On Page Two, just above the header "Individual Rights," the generic phrase "Kentucky Public Records Law" should probably be replaced with the more specific phrase "Kentucky Open Records Act," which is the name of the Kentucky statute that governs access to public records.

(2) On Page Two or Three, in the list of "Individual Rights," an additional bullet point should be added that provides: "Individuals have the right to receive training that will facilitate compliance with all responsibilities and restrictions set forth in this policy."

(3) On Page Three, just below the header "Individual Responsibilities," the words "operational or copyrighted" should be deleted. The word "operational" is too vague to have any meaning. The word "copyrighted" could apply to substantially all content on all university computers, including faculty members' teaching materials or published articles—or even to Web content such as course descriptions or student handbooks that should be readily available to the public.

(4) On Page Three, just below the header "Individual Responsibilities," the second sentence (which begins with the words "Per Northern Kentucky University's Information Security Policy. . .") should be replaced with a sentence that simply states "Highly sensitive data must be stored in compliance with Northern Kentucky University's Information Security Policy," followed by a hyperlink. This change is needed because NKU's Information Security Policy will presently be changing. After the change, the detailed prescriptions in the present draft Acceptable Use policy may no longer reflect the revised Information Security Policy.

(5) On Page Three, the first bullet point below the header "Individual Responsibilities" begins with the words "Maintaining current operating system. . . ." Under the same header, the third bullet point begins with the words "Installing, using, scanning," Both of these bullet points should be deleted, because the responsibility to install software, firmware, and virus protection lies with the University, and not with the individual user.

(6) On Page Three, the eighth bullet point below the header “Individual Responsibilities” begins with the words “Using only the access and privileges. . . “ In this bullet point, the following additional language should be added to clarify:

However, Incidental personal use of university technology resources is not prohibited by this policy. Incidental personal use is an accepted and appropriate benefit of being associated with NKU’s rich technology environment. Appropriate incidental personal use of technology resources does not result in any measurable cost to the university, and benefits the university by allowing personnel to avoid needless inconvenience. Incidental personal use must adhere to all applicable university policies. Under no circumstances may incidental personal use involve violations of the law, or interfere with the fulfillment of an employee’s university responsibilities.

This language is adopted from language set forth in Indiana University’s Acceptable Use Policy, <https://policies.iu.edu/policies/it-01-appropriate-use-it-resources/index.html>, and in the policy of many other universities. It also reflects current salutary practice at NKU, as set forth on Pages 148-149 of the NKU Faculty Handbook (“the use of personal office space, local telephone, library resources and personal computer equipment incidental to outside activities . . . are permitted under the University’s Ethical Principles and Code of Conduct . . . and the Faculty Handbook”). This principle should be stated explicitly in our Acceptable Use policy.

(7) On Page Four, the third bullet point prohibits users from extending the network via services or devices. The PCC does not understand why this restriction is necessary or desirable.

(8) On Page Four, the sixth bullet point prohibits users from introducing viruses to the network. The word “intentionally” should be added as the first word of the bullet point, which would now begin with “Intentionally introduce. . . .”

(9) On Page Four, the third-from-last bullet point concerns copyright infringement. Its use of the word “per” seems to be a typographical error that may reverse the intended meaning of the provision. The phrase “per copyright law” should be replaced with the phrase “in violation of copyright law.”

(10) On Page Four, in the third sentence below the header “University Processes/Privacy,” the words “are considered university property” should be deleted. The sentence would thus read: “In addition, all documents created, stored, transmitted, or received on university computers and networks may be subject to monitoring by systems administrators.” Because Intellectual Property is governed by other policies that generally do NOT vest ownership of faculty members’ work in the University, it is inaccurate and undesirable to characterize the university’s right to surveil users’ files as a “property” interest in the contents of documents stored on university computers.

(11) On Page Four, in the second bullet-point, the words “bona fide” should be inserted before the word “investigation,” so that the bullet-point would now begin with the words: “In connection with a bona fide investigation by the university. . . .”

(12) On Page Five, following immediately following the header “University Rights,” the long sentence should be divided into two sentences as follows. First, before the list of bullet points, the sentence should simply read: “When compelled by court order. . . .” This list of bullet points should then follow those five words. After the list of bullet points, a concluding sentence should state: “In the absence of a court order, any such actions shall be taken only after the area vice president appropriate to the circumstances makes a written determination that there is an urgent and compelling need to do so.” These changes would clarify that these actions may not be taken without a court order or VP determination, and to impress upon each individual VP the seriousness of granting such a determination.

(13) On Page Five, under the header “University Rights,” the first bullet-point governs “Compensated outside work.” A second sentence should be added to this bullet-point to clarify that: “Work completed in satisfaction of a faculty member’s obligation to produce teaching materials, scholarly or creative activity, or service to the community is not considered ‘outside work,’ even if such work is compensated.” This sentence is needed to clarify that faculty members may use NKU resources to write scholarly books, or commissioned journal articles, for example. These works are compensated by outside entities, but are part of the ordinary scholarly work that is expected from NKU faculty members.

(14) On Page Five, under the header “Enforcement: Misuse of Electronic Resources,” the final bullet point states that “civil and/or legal action may be initiated.” Because this provision is triggered by “violations of university policies” rather than by “violations of law,” this bullet point should be deleted or amended. The University would not be justified in bringing a civil or legal action in an instance where no law has been violated. For the same reason, the word “fines” should be deleted from the preceding and succeeding bullet points. Without prevailing in a civil action, the University has no authority to levy “fines” against its employees, and should not idly threaten to do so.

(15) On Pages Five and Six, under the header “Enforcement: Misuse of Electronic Resources,” the draft policy threatens that faculty members found to have violated this policy may be subject to termination of employment. The draft policy does not address the procedures by which guilt might be assessed or penalties meted out. To avoid any ambiguity, language should be added immediately following the list of bullet points at the top of Page Six—and before the three subsequent paragraphs—to clarify that:

Such penalties shall be levied through ordinary disciplinary procedures set forth in other official University personnel policy documents, such as the NKU Personnel Policies and Procedure Manual, the NKU Faculty Policies and Procedures (the “Faculty Handbook”), or the Chase College of Law Faculty Policies and Procedures (the “Chase Faculty Handbook”).

(16) Throughout the document, a number of the hyperlinks are broken or incorrect. The PCC recommends that all hyperlinks be checked (and corrected as needed) before the policy is finalized.

Thank you for taking these comments into consideration.

CATEGORY:	University policy
POLICY STATUS:	Approved

POLICY TITLE: ACCEPTABLE USE POLICY
POLICY NUMBER:
POLICY ADDRESS:
POLICY PURPOSE: Describes expectations to anyone using NKU computing resources.
APPLIES TO: Faculty, staff and students.

CONTENTS:

POLICY STATEMENT

1.0 Overview:

This policy applies to all persons using and/or attempting to access or use Northern Kentucky University computing resources. This includes but is not limited to University students, faculty and staff, authorized University guests, and all persons authorized for access or use privileges by the University, hereafter referred to as ‘users’.

2.0 Scope:

Computing resources covered by this policy include, without limitation:

- All University owned, operated, leased or contracted computers, networking, telephone, mobile devices, copiers, media, and information resources, whether they are individually controlled, shared, standalone or networked
- All information and data maintained in any form and in any medium within the University's computer resources
- All University voice and data networks, telephone systems, telecommunications infrastructure, communications systems and services, and physical facilities, including all hardware, software, applications, databases, cellular devices, mobile devices, and storage media.

Individual areas (e.g., departments, colleges) within the University may define supplemental policies or conditions of acceptable use for electronic resources under their control. These additional policies or conditions must be consistent with this policy but may provide additional detail, guidelines and/or restrictions. This policy will supersede any inconsistent provision of any departmental policy or condition.

Four general principles underlie eligibility and acceptable-use policies for information technology:

- University information technology is for University faculty, students, and staff to use for core University purposes
- Any use counter to this, or which interferes with core use by others, is unacceptable
- Some applications of University information technology may be unacceptable even if they serve core purposes
- Unauthorized access or use of University computing resources or data is strictly prohibited.

3.0 Policy: Confidentiality

All users with access to confidential data are to utilize all appropriate and

accepted precautions to maintain the accuracy, integrity, and confidentiality of the data and ensure that no unauthorized disclosures occur. Individuals are responsible to take appropriate action to insure the protection, confidentiality, and security of the University's information. Individual student records are subject to special protection as specified in the Family Educational Rights and Privacy Act of 1974 (<http://www.ed.gov/offices/OM/ferpa.html>). Such data (e.g. SSN's) must be handled with a high degree of security and confidentiality in compliance with policies, regulations, and laws, and must only be collected and stored when it is essential for approved business processes or to meet legal requirements. Violation of usage may be cause for dismissal from employment, disciplinary actions, and civil or criminal penalties.

User Rights

The University provides electronic resources to users to effectively perform their job duties. The University will not routinely monitor an individual user's electronic data, software, or communication files, unless warranted by probable cause.

All users have the following rights:

- All users are granted access to and permitted use of the University's Electronic resources as related to specific purposes based on the user's particular needs or classification
- Users have the authority to read, write, edit, or delete information in files or databases, as established by the designated roles and responsibilities of the user, and according to the University Records Management policies
- All users are provided with the University's on-campus network access, including electronic mail ("email") and Internet access.

User Responsibilities

Data that is considered critical/sensitive or regulated/operational or copyrighted must be securely housed within the IT data center or within approved safe electronic storage media. Each user shall be responsible for the security and integrity of information stored on his or her personal desktop system, laptop, storage, and mobile devices. This includes:

- Maintaining the currency of operating system, software, and firmware, as supported by the University
- Strictly following all data protection guidelines, including FERPA guidelines
- Installing, using, scanning, and regularly updating virus protection software (see NKU Anti-Virus Policy)
- Making regular backups of information and files
- Controlling and securing physical and network access to Electronic resources and data
- Abiding by password protection practices, by choosing appropriate passwords, protecting the security of passwords, and changing passwords on a regular basis
- Using only the access and privileges associated with his or her computer account(s) and utilizing those account(s) for the purposes for which they were authorized

-
- Respecting and honoring the rights of other individuals, with regard to intellectual property, privacy, freedom from harassment, academic freedom, copyright infringement, and use of electronic resources

A user suspecting that his or her access has been compromised is to report it to IT Security via the IT Service Center and change passwords and access modes immediately.

User Restrictions Users may NOT do the following:

- Provide access or passwords to any user not authorized for such access
 - Make use of accounts, passwords, privileges or Electronic resources to which they are not authorized
 - Tamper with, modify, or alter restrictions or protection placed on their accounts, the University system, or network facilities
 - Extend the network by introducing a hub, switch, router, wireless access point, or any other service or device that provides more than one device to the University network without consent and approval from IT network and security management
 - Use the University's Internet access or network in a malicious manner to alter, destroy, or improperly access any information available on the Internet or on any network accessible through the Internet
 - Share remote access authentication with other users or non-users
 - Introduce, create or propagate computer viruses, worms, Trojan Horses, or other malicious code to University Electronic resources
 - Use knowledge of security or access controls to damage computer and network systems, obtain extra Electronic resources, or gain access to accounts, data or information for which they are not authorized
 - Eavesdrop or intercept transmissions, emails or messages not intended for them
 - Physically damage or vandalize electronic resources
 - Attempt to degrade the performance of the system or to deprive authorized users of Electronic resources or access to any University Electronic resources
 - Alter the source address of messages, or otherwise forge email messages
 - Send email chain letters or mass mailings for purposes other than official University business
 - Use internal or external systems to relay mail between two non-University email systems
 - Engage in activities that harass, degrade, intimidate, demean, slander, defame, interfere with, or threaten others
 - Communicate or act on behalf of the University via any computing or internet form unless they have the authority to do so
 - Install Servers that have not been identified to and approved by IT Services
 - Install network game servers, unless authorized by the office of the CIO
 - Install and/or download music, video, other copyright media or software per copyright laws
-

-
- Obtain access to NKU networks and computing devices if not an authorized user
 - Copy or distribute sensitive data regarding students, faculty or staff without proper and approved safe storage devices, and only as required by the job duties.

University Processes

Users should be aware that centralized data, software, and communications files are regularly copied to backup tapes and stored for potential recovery. All activity on systems and networks may be monitored, logged, and reviewed by system administrators and/or governmental agencies, or discovered in legal proceedings or open records procedures. In addition, all documents created, stored, transmitted or received on University computers and networks are considered University property, and may be subject to monitoring by systems administrators.

University Rights

The University reserves the right to:

- Access, monitor and disclose the contents of an individual user's account(s)
- Access, monitor and disclose the activity of an individual user's account(s)
- Access any University-owned technology resource and any non-University-owned technology resource, on University property, connected to University networks.

This action may be taken:

- To maintain the network's integrity
- To maintain the rights of others authorized to access the network
- To maintain the security of a computer or network system
- To prevent misuse of University resources
- To support the business of the University if impacted due to the sudden death, leave of absence, or incapacitation of an employee.

Any such action will be taken only after obtaining approval from the area vice president appropriate to the circumstances, or when compelled by court order, or when there is deemed to be an urgent and compelling need to do so. The university may terminate access upon misuse.

Copyrights and Licenses

Software and media may not be copied, installed or used on University Electronic resources except as permitted by law. Software installations must be communicated to and approved by IT Services. Software, subject to licensing, must be properly licensed, and all license provisions (including installation, use, copying, number of simultaneous users, terms of the license, etc.) must be strictly adhered to. Creating or using unauthorized copies of software or media is a violation of this University policy. Such conduct may be in violation of the law and could subject the user to disciplinary action, fines, and/or imprisonment.

All copyrighted information retrieved from Electronic resources, or stored, transmitted or maintained with Electronic resources, must be used in conformance with applicable copyright and other laws. Copied material, used legally, must be properly attributed in conformance with applicable legal and professional standards. See U.S. Copyright laws (<http://www.copyright.gov/title17/>).

Non-Organizational Use

Users may not use Electronic resources for:

- Compensated outside work, except as authorized by the Provost/Vice President for Academic Affairs pursuant to an approved grant or sponsorship agreement
- The benefit of organizations not related to the University, except those authorized by a University dean, or the director of an administrative unit, for appropriate University-related service
- Personal gain or benefit
- Political or lobbying activities not approved by the Office of the Provost/Vice President for Academic Affairs
- Private business or commercial enterprise
- Illegal activities.

University Electronic resources may not be used for commercial purposes, except as specifically permitted under other written policies of the University. Any such commercial use must be properly related to University activities and provide for appropriate reimbursement to the University for taxes and other costs the University may incur by reason of the commercial use.

4.0 Enforcement:

Misuse of Electronic resources

In any case where Acceptable Use comes into question, management of the University reserves the right to determine what is appropriate and acceptable and what is not. Violations of University policies will result in one or more of the following actions:

1. User will be notified that the misuse must cease and desist.
2. User will be required to reimburse the University or pay for Electronic resource(s).
3. User will be denied access to the Electronic resource(s), temporarily or permanently.
4. The appropriate University disciplinary action will be initiated. Actions may include sanctions, up to and including, termination of employment or expulsion, legal actions, fines, etc.
4. Civil and/or legal action may be initiated.
5. Law enforcement authorities may be contacted to initiate criminal prosecution.

All users are encouraged to report to the IT Service Center any suspected violations of University computer policies, such as unauthorized access attempts. Users are expected to cooperate with system administrators during investigations of system abuse. Failure to cooperate may be grounds for disciplinary action,

expulsion, legal actions, fines and other actions as deemed necessary. If persuasive evidence exists of the misuse of Electronic resources and that evidence points to a particular individual, IT management must be notified immediately.

The University retains final authority to define what constitutes proper use and may prohibit or discipline use the University deems inconsistent with this or other University policies, contracts and standards.

TECHNICAL MAINTENANCE AND ADMINISTRATIVE RIGHTS University System Administrators and Authorized IT Staff

All system administrators (those individuals charged with the daily administration of Computer resources within a unit of the University) will preserve users' privileges and rights of privacy consistent with this and other applicable University policies. Access privileges will be used only to the extent required by the performance of job responsibilities. Administrators will take all reasonable steps necessary to preserve the availability and integrity of Electronic resources, including:

- Reject or destroy email messages and email attachments that are suspected of containing malicious code, phishing, viruses or worms
- Eliminate sources of malware, viruses, phishing, or other forms of security threats, including shut down of ports, usernames, passwords, and equipment, until it is safe to reconnect to network
- Investigate and report suspected violations of University policies or procedures □ Restore the integrity of the affected system in case of abuse, virus or other malfunction
- Ensure conformance with legal obligations as they pertain to the administration of Electronic resources.

Physical Access Control

Direct physical access to certain Electronic resources such as servers, data networking devices, and telecommunications switches is restricted to authorized personnel only. If University personnel believe that an unauthorized person gained or attempted to gain access to a server or network equipment room, they must contact the Office of Information Technology and/or University's Department of Public Safety immediately.

Rooms containing critical Electronic resources must be secured, and access to those rooms must be limited to authorized users only. All entrances to such rooms must be closed and locked at all times. Alarms, sensors and other types of physical security systems must be utilized to further secure these facilities and to detect and report emergency conditions that might occur. Appropriate fire suppression systems must be in place. Authorized personnel may be granted access to server or network equipment rooms through the issuance of ID cards or keys or through the use of passwords or other access codes, and access is restricted to role-based authority.

5.0 Policy Amendments:

The University reserves the right to change the policies, information,

requirements and procedures, announced in this policy, at any time. Changes required by University contractual commitments shall be effective and binding to users upon execution of any such contract by the University. A user shall be deemed to have accepted and be bound by any change in University policies, information, requirements or procedures, announced in this policy, at any time following announcement or publication of such change.

**EXCLUSIONS OR
SPECIAL
CIRCUMSTANCES:
CONSEQUENCES:**

RESPONSIBLE Information Technology

OFFICE:

APPROVED BY:

APPROVED ON:

EFFECTIVE ON: 9/1/2008

REVIEW CYCLE:

BACKGROUND:

RELATED

DOCUMENTS:

DEFINITIONS:

REVIEW/CHANGE

HISTORY:

ACCEPTABLE USE

POLICY NUMBER: RESERVED FOR FUTURE USE

POLICY TYPE: HYBRID

RESPONSIBLE OFFICIAL TITLE: SENIOR VICE PRESIDENT, ADMINISTRATION & FINANCE

RESPONSIBLE OFFICE: OFFICE OF INFORMATION TECHNOLOGY

EFFECTIVE DATE: UPON APPROVAL

NEXT REVIEW DATE: APPROVAL PLUS FOUR YEARS

SUPERSEDES POLICY DATED: [CLICK HERE TO ENTER A DATE.](#)

REQUIRES BOARD OF REGENTS APPROVAL: YES NO

I. POLICY STATEMENT

Overview:

A trusted and effective information technology environment is vital to the mission and core values of Northern Kentucky University. NKU provides a wide variety of institutional electronic systems, computer services, networks, databases, and other resources. These are intended to support the educational, research, and work activities of members of the university's academic community and their external collaborators, to support the operations of the university, to provide access to services of the university and other publicly available information, and to ensure a safe and secure IT operating environment to all members of the university community.

This policy is to define and promote the responsible use of information technology at NKU. Access to and usage of information technology resources necessitates certain expectations and responsibilities for all users.

Within NKU's IT environment, additional rules will apply to specific computers, computer systems, software applications, databases or networks or to college/departmental rules and activities. Departmental rules must be consistent with this policy, but may also impose additional, or more specific requirements or responsibilities on individuals. This policy will supersede any inconsistent provision of any departmental policy or rule.

Computing resources covered by this policy include, without limitation:

- All university owned, operated, leased or contracted computers, networking, telephone, mobile devices, copiers, printer, media, and information resources, whether they are individually controlled, shared, standalone or networked
- All information and data maintained in any form and in any medium within the university's computer resources including managed server ("J" / "K") drives, or the Microsoft OneDrive service, provided through NKU.
- All university voice and data networks, telephone systems, telecommunications infrastructure, communications systems and services, and physical facilities, including all hardware, software, applications, databases, cellular devices, mobile devices, and storage media.

Three general principles underlie eligibility and acceptable-use policies for information technology:

- University information technology is for university faculty, students, and staff to use for core university purposes
- Some applications of University information technology may be unacceptable even if they serve core purposes
- Unauthorized access or use of university computing resources or data is strictly prohibited.

II. ENTITIES AFFECTED

Scope / Applicability:

This policy applies to all persons using and/or attempting to access or use Northern Kentucky University computing resources regardless of whether these resources are accessed from NKU's campus or from remote locations. This includes but is not limited to University students, faculty and staff, authorized University guests, alumni, affiliates, agents of the administration, organizations accessing network services, and all individuals authorized for access or use privileges by the University.

III. RESPONSIBILITIES

Policy: Confidentiality

All individuals with access to confidential data are to utilize all appropriate and accepted precautions to maintain the accuracy, integrity, and confidentiality of the data and ensure that no unauthorized disclosures occur. Individuals are responsible to take appropriate action to insure the protection, confidentiality, and security of the University's information. Individual student records are subject to special protection as specified in the Family Educational Rights and Privacy Act (FERPA) of 1974

(<https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html?src=rn>). Such data (e.g.SSN's) must be handled with a high degree of security and confidentiality in compliance with policies, regulations, and laws, and must only be collected and stored when it is essential for approved business processes or to meet legal requirements. Violation of usage may be cause for dismissal from employment, disciplinary actions, and civil or criminal penalties.

- Refer to the Information Security Policy (http://policy.nku.edu/content/dam/policy/docs/a-through-z-policy-finder/PROVED_InformationSecurity7-2-2016.pdf) for specific details to ensure confidentiality and integrity of university data.
- The university will access IT resources as necessary for system maintenance, including security measures. The Network Operations Center (NOC) and formally designated IT managers are authorized to monitor network traffic for malicious activity or suspicious patterns.
- The University's routine operation of IT resources may result in the creation of log files and other records about usage. This information is necessary to analyze trends, balance traffic, and perform other essential administrative tasks. IT may store incident related data as required. IT may store aggregate data and usage logs for operational, compliance, and statistical purposes.
- The university may be compelled by a court of competent jurisdiction or a request for public records, to disclose individuals' electronic records in response to various legal requirements, including subpoenas, court orders, search warrants, discovery requests in litigation and requests for public records under the Kentucky Public Records Law or by request of the Office of General Counsel.

Individual Rights:

Northern Kentucky University provides electronic resources to individuals to effectively perform their job duties. The university will not routinely monitor an individual's electronic data, software, or communication files, unless warranted by probable cause.

All individuals have the following rights:

- All individuals, including faculty, staff, students, authorized university guests, alumni, affiliates, agents of the administration and community members are granted access to and permitted use of the

university's electronic resources as related to specific purposes based on the individual's particular business needs or classification

- Individuals have the authority to read, write, edit, or delete information in files or databases, as established by the designated roles and responsibilities of the individual, and according to the University Records Management policies (<http://policy.nku.edu/content/dam/policy/docs/a-through-z-policy-finder/Administrative-Regulations/Records%20Management%20Policy.pdf>).
- All individuals are provided with the university's on-campus network access, including electronic mail ("email") and internet access.

Individual Responsibilities:

Data that is considered critical/sensitive or regulated/operational or copyrighted must be securely housed within the IT data center or within approved safe electronic storage media. Per Northern Kentucky University's Information Security Policy, http://policy.nku.edu/content/dam/policy/docs/a-through-z-policy-finder/APPROVED_InformationSecurity7-2-2016.pdf the university forbids the storage of highly sensitive data on any data storage device or media other than a centrally managed server ("J" / "K" drives), or the Microsoft OneDrive service, provided through NKU. Storing such data on hard drives (laptops, desktops, tablets, etc.) can subject the data to breach by viruses, malware, hacking, physical loss of device, etc.

If an individual is required to store highly sensitive data for a business need that is outside NKU managed networks, that individual must obtain permission from the Office of the CIO and the area Vice President. The written request for authorization must state the unique business need, the type of data that will be stored, the type of data storage device that will be used, and the mitigating controls that will be employed to protect the highly sensitive data. Each individual shall be responsible for the security and integrity of information stored on his or her personal desktop system, laptop, storage, and mobile devices. This includes:

- Maintaining current operating system, software, and firmware, as supported by the university
- Strictly following all data protection guidelines, including FERPA guidelines (<https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html?src=rn>)
- Installing, using, scanning, and regularly updating virus protection software (see NKU Anti-Virus Policy <http://policy.nku.edu/content/dam/policy/docs/a-through-z-policy-finder/Antivirus%20Policy.pdf>)
- All Individuals accessing or storing university data on personally owned devices, such as mobile phones, tablets, computers, are responsible to ensure security of the data through strong passwords and encryption to minimize risks of data leaks. Protected data may not be stored on personally owned devices unless effective security controls have been implemented to protect the data.
- Making regular backups of information and files
- Controlling and securing physical and network access to electronic resources and data
- Abiding by password protection practices, by choosing appropriate passwords, protecting the security of passwords, and changing passwords as needed
- Using only the access and privileges associated with his or her computer account(s) and utilizing those account(s) for the purposes for which they were authorized
- Respecting and honoring the rights of other individuals, with regard to intellectual property, privacy, freedom from harassment, academic freedom, copyright infringement, and use of electronic resources
- An individual suspecting that his or her access has been compromised is to report it to IT Security via abuse@nku.edu or the IT Help Desk and change passwords and access modes immediately.

Individual Restrictions

Individuals may NOT do the following:

- Provide access or passwords to any individual not authorized for such access

- Make use of accounts, passwords, privileges or electronic resources to which they are not authorized
- Tamper with, modify, or alter restrictions or protection placed on their accounts, the university system, or network facilities
- Extend the network by introducing a hub, switch, router, wireless access point, or any other service or device that provides more than one device to the university network without consent and approval from IT network and security management
- Use the university's internet access or network in a malicious manner to alter, destroy, or improperly access any information available on the internet or on any network accessible device
- Share remote access authentication with other individuals
- Introduce, create or propagate computer viruses, worms, Trojan horses, or other malicious code to university electronic resources
- Use knowledge of security or access controls to damage computer and network systems, obtain extra electronic resources, or gain access to accounts, data or information for which they are not authorized
- Eavesdrop or intercept transmissions, emails or messages not intended for them
- Physically damage or vandalize electronic resources
- Attempt to degrade the performance of the system or to deprive authorized individuals of electronic resources or access to any university electronic resources
- Alter the source address of messages, or otherwise forge email messages
- Send email chain letters or mass mailings for purposes other than official university business
- Use internal or external systems to relay mail between two non-university email systems
- Communicate or act on behalf of the university via any computing or internet form unless they have the authority to do so
- Install physical or virtual servers that have not been identified to and approved by the office of the CIO
- Install network game servers, either virtual or physical, unless authorized by the office of the CIO
- Install and/or download music, video, other copyright media or software per copyright laws
- Obtain access to NKU networks and computing devices if not an authorized individual
- Copy or distribute sensitive data regarding students, faculty or staff without proper and approved safe storage devices, and only as required by the job duties

University Processes/ Privacy Individuals should be aware that centralized data, software, and communications files are regularly backed up to a storage area network (SAN) and stored for potential recovery. All activity on systems and networks may be monitored, logged, and reviewed by system administrators and/or governmental agencies, or discovered in legal proceedings or open records procedures. In addition, all documents created, stored, transmitted or received on university computers and networks are considered university property, and may be subject to monitoring by systems administrators. The university will never disclose contents of communications to an outside entity unless formally instructed to do so by the Office of Legal Affairs and General Counsel and:

- When required by law. If necessary to comply with the applicable legal requirement, such disclosures may occur without notice to the individual or without the individual's consent, as determined by the Office of Legal Affairs and General Counsel.
- In connection with an investigation by the university or an external legal authority into any violation of law or of any university policy, rule or ordinance. When the investigational process requires the preservation of the contents of an individual's electronic records to prevent their destruction, the Office of Legal Affairs and General Counsel may authorize such an action.
- If appropriate university personnel determines that access to information in an employee's electronic account or file is essential to the operational effectiveness of a university unit or program and the employee is unavailable or refuses to provide access to the information.

- If the university receives an appropriately prepared and presented written request for access to information from the lawful representative of a deceased or incapacitated individual.

University Rights After obtaining approval from the area vice-president appropriate to the circumstances, or when compelled by court order, or when there is deemed to be an urgent and compelling need to do so. The university reserves the right to:

- Access, monitor and disclose the contents of an individual's account(s)
- Access any university-owned technology resource and any non-university owned technology resource, on university property, connected to university networks.
- Take this action:
 - To maintain the network's integrity
 - To maintain the rights of others authorized to access the network
 - To maintain the security of a computer or network system
 - To prevent misuse of university resources
 - To support the business of the university if impacted due to the sudden death, leave of absence, or incapacitation of an employee.
- Terminate access upon misuse.

Non-Organizational Use

Users may not use electronic resources for:

- Compensated outside work, except as authorized by the Provost/Vice President for Academic Affairs pursuant to an approved grant or sponsorship agreement
- The benefit of organizations not related to the University, except those authorized by a University dean, or the director of an administrative unit, for appropriate University-related service
- Personal gain or benefit
- Political or lobbying activities not approved by the Office of the Provost/Vice President for Academic Affairs
- Private business or commercial enterprise
- Illegal activities.

University electronic resources may not be used for commercial purposes, except as specifically permitted under other written policies of the University.

Any such commercial use must be properly related to University activities and provide for appropriate reimbursement to the University for taxes and other costs the University may incur by reason of the commercial use.

Enforcement: Misuse of Electronic resources

In any case where Acceptable Use comes into question, university management reserves the right to determine what is appropriate and acceptable and what is not. Violations of university policies will result in one or more of the following actions:

- Individual will be notified that the misuse must cease and desist.
- Individual will be required to reimburse the university or pay for electronic resource(s).
- Individual will be denied access to the electronic resource(s), temporarily or permanently.
- The appropriate university disciplinary action will be initiated. Actions may include sanctions, up to and including, termination of employment or expulsion, legal actions, fines, etc.
- Civil and/or legal action may be initiated.

- Law enforcement authorities may be contacted to initiate criminal prosecution.

All individuals are encouraged to report to abuse@nku.edu or the IT Help Desk any suspected violations of university computer policies, such as unauthorized access attempts.

Individuals are expected to cooperate with system administrators during investigations of system abuse. Failure to cooperate may be grounds for disciplinary action, expulsion, legal actions, fines and other actions as deemed necessary. If persuasive evidence exists of the misuse of electronic resources and that evidence points to a particular individual, the Office of the CIO must be notified immediately.

The university retains final authority to define what constitutes proper use and may prohibit or discipline improper use the university deems inconsistent with this or other university policies, contracts and standards.

Copyrights and Licenses

Software and media may not be copied, installed or used on university electronic resources except as permitted by law.

- Software installations must be communicated to and approved by IT Services.
 - Proof of License, outlining the type and number of installations must be provided to the Office of Information Technology.
- Software, subject to licensing, must be properly licensed, and all license provisions (including installation, use, copying, number of simultaneous users, terms of the license, etc.) must be strictly adhered to.
- Creating or using unauthorized copies of software or media is a violation of this university policy. Such conduct may be in violation of the law and could subject the user to disciplinary action, fines, and/or imprisonment.
- All copyrighted information retrieved from electronic resources, or stored, transmitted or maintained with electronic resources, must be used in conformance with applicable copyright and other laws.
- Copied material, used legally, must be properly attributed in conformance with applicable legal and professional standards. See U.S. Copyright laws (<http://www.copyright.gov/title17/>).

Technical Maintenance and Administrative Rights

University System Administrators and Authorized IT Staff

All system administrators (those individuals charged with the daily administration of computer resources within a unit of the university) will preserve individuals' privileges and rights of privacy consistent with this and other applicable university policies. Access privileges will be used only to the extent required by the performance of job responsibilities. Administrators will take all reasonable steps necessary to preserve the availability and integrity of electronic resources, including:

- Reject or destroy email messages and email attachments that are suspected of containing malicious code, phishing, viruses or worms.
- Eliminate sources of malware, viruses, phishing, or other forms of security threats, including shut down of ports, user names, passwords, and equipment, until it is safe to reconnect to network.
- Investigate and report suspected violations of university policies or viruses or other malfunctions.
- Ensure conformance with legal obligations as they pertain to the administration of electronic resources.

Physical Access Control

- Direct physical access to certain electronic resources such as servers, data networking devices, and telecommunications switches is restricted to authorized personnel only. If university personnel believe that an unauthorized person gained or attempted to gain access to a server or network equipment room, they must contact the Office of Information Technology and/or University Police immediately.

- Rooms containing critical electronic resources must be secured, and access to those rooms must be limited to authorized individuals only. All entrances to such rooms must be closed and locked at all times. Alarms, sensors and other types of physical security systems must be utilized to further secure these facilities and to detect and report emergency conditions that might occur.
- Appropriate fire suppression systems must be in place. Authorized personnel may be granted access to server or network equipment rooms through the issuance of ID cards or keys or through the use of passwords or other access codes, and access is restricted to role-based authority.

Policy Amendments:

- Northern Kentucky University reserves the right to change the policies, information, requirements and procedures, announced in this policy, at any time. Changes required by university contractual commitments shall be effective and binding to individuals upon execution of any such contract by the university.
- An individual shall be deemed to have accepted and be bound by any change in university policies, information, requirements or procedures, announced in this policy, at any time following announcement or publication of such change.

IV. EXCEPTIONS

V. REFERENCES AND RELATED MATERIALS

REFERENCES & FORMS

Link any forms or instructions needed to comply or implement this policy. If links are unavailable, attach forms to this policy as examples.

Data Governance website <http://datagovernance.nku.edu/>

FERPA guidelines (<https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html?src=rn>)

U.S. Copyright laws (<http://www.copyright.gov/title17/>

RELATED POLICIES

Link any currently existing policies related to this policy. If unable to obtain a link, simply list the names of the related policies.

NKU Anti-Virus Policy <http://policy.nku.edu/content/dam/policy/docs/a-through-z-policy-finder/Antivirus%20Policy.pdf>

NKU Data governance Policy http://policy.nku.edu/content/dam/policy/docs/a-through-z-policy-finder/APPROVED_DataGovernance7-2-2016.pdf

NKU Information Security Policy (http://policy.nku.edu/content/dam/policy/docs/a-through-z-policy-finder/APPROVED_InformationSecurity7-2-2016.pdf)

NKU Records Management policies (<http://policy.nku.edu/content/dam/policy/docs/a-through-z-policy-finder/Administrative-Regulations/Records%20Management%20Policy.pdf>)

DRAFT

MEMORANDUM

To: PCC

From: K. Katkin, Chair

Re: Draft Comments in Response to NKU's "Acceptable Use Policy" Proposal

Date: Jan 11, 2018

I am the Chair of the Professional Concerns Committee (PCC) of the NKU Faculty Senate. At its meetings of December 7, 2017 and January 18, 2018, the PCC discussed the proposed revisions to NKU's "Acceptable Use Policy" that have been released for public comment. On behalf of the PCC, I hereby offer the following comments on the draft Policy proposal entitled "Acceptable Use Policy."

(1) On Page Two, just above the header "Individual Rights," the generic phrase "Kentucky Public Records Law" should probably be replaced with the more specific phrase "Kentucky Open Records Act," which is the name of the Kentucky statute that governs access to public records.

(2) On Page Two or Three, in the list of "Individual Rights," an additional bullet point should be added that provides: "Individuals have the right to receive training that will facilitate compliance with all responsibilities and restrictions set forth in this policy."

(3) On Page Three, just below the header "Individual Responsibilities," the words "operational or copyrighted" should be deleted. The word "operational" is too vague to have any meaning. The word "copyrighted" could apply to substantially all content on all university computers, including faculty members' teaching materials or published articles—or even to Web content such as course descriptions or student handbooks that should be readily available to the public.

(4) On Page Three, the eighth bullet point below the header "Individual Responsibilities" begins with the words "Using only the access and privileges. . ." In this bullet point, the following additional language should be added to clarify:

However, Incidental personal use of university technology resources is not prohibited by this policy. Incidental personal use is an accepted and appropriate benefit of being associated with NKU's rich technology environment. Appropriate incidental personal use of technology resources does not result in any measurable cost to the university, and benefits the university by allowing personnel to avoid needless inconvenience. Incidental personal use must adhere to all applicable university policies. Under no circumstances may incidental personal use involve violations of the law, or interfere with the fulfillment of an employee's university responsibilities.

This language is adopted from language set forth in Indiana University's Acceptable Use Policy, <<https://policies.iu.edu/policies/it-01-appropriate-use-it-resources/index.html>>, and in the policy of

many other universities. It also reflects current salutary practice at NKU, and should be stated explicitly in our policy.

(5) On Page Four, the third bullet point prohibits users from extending the network via services or devices. The PCC does not understand why this restriction is necessary or desirable.

(6) On Page Four, the sixth bullet point prohibits users from introducing viruses to the network. The word “intentionally” should be added as the first word of the bullet point, which would now begin with “Intentionally introduce. . . .”

(7) On Page Four, the third-from-last bullet point concerns copyright infringement. Its use of the word “per” seems to be a typographical error that may reverse the intended meaning of the provision. The phrase “per copyright law” should be replaced with the phrase “in violation of copyright law.”

(8) On Page Four, in the third sentence below the header “University Processes/Privacy,” the words “are considered university property” should be deleted. The sentence would thus read: “In addition, all documents created, stored, transmitted, or received on university computers and networks may be subject to monitoring by systems administrators.” Because Intellectual Property is governed by other policies that generally do NOT vest ownership of faculty members’ work in the University, it is inaccurate and undesirable to characterize the university’s right to surveil users’ files as a “property” interest in the contents of documents stored on university computers.

(9) On Page Four, in the second bullet-point, the words “bona fide” should be inserted before the word “investigation,” so that the bullet-point would now begin with the words: “In connection with a bona fide investigation by the university. . . .”

(10) On Page Five, following immediately following the header “University Rights,” the long sentence should be divided into two sentences as follows. First, before the list of bullet points, the sentence should simply read: “When compelled by court order. . . .” This list of bullet points should then follow those five words. After the list of bullet points, a concluding sentence should state: “In the absence of a court order, any such actions shall be taken only after the area vice president appropriate to the circumstances makes a written determination that there is an urgent and compelling need to do so.” These changes would clarify that these actions may not be taken without a court order or VP determination, and to impress upon each individual VP the seriousness of granting such a determination.

(11) On Page Five, under the header “Enforcement: Misuse of Electronic Resources,” the final bullet point states that “civil and/or legal action may be initiated.” Because this provision is triggered by “violations of university policies” rather than by “violations of law,” this bullet point should be deleted or amended. The University would not be justified in bringing a civil or legal action in an instance where no law has been violated. For the same reason, the word “fines” should be deleted from the preceding and succeeding bullet points. Without prevailing in a civil action, the University has no authority to levy “fines” against its employees, and should not idly threaten to do so.

(12) On Pages Five and Six, under the header “Enforcement: Misuse of Electronic Resources,” the draft policy threatens that faculty members found to have violated this policy may be subject to termination of employment. The draft policy does not address the procedures by which guilt might be assessed or

penalties meted out. To avoid any ambiguity, language should be added immediately following the list of bullet points at the top of Page Six—and before the three subsequent paragraphs—to clarify that:

Such penalties shall be levied through ordinary disciplinary procedures set forth in other official University personnel policy documents, such as the NKU Personnel Policies and Procedure Manual, the NKU Faculty Policies and Procedures (the “Faculty Handbook”), or the Chase College of Law Faculty Policies and Procedures (the “Chase Faculty Handbook”).

Thank you for taking these comments into consideration.

Best,

--Ken Katkin, PCC Chair (2015-16 & 2016-17)

Professor of Law

Salmon P. Chase College of Law

556 Nunn Hall

Northern Kentucky University

Highland Heights, KY 41099

(859) 572-5861 phone

(859) 572-5342 fax

katkink@nku.edu

MEMORANDUM

To: PCC

From: Ken Katkin, Chair

Re: Amended Proposed Revisions to Faculty Handbook re Health Insurance Benefits for Short-Term Non-Tenure-Track Temporary (NTTT) Faculty Members

Date: January 11, 2018

Section 1.4 of the NKU Faculty Handbook governs certain terms and conditions of employment for full-time, non-tenure-track, temporary faculty members (NTTTs) at NKU. In this context, in pertinent part, the fourth paragraph of Section 1.4 of the Handbook currently states that for full-time NTTTs, "health insurance is provided by the University if the appointment is full-time for the complete academic year."

To comply with the Affordable Care Act, however, the University now provides health insurance to full-time NTTTs who are expected to work on average 30 hours or more per week for three months or more, even if those NTTTs are contracted to work for less than a complete academic year. Therefore, to bring the Faculty Handbook into conformity with the current practice required under the Affordable Care Act, and also to reflect comments received at the Faculty Senate meeting of December 15, 2017, Section 1.4 of the Handbook should be amended.

Therefore, I propose that PCC revise its prior recommendation to Faculty Senate to now propose that the relevant language in the fourth paragraph of Section 1.4 of the NKU Faculty Handbook be amended by adding the following words:

"health insurance is provided by the University if the appointment is full-time for the complete academic year. **If the appointment is full-time for less than one complete academic year, health insurance is provided by the University as needed to comply with local, state, or federal laws or regulations.**"

On the following page, the paragraph at issue is set forth as it currently appears in the Faculty Handbook, and as it would appear, as amended.

NKU Faculty Handbook Section 1.4, fourth paragraph (current language):

Non-tenure-track, temporary faculty are provided with Social Security contributions by the University. In addition, health insurance is provided by the University if the appointment is full-time for the complete academic year.

NKU Faculty Handbook Section 1.4, fourth paragraph (with amendment highlighted):

Non-tenure-track, temporary faculty are provided with Social Security contributions by the University. In addition, health insurance is provided by the University if the appointment is full-time for the complete academic year. **If the appointment is full-time for less than one complete academic year, health insurance is provided by the University as needed to comply with local, state, or federal laws or regulations.**

NKU Faculty Handbook Section 1.4, fourth paragraph (as amended):

Non-tenure-track, temporary faculty are provided with Social Security contributions by the University. In addition, health insurance is provided by the University if the appointment is full-time for the complete academic year. If the appointment is full-time for less than one complete academic year, health insurance is provided by the University as needed to comply with local, state, or federal laws or regulations.

To: Sue Ott Rowlands, Provost and Executive Vice President for Academic Affairs
From: Allen Cole, University Registrar at NKU

Subj: Shortened Semester Recommendation

FINAL: Jan 4, 2018

The recommendation is that the concept is worth exploring campus-wide.

Rationale:

Supporting student success and the educational experience are key motivations, whereby shortening each of the two semesters of Fall and Spring by one week could provide the following:

- a. more options for an enhanced and robust Winter Session
- b. consistency between all 3 semesters (Fall, Spring, Summer) as each would have 15 weeks available for instruction time
- c. a better alignment with the emerging 7-weeks sub-sessions that will happen over all semesters.

The two models that were examined and compared directly to NKU were UC and WKU. But, each does not fit exactly to NKU current needs, from an overall structure perspective. Aspects of each were helpful, however. The new energy at NKU around online and 7-weeks sessions, which will be held year-around, is a factor to build into the calendar. So, shortening the two main semesters by 1 week could yield some structural benefits. We could add 1 week to Summer (for consistency of 15 weeks for every semester) and have more strategic time between semesters, for processing and preparation.

Winter Session would remain as is, with its niche and purpose, but have an additional week.

Notable Impacts to explore:

The group also explored possible class time period grids that would need to be scrutinized by the campus, as time periods would change (e.g. 50 min periods become 55 min). And maybe a change to 15 minutes between classes could be made. The impact on campus space utilization is another factor to be considered, as there would be less class periods than currently exist, but with HIC/Founders, then there are potentially more classrooms available for use. Also, must determine how science/weekly labs fit into such a revised class schedule.

A noticeable change will be the start of Spring Semester classes on the Tuesday after MLK holiday, which adds 1 week to Winter Session and allows for more preparation time for the Spring semester.

Spring Break needs to be placed between the two 7-weeks sub-sessions.

Conversely, Fall Semester would not feel much different, except to start a week later in August. The December commencement would be the same time as current. The two days of fall break should be changed, either eliminated or moved to one day off, on a Friday, where less impact would be felt in lost class instruction time.

Other considerations:

Some Summer related questions are: a) What is the impact, if any, on financial aid? b) What is the impact, if any, on faculty work load and 10-month faculty contracts, c) What is the impact, if any, on Summer camps or special groups (Governor’s Scholars), and d) What academic polices might need to be changed?

The 5-week MBA sessions would have less time between each session in Fall and Spring Semesters, but Summer *might* allow for an additional MBA session.

Starting a week later in January would help with the arrival and orientation of international and transfer students.

Teaching placements for education students in local schools may need adjusting, due to a later start in Spring Semester.

Other items specific to the Provost’s charge:

- a. SACS and federal requirements can be fulfilled with properly planned class times.
- b. Review of peer institutions shows that within the KY publics only WKU uses the shorter semester length. UC and other Ohio colleges use the shorter semester, as well.
- c. The NKU admission office has not noticed any competitive disadvantage when recruiting students who are also considering WKU or UC.
- d. Best Practices can be fulfilled by adjusting the allocated class minutes as needed.

The 11 members of the Work Group are: Allen Cole, University Registrar

Frank Robinson, Norse Advising	Frank Braun, Chair of the Council of Chairs
Mary Paula Schuh, Campus Planning	Arnie Slaughter, Student Affairs
Susannah Coaston, Faculty in Counseling	Traci Freeman, Nursing Faculty
Ben Jager, President’s Office	Francois LeRoy, International
Keith Walters, Chemistry Chair	Diane Williams, Learning PLUS

The Academic Affairs Council endorses this recommendation at its meeting on 1-4-2018.

MEMORANDUM

To: PCC

From: K. Katkin, Chair

Re: Withdrawal of Application for Promotion During RPT Process (Proposed Faculty Handbook Amendment)

Date: January 11, 2018

The Faculty Advocate referred to PCC a question concerning promotion or tenure in a non-mandatory year. **Should a faculty member be allowed to withdraw the application for promotion and/or tenure and materials after receiving a negative recommendation from the departmental review committee?** The Faculty Handbook is silent on this question. According to the Faculty Advocate, over time different Provosts at NKU have adopted varying stances on this issue. Accordingly, the Faculty Advocate recommended that PCC consider whether Faculty Senate should recommend that the Faculty Handbook be amended to provide a definitive answer to this question.

The PCC discussed this issue at its meetings of November 16, 2017 and December 7, 2017. At the December 7 meeting, the PCC concurred with the Provost's recommendation that the handbook should be amended to clarify that a faculty member should not be allowed to withdraw the application and materials after receiving a negative recommendation from the departmental review committee.

The PCC therefore now recommends to Faculty Senate that the NKU Faculty Handbook should be amended by adding a sentence to the end of current Section 3.2.2 that would read as follows:

Once filed with the RPT committee, an application for reappointment, promotion, tenure, or a combination thereof, may not be withdrawn or rescinded.

As amended, Section 3.2.2 would thus read:

3.2.2 INITIATION OF REQUEST

The applicant is responsible for initiating consideration by applying for reappointment, promotion, tenure, or a combination of them. A full-time administrator with academic rank may apply for tenure or promotion supported by documentation. The applicant will compile an RPT dossier, including a cover sheet provided by the provost's office. **Once filed with the RPT committee, an application for reappointment, promotion, tenure, or a combination thereof, may not be withdrawn or rescinded.**