NKU—Faculty Senate Evaluation of Administrators—PCC Draft, May 5, 2016

The evaluation forms will be distributed electronically to eligible faculty, and faculty shall submit their responses electronically. All full-time faculty members are eligible to participate in the evaluation. Evaluations will be anonymous and confidential.*

The evaluation instrument and instructions will be distributed to eligible evaluators. A deadline date for responses will be included.

The faculty portion of the evaluation process must be completed prior to the close of the Spring Semester each year.

Each evaluator will be requested to complete the Administrator's Evaluation Form and return it, along with any narrative comments. Narrative comments are encouraged.

Completed forms will be returned electronically to Faculty Senate Office.

After the evaluation instruments have been returned to the Faculty Senate, a statistical summary of the results will be developed. Copies of the summary and the verbatim transcript of narrative comments will then be forwarded only to the administrator being evaluated, his or her immediate supervisor, the Provost/Vice President for Academic Affairs, and the President. In the case of the President, the summary and transcripts will also be forwarded to the Chair of the Board of Regents. The information can be shared with others only by specific permission of the person evaluated. The evaluations are part of the administrator's confidential personnel file. The Faculty Senate President has access to all the compiled results, and will meet with the University President, as well as the Chair of the Board of Regents, to discuss the President's results.

The results of the survey will be utilized as a formal and significant part of the performance appraisal by the appropriate supervisor of the evaluated administrator. The evaluator will weigh the results of the survey within the greater context of the evaluation, and will receive a formal response to the survey results from the evaluated administrator. The Provost—as Chief Academic Officer—will report to the relevant faculty a synopsis of the administrator's evaluation.** Should significant concerns arise from the survey results, both the Provost and the administrator will respond formally to the affected faculty, including suggestions to address areas of administrator performance needing improvement. Every effort should be made to have these suggestions be specific and achievable.

*An option to sign the evaluation will be available.

**Using the same process, the President will report to the faculty about the evaluation of the Provost.

Page 94, #5

Replace the sentence:

The investigator must be satisfied that the explanation has been understood and consent in writing obtained without duress or deception.

With:

The investigator must be satisfied that the explanation has been understood and obtain consent in writing, unless documentation of informed consent has been waived, without duress or deception.

Page 96, Section C

Replace all of Section C with:

C. Research that involves human subjects but does not need approval from the Institutional Review Board

In pursuit with CFR 46.101, federal guidelines state that only the IRB can determine the status of a proposed study. Because of this mandate, all potential research studies involving human participants or identifiable records must be submitted to the IRB for review before being started.

One narrowly defined study type is recognized as an exception to this policy. IRB review and approval is not needed for:

1. Studies in undergraduate classes or graduate seminars that involve human participants and are:

a. conducted solely for instructional purposes, and

b. not intended to contribute to general knowledge.

When a study is designed to provide a learning experience for students and when the instructor and student investigator(s) have no plan, intention, desire, or hope to publish, present, or report the findings of this study in any off-campus setting (e.g., journal, report, conference, other off-campus outlet, etc.), the activity will not be considered to be research, and will not require IRB review.

In this instance, faculty instructors are wholly responsible for classroom projects conducted by students in their classes, and for ensuring that these student projects treat human participants ethically.

Page 97, paragraph 1

Replace paragraph 1 (The principal investigator should provide the board with…), with:

The Principal Investigator should provide the board with a protocol for each new research project involving human subjects. In addition, all supporting documents should be included, such as: questionnaires, signed letters of participation and agreement by institutions participating with Northern Kentucky University, personal interview statements, and debriefing procedures. In accordance with board guidelines, a single copy should be submitted to the IRB Administrator for review. Please note, grant proposals for external support should not be used as the protocol because they are often too long and frequently do not address the concerns of the board.

Page 97, Section F, 1st sentence

Replace this sentence:

All protocols are screened for completeness by the board chair prior to the conduct of a formal review.

With:

All protocols are screened for completeness during IRB Pre-Review by the IRB Administrator prior to the conduct of a formal review.

Page 99, Section G

Replace Section G with:

G. Actions by the Institutional Review Board

In pursuit with 45 CFR 46, after review and discussion of the protocol, the board will take one of the following actions:

1. Classify the Submission as Not Research: This includes quality improvement projects taking place in the classroom with no intention to present or publish collected data.

2. Approve the Research as Exempt: Exempt studies are those that involve no danger to the subjects. This includes procedures such as standard classroom activities or interviews on non-threatening topics. Projects that do not involve changes in the ordinary risks of daily life or in recognized occupational 6 risks are also considered no-risk. Written informed consent is required in exempt IRB studies. No need for IRB oversight unless changes are made to the protocol.

3. Approve the Research as Expedited: The research may involve some risk to the subjects, but is not unreasonable. The potential benefits of the research outweigh the risks, and risk-management procedures have been taken to minimize the risks. This approval requires oversight

by the IRB and annual continuations must be submitted if the study will continue past the one year approval date.

4. Full Board Review Approval: A Full Board Review approval requires quorum approval of the IRB. The board may request the investigator to be present to discuss the research proposal. This may occur when the IRB finds the research to have more than minimal risks and as defined by federal regulations, the elements, procedures or interventions require additional provisions or safeguards.

5. Disapprove the Research: The board is of the opinion that the potential benefits of the research do not outweigh the risks to the subjects. Some modifications or clarifications might be requested of the PI in all types of research. The modifications required by the board may include such items as revising the consent form to explain the procedures more clearly, restricting use of a certain procedure, or requiring use of specified safeguards necessary for the protection of human subjects.

Page 100, Section K

2nd Sentence, replace this sentence:

Such forms must be retained by the investigator (or faculty advisor) for a minimum of three (3) years after termination of the project.

With:

Such forms must be retained by the investigator (or faculty advisory) for a minimum of six (6) years after termination of the project. If the records are part of a misconduct investigation, all records must be retained for a minimum of seven (7) years after the termination of the project.

Page 101, paragraph 2, sentence 1

Replace this sentence:

These records shall be maintained for at least three (3) years after completion of the research and shall be available to authorized member of the Department of Health and Human Services at reasonable times and in a reasonable manner.

With:

These records must be retained by the investigator (or faculty advisory) for a minimum of six (6) years after termination of the project. If the records are part of a misconduct investigation, all records must be retained for a minimum of seven (7) years after the termination of the project.

The records must be available to authorized members of the Department of Health and Human Services at reasonable times and in a reasonable manner.

16.5. ADVISING OF STUDENTS

Faculty should be familiar with the University's academic requirements, policies, and procedures as outlined in the University Catalog, including the Classification of Admissions Policy and the Placement Policy. Faculty should also be familiar with the Philosophy of Advising statement in the admissions section of the University Catalog. The catalog can be found online at: https://catalog.nku.edu.

16.6. HUMAN SUBJECT POLICIES

16.6.1. GENERAL

The Northern Kentucky University Institutional Review Board for the Protection of Human Subjects is appointed by the provost, who has administrative responsibility for safeguarding the rights and welfare of human subjects involved in research. The board consists of at least five members with varying academic backgrounds and at least one who is not an employee or agent of the University. Membership of the board will be reviewed annually by the provost, who will report any changes to the United States Secretary of Health and Human Service.

University policies and federal regulations regarding research with human subjects are implemented by the board and the University Office of Research, Grants, and Contracts, which serves as the administrative arm to the board and the provost.

The protection of human subjects from unnecessary risks can be achieved when: the human subject's participation is voluntary as reflected on the consent forms; the degree and nature of the risk have been carefully explained to the human subject; and there is a desirable balance between the potential benefits of the research and the risks undertaken by the human subject. The board has the sole responsibility to approve research with human subjects performed under the auspices of the University.

In reviewing all biomedical and behavioral research that involves human subjects conducted at Northern Kentucky University, the Institutional Review Board for the Protection of Human Subjects will utilize the following principles:

- A human subject will not be exposed to unreasonable risk to health or well-being whether physical, psychological, or social.
- Commensurate with the principle of protection of human subjects, the procedures for assessing and minimizing risk to human subjects shall respect and protect the academic freedom of the University's faculty and students in their pursuit of knowledge.
- The risks to an individual must be outweighed by the potential benefit to him/her or by the importance of the knowledge to be gained.

- The identity and personal privacy of human subjects and the confidentiality of information received will be protected.
- The nature of the research, the procedures to be followed, and the possible risks involved must be carefully and fully explained to the subject, parent or guardian, as appropriate. The investigator must be satisfied that the explanation has been understood and consent in writing obtained without duress or deception.
- Voluntary participation is essential in all projects. No information concerning a project may be withheld from a potential subject in order to increase the willingness of the subject to participate in the project.
- A subject may request at any time that his/her participation in the experiment be terminated, and the request shall be honored promptly and without prejudice.
- It shall be the responsibility of the individual investigator to decide when he/she does not have adequate knowledge of the possible consequences of his/her research, or of research done under his/her direction. When in doubt, he/she shall obtain the advice of others who do have the requisite knowledge.
- Potentially hazardous research procedures must be preceded by laboratory and animal experimentation or other scientifically established procedures that offer reasonable assurance that the safety of human subjects will be preserved.
- Remuneration may be offered to an individual for the time involved in a study, provided the investigator is satisfied that under the circumstances the remuneration is not so large as to constitute an undue or unreasonable inducement.
- It shall be a responsibility of Northern Kentucky University to ensure that research involving human subjects conducted by faculty, students, and employees of the University shall be performed carefully and with regard to the above principles.

16.6.2. RESEARCH THAT INVOLVES HUMAN SUBJECTS

There is human-subject involvement when an investigator obtains:

- Data through intervention or interaction with the individual; and/or
- Identifiable private information.

“Intervention” includes both physical procedures from which data are gathered and manipulations of the subject or the subject’s environment that are performed for research purposes.

“Interaction” includes communication or interpersonal contact between investigator and subject.

“Private information” includes information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place and information

that has been provided for specific purposes by an individual will not be made public. Private information must be individually identifiable.

All research conducted on human subjects—whether supported partly or wholly by external funds, University funds, or without funds—must have prior approval by the Institutional Review Board.

All proposals that request external support for activities involving human subjects under the auspices of the University must be submitted through the office of Research, Grants, and Contracts to the funding agency.

16.6.3. RESEARCH THAT INVOLVES HUMAN SUBJECTS BUT DOES NOT NEED APPROVAL FROM THE INSTUTUIONAL REVIEW BOARD

Approval from the Institutional Review Board is not required when the research:

- Is conducted in accepted educational settings, involving normal educational practices such as research on instructional strategies or classroom management methods;
- Involves the use of educational tests, if the information does not identify the subjects;
- Involves surveys or interviews, except when responses are identifiable with the individual subjects;
- Involves observations, except when observations are recorded in such a manner that the subjects can be identified; and/or
- Involves the collection or study of existing data, documents, records, diagnostic specimens, if these sources are publicly available or if the information is recorded in a way that cannot be identified with the subjects.

All research proposals with human-subject involvement must be reviewed by the board chair or board reviewer designated by the chair to assess and confirm exempt status.

16.6.4. INVESTIGATOR'S LEGAL RESPONSIBILITY IN RESEARCH WITH HUMAN SUBJECTS

The investigator is legally responsible for any research or related activities that involve human subjects conducted under the auspices of the University and/or that utilize University time, facilities, resources, and/or students. The University's legal counsel has the responsibility for resolution of any legal questions.

16.6.5. APPLICATION PROCEDURES

Principal investigators are required to submit a protocol describing the proposed research project to the Institutional Review Board for review and approval.

The principal investigator should provide the board with a protocol for each new research project involving human subjects. In addition, all supporting documents should be included, such as: questionnaires, signed letters of participation and agreement by institutions participating with Northern Kentucky University, consultants, physicians, sponsors, faculty advisers, personal interview statements, and debriefing procedures. A single stapled copy, in accordance with board guidelines, should be submitted to the board chair for exempt or expedited review. If a full board review is necessary, ten (10) additional copies will be required. The protocol should be limited to ten (10) pages or fewer. Grant proposals for external support are usually too long and frequently do not address the concerns of the board.

The investigator should discuss the need for the research, its objectives, the methods to be used to accomplish the objectives, the risks involved, and the procedures used to protect the subjects from, or minimize, the risks. Risks may be classified as physical, psychological, social to individuals, and social to groups. These are defined as follows:

Physical Risk: The extent to which physical injury is a possibility from physical activity, injections, or stimuli from electrical apparatus, fumes, light, noise, etc.

Psychological Risk: The extent to which research interrupts the normal activity of human subjects resulting from immediate or long-term stress. Stress includes any situation that threatens one's desired goals.

Social Risk to Individuals: The extent to which a subject is deprived of formal or informal relationships within social groups.

Social Risk to Groups: The extent to which a subject group, either formal or informal, is exposed to factors that may reduce the group's viability.

Any research proposing to place any individual at risk is obligated to obtain and document legally effective informed consent. Informed consent is the knowing consent of an individual, or his/her legally authorized representative, who is able to exercise free power of choice without undue inducement or any element of force, fraud, deceit, duress, or other form of constraint or coercion.

Research that has been approved by the board may be reviewed, approved, or disapproved by University officials. They may not, however, approve the research if the Institutional Review Board has not first approved it.

16.6.6. REVIEW OF APPLICATION BY THE INSTITUTIONAL REVIEW BOARD

All protocols are screened for completeness by the board chair prior to the conduct of a formal review. A board member may not cast a vote, or be otherwise involved, in either the initial or conducting review or any activity in which he/she has any conflicting interest, or any involvement, except to provide information requested by the board. The review performed by the board will determine whether subjects will be placed at risk. The policy criterion for determining risk is defined as follows:

"Subject at risk" is any individual who may be exposed to the possibility of injury, including physical, psychological, or social injury, as a consequence of participation as a subject in any research, development, or related activity that departs from the application of established and accepted methods necessary to meet his/her needs or that increases the ordinary risks of daily life, including the recognized risks inherent in a chosen occupation or field of service.

If risk is involved, the answers to the following questions will be considered:

- Are the risks to the subject too outweighed by the benefits to the subject and the importance of the knowledge to be gained as to warrant a decision to allow the subject to accept these risks?
- Are the rights and welfare of any such subjects adequately protected?
- Is legally effective informed consent obtained by adequate and appropriate methods in accordance with the provisions of federal regulations?

The board may use expedited review procedures for certain kinds of research involving no more than minimal risk and for minor changes in research protocols having prior board approval. Such review will be conducted by the board chair or by one or more experienced board reviewers designated by the chair. Under the expedited procedure, the reviewer(s) may exercise all the authorities of the board except that of final disapproval of the research. All board members will be notified of all research approved in the expedited review procedure. Any protocol not approved under the expedited procedure will be referred to the full board for review.

Approval of research will necessitate that the board determine that the following requirements are satisfied:

- Risks to subjects are minimized.
- Risks to subjects are reasonable in relation to anticipated benefits.
- Selection of subjects is equitable.
- Informed consent will be obtained from each prospective subject or the subject's legally authorized representative.
- The informed consent will be appropriately documented.
- Data will be regularly monitored to insure subjects' safety.

16.6.7. ACTIONS BY THE INSTITUTIONAL REVIEW BOARD

After review and discussion of the protocol, the board will take one of the following actions:

16.6.7.1. CLASSIFY THE RESEARCH AS *NO RISK*

No risk projects are those that involve no danger whatever to the subjects. This includes procedures such as standard classroom activities or interviews on non-threatening topics. Projects that do not involve changes in the ordinary risks of daily life or in recognized occupational risks are also considered *no risk*. Written informed consent is required in *no risk* projects.

16.6.7.2. APPROVE THE RESEARCH AS *RISK*

The research may involve some risk to the subjects, but is not unreasonable. The potential benefits of the research outweigh the risks, and risk-management procedures have been taken to minimize the risks.

16.6.7.3. CONDITIONALLY APPROVE THE RESEARCH AS *RISK*

The board will require minor modifications to a part of the proposed research. The modifications required by the board may include such items as revising the consent form to explain the procedures more clearly, restricting use of a certain procedure, or requiring use of specified safeguards necessary for the protection of human subjects. The board may request the investigator to be present to discuss the research proposal.

16.6.7.4. DISAPPROVE THE RESEARCH

The board is of the opinion that the potential benefits of the research do not outweigh the risks to the subjects.

16.6.8. DISPOSITON OF THE RECOMMENDATIONS

Approvals, recommendations, restrictions, conditions, or disapprovals of application are communicated to the investigator by the board chair. If an application is disapproved for nonconformity with the policies of the board and the University, the board shall forward to the investigator a statement setting forth in detail the reasons for the nonconformity and recommendations of the board for modification of the research proposal.

16.6.9. RIGHTS OF APPEAL

If the investigator believes that the proposal has been disapproved because of incorrect, unfair, or improper evaluation by the board, the investigator may appeal to the appropriate dean who then may request a reconsideration and hearing of the proposal by the board. Within ten (10) days after a negative decision, the affected investigator must show cause in writing or at a designated hearing as to why the board's decision should be reversed.

16.6.10. APPEAL DECISION

The board may take one of the following actions:

- Approve;
- Require modification; or
- Disapprove.

16.6.11. RECORDS AND DOCUMENTATION OF THE INVESTIGATOR

The investigator is required to obtain and keep documentary evidence of informed consent of the human subjects or their legally authorized representatives. Such forms must be retained by the investigator (or faculty advisor) for a minimum of three (3) years after termination of the project.

16.6.12. INSTITUTIONAL REVIEW BOARD RECORDS

The board is required to keep copies of all documents presented or required for initial and continuing review by the board. These include copies of all research proposals received, scientific evaluations (if any accompany the proposals), approved sample consent documents, progress reports submitted by investigators, and reports of injuries to subjects. Minutes of board meetings shall reflect meeting attendance; actions taken by the board; votes on actions, which will show the number of members voting for, against, and abstaining; the basis for requiring changes in or for disapproving research; and written summaries of discussions about controverted issues and their resolution. Other documents will include records of continuing review activities; copies of all correspondence between the board and investigators; a list of board members; written procedures; statements of significant new findings; reports of injuries; progress reports; and unanticipated problems.

These records shall be retained for at least three (3) years after completion of the research and shall be available to authorized member of the Department of Health and Human Services at reasonable times and in a reasonable manner. These records will be continually reviewed by the Office of Research, Grants, and Contracts with follow-up concerning conditions of approvals, additional information requested, etc.

The records of the board pertaining to individual research activities are not accessible to persons outside the board other than the records of projects supported by external funds that are subject to inspection by federal employees.

Except as otherwise provided by law, information acquired in connection with a research, development, or related activity that refers to or can be identified with a particular subject will not be disclosed except:

- With the consent of the subject or a legally authorized representative; or
- As may be necessary for the Secretary of Health and Human Services to carry out his/her responsibilities under federal regulations.

16.6.13. POLICY FOR LIABILITY FOR INSTITUTIONAL REVIEW BOARD

Due to the privilege of sovereign immunity, the University, as an institution, is protected through the State Board of Claims. In addition, the University maintains a professional liability policy covering most actions of the faculty and staff. In the event the professional liability policy should fail, the University Board of Regents, in its By Laws adopted August 27, 1976 and revised August 13, 1992, insured that if any legal action is taken or claims filed against any faculty or staff member, he/she will be provided legal defense and indemnification for any acts or actions taken while on official business of the University (see Section 1.3, Legal Defense and Indemnification/Notice Requirement, and Appendix B, Article IV, Regents' By Laws).

16.7. SCIENTIFIC/RESEARCH MISCONDUCT

16.7.1. PREAMBLE AND POLICY STATEMENT

The preeminent principle in all research is the quest for truth. The credibility of such research must be above reproach if the public trust is to be maintained. Any compromise of the ethical standards required for conducting academic research cannot be condoned. While breaches in such standards are rare, these must be dealt with promptly and fairly by all parties in order to preserve the integrity of the research community.

A critical element of any policy on research misconduct is that it be a fair and effective process for distinguishing instances of genuine and serious misconduct from insignificant deviations from acceptable practices, technical violations of rules, or simple carelessness. The policy defined in this Handbook will allow such distinctions to be made in a manner that minimizes disruption and protects the honest researcher from false or mistaken accusations.

Research misconduct, as defined in Section 8.2, below, is not condoned at Northern Kentucky University and allegations of such misconduct will be investigated in accordance with the

To: Chief Information Officer, Office of Information Technology
From: Prof. Ken Katkin, PCC Chair
Re: NKU Policy on "Data Governance & Security"
Filed: June 6, 2016

I am the Chair of the Professional Concerns Committee (PCC) of the NKU Faculty Senate. Neither the PCC nor the Faculty Senate meet over the summer. I have not conferred with any other member of the PCC before filing these comments. Accordingly, the following comments represent only my own views. However, I intend to disseminate these comments to the incoming PCC Members in advance of our first meeting in Fall 2016.

I offer the following comments on the draft Policy proposal entitled "Data Governance & Security." These comments are consistent with comments that I filed separately in the response to the draft Policy proposal entitled "Information Security Policy," which has been opened for public comment concurrently with the present proposal.

(1) On Page One, the data classification table cross-referenced in the definition of "data classification" adopts a definition of "public data" that places excessive and undesirable restrictions on the use and dissemination of such data. In order to preserve the open information sharing requirements of NKU's academic culture, to protect the freedom of speech of all NKU community members, and to comply with the letter and spirit of Kentucky's Open Records Act, the following revisions to the draft language in the "public data" column are needed.

(a) In the current draft of the table cross-referenced in the definition of "data classification," public "access" to "public data" is limited only to "NKU affiliates and general public with a need-to-know." This language raises the possibility that an NKU community member could be disciplined for sharing public data with someone who does not have a "need-to-know." By definition, "public data" should be available to the public, without any threshold need to demonstrate any need-to-know. See Ky. Rev. Stat. § 61.872(2) ("Any person shall have the right to inspect public records."). The language describing who is entitled to have "access" to "public data" should therefore be amended to simply read: "unrestricted."

(b) In the current draft of the table cross-referenced in the definition of "data classification," the language describing "legal requirements" of "public data" seems not to comply with the presumption of openness set forth in the Kentucky Open Records Act and in the University's own stated commitment to preserve the open information sharing requirements of NKU's academic culture. As drafted, this policy language states that protection of public data "is at the discretion of the owner or custodian" of the data. This language seems to imply that the owner or custodian of public data has discretion to withhold public data from the public. The Kentucky Open Records Act, in contrast, codifies into Kentucky law the policy "that free and open examination of public records is in the public interest and the exceptions provided for by KRS 61.878 or otherwise provided by law shall be strictly construed, even though such examination may cause inconvenience or embarrassment to public officials or others." Ky. Rev. Stat. § 61.871. In most instances, therefore, if an NKU owner or custodian were to exercise "discretion" to deny access to public data, such an exercise would violate the Kentucky Open Records

Act. To resolve this problem, the language describing the "legal requirements" of "public data" should be amended to read: "is governed by the Kentucky Open Records Act, KRS §§ 61.870 to 61.884."

(c) In the current draft of the table cross-referenced in the definition of "data classification", the list of "examples" of "public data" seems misleadingly restrictive, in that all but one example concerns material that the University voluntarily publicizes through its Web Site. In fact, however, the category of "public data" includes all institutional data that is not "confidential data" or "private data," including a great deal of data (such as salary data) that is not routinely or voluntarily posted on University Web Sites. The Kentucky Open Records Act defines "public records" as "all books, papers, maps, photographs, cards, tapes, discs, diskettes, recordings, software, or other documentation regardless of physical form or characteristics, which are prepared, owned, used, in the possession of or retained by a public agency," Ky. Rev. Stat. § 61.870(2), except those that fall within a specific exception set forth at Ky. Rev. Stat. § 61.878. To avoid creating the misleading impression that "public data" is limited only to categories of information that the University chooses voluntarily to publicize, an additional bullet point should be added to the list of examples, which would read: "all institutional data made available to the general public by the Kentucky Open Records Act."

(2) In Section V of the draft Policy proposal entitled "Data Governance & Security," the phrase "institutional data" appears several times in the bullet-pointed list of "employee do's and don'ts" on Page Three. On these lists, the phrase "institutional data" should be replaced in all instances with the phrase "confidential data." Otherwise, as drafted, the proposed policy would impose restrictions on NKU employees' access to "public data" that conflict with the openness mandated by the Kentucky Open Records Act. See Ky. Rev. Stat. § 61.872(2) ("Any person shall have the right to inspect public records.").

Rights to inspect public records under the Open Records Act are not restricted "only for the purpose of conducting university business" or only to data needed by NKU employees "to perform their job[s]." To the contrary, the Kentucky Open Records Act fully applies to data requests for public records made for no reason other than "to satisfy personal curiosity." And indeed, in the context of NKU's structure of collegial governance, it is difficult to draw meaningful lines between a faculty or staff member's "personal curiosity" about public institutional data and that person's informed participation in shared governance, which is a job function. Accordingly, while such restrictions may be desirable for NKU employees charged with custody of "confidential data," these restrictions are inappropriate when applied to the "public data" that constitutes the lion's share of all NKU "institutional data."

Accordingly, the language on Page Three should be revised to read as follows:

> Employees are expected to
>
> - Access confidential institutional data only for the purpose of conducting university business
> - Access confidential data only as needed to perform their jobs
> - Respect and protect the confidentiality and privacy of the individuals whose confidential records they have access to
> - To abide by all applicable laws or policies with respect to access, use, or disclosure of information
>
> Employees should not:

- Disclose confidential data to others except as required by their job responsibilities
- Use confidential data for their own or others personal gain or profit
- Access confidential data to satisfy personal curiosity
- Forge, falsify, or alter (without authorization) documents, records, or university data in any form (including financial documents)

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

DATA GOVERNANCE & SECURITY

POLICY NUMBER: RESERVED FOR FUTURE USE
POLICY TYPE: ADMINISTRATIVE
RESPONSIBLE OFFICIAL TITLE: CHIEF INFORMATION OFFICER
RESPONSIBLE OFFICE: OFFICE OF INFORMATION TECHNOLOGY
EFFECTIVE DATE:7/2/2016
NEXT REVIEW DATE: 6/1/2017
SUPERSEDES POLICY DATED: N/A
REQUIRES LEGAL/COMPLIANCE REVIEW:
(PER SECTION V. OF THE APPROVED POLICY REQUEST FORM) ☒YES ☐NO
REQUIRES I.T. POLICY COUNCIL REVIEW:
(PER SECTION V. OF THE APPROVED POLICY REQUEST FORM) ☒YES ☐NO
REQUIRES PROFESSIONAL CONCERNS COMMITTEE REVIEW:
(PER SECTION V. OF THE APPROVED POLICY REQUEST FORM) ☐YES ☒NO
REQUIRES HUMAN RESOURCES REVIEW:
(PER SECTION V. OF THE APPROVED POLICY REQUEST FORM) ☐YES ☒NO
REQUIRES BOARD OF REGENTS APPROVAL:
(PER SECTION V. OF THE APPROVED POLICY REQUEST FORM) ☐YES ☒NO

I. POLICY STATEMENT

Northern Kentucky University's (NKU) institutional data is a valuable asset and resource and must be maintained and protected as such. Although individuals, offices, departments, programs or colleges may have responsibilities for creating and maintaining portions of university information and records, NKU itself retains ownership of, and responsibility for the information.

The purpose of this policy is to protect NKU's information resources from accidental or intentional unauthorized access, modification, or damage, while also preserving the open information sharing requirements of its academic culture.

Permission to access institutional data should be granted to all university employees for all legitimate university purposes.

II. ENTITIES AFFECTED

All Northern Kentucky University community members who have access to university institutional data as well as all university colleges, units, divisions and their agents and contractors. It also applies, to the extent possible, to any person or organization, whether affiliated with the university or not, in possession of university institutional data.

III. SCOPE AND APPLICABILITY

This policy applies regardless of the environment, media or device where the data resides or is used and regardless of how the data is transmitted or stored.

IV. DEFINITIONS

Data Classification – Classification of data to provide a basis for understanding and managing institutional data based on the level of criticality and required confidentiality of data. For NKU's data classifications see the data classification table located here:

Data Communities - Data stewards /data custodians who are responsible for ownership of common data elements used across the university. Data community members work together to provide a formal communication to NKU data producers/consumers when common data elements require a change.

Data Custodians - Individuals appointed by and accountable to the data stewards. Data custodians are responsible for the operation and management of systems and servers that collect, manage, store, and/or provide access to institutional data.

Data Producers/Consumers - All NKU employees who produce and/or have access to institutional data in order to perform assigned duties or in fulfillment of assigned roles or functions within the university; this access is granted solely for the conduct of university business. Data producers/consumers are responsible for knowing and following university policies and procedures on data governance.

Data Stewards – Institutional officers, who are appointed by the President or Provost, and have authority over policies and procedures for one or more types of institutional data and the access and usage of that data within their delegations of authority. Each data steward appoints data custodians for their specific functional area of responsibility.

Data Quality - The management, process, and measurement of information's fitness to serve its purpose in a given context. Aspects of data quality encompass:

- Accuracy
- Completeness
- Consistency across the university
- Relevancy
- Unduplicated
- Traceability
- Interpretability
- Timeliness
- Accessibility

Institutional Data - Data elements which are created, received, maintained, and/or transmitted by NKU administrative information systems. Information is a collection of Institutional Data representing quantitative/qualitative measurements and facts related to the business of the University. Click here for types of NKU institutional data.

V. RESPONSIBILITIES AND INFORMATION

All university community members who work with or use institutional data in any way must comply with all federal, state and other applicable laws, university policies, procedures and guidelines and applicable contracts and licenses. Examples include, but are not limited to:

- Family Education Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Kentucky Open Records Laws
- Kentucky Revised Statutes
- Kentucky Statutes regarding Personal Information Security and Breach Investigations (KRS 61.934 to 61.934)

- Payment Card Industry Standards (PCI-DSS)
- Other NKU information and security policies

NKU employees and their supervisors are responsible for understanding and complying with all laws, rules, policies, standards, guidelines, contracts and licenses that are applicable to their own and their subordinates' specific uses of institutional data.

Employees are expected to

- Access confidential data only for the purpose of conducting university business
- Access only the confidential data required to perform their job
- Respect and protect the confidentiality and privacy of the individuals whose confidential records they have access to
- To abide by all applicable laws or policies with respect to access, use, or disclosure of confidential information

Employees should not:

- Disclose confidential data to others except as required by their job responsibilities
- Use confidential data for their own or others personal gain or profit
- Access confidential data to satisfy personal curiosity
- Forge, falsify, or alter (without authorization) documents, records, or university data in any form (including financial documents)

University community members who are acting in one or more specific roles when collecting, maintaining, accessing or using institutional data must understand and fulfill the responsibilities associated with their roles. These roles are (see definitions in Section IV.):

- Data Steward
- Data Custodian
- Data Producer/Consumer

For specific instructions on how to access institutional data via NKU administrative information systems, please contact the designated Data Custodian of that system.

VI. COMMITTEE

The Data Governance Committee was formed to recommend and oversee the implementation and management of a formal data governance program that functions across the university. For a list of the members of the committee, please click here.

Data classifications are created and maintained by the Data Governance Committee.

VII. VIOLATIONS

Any member of the university community found to have violated this policy is subject to discipline in accordance with applicable university policies and procedures, or, in the case of student violations processed under the Code of Students Rights and Responsibilities, expulsion.

VIII. DATA QUALITY REPORTING REQUIREMENTS

To submit an NKU data quality issue, click here. You will need to sign in using your NKU user ID and password.

To see a flowchart depicting the data quality issue resolution process, click here.

IX. 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, Data Dictionary and Report Repository

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.

Credit Card Processing and Security Policy, Security Policy, Records Management Policy

REVISION HISTORY

REVISION TYPE	MONTH/YEAR APPROVED
New Policy	07/2016
Choose an item.	
Choose an item.	
Choose an item.	
Choose an item.	
Choose an item.	
Choose an item.	

DATA GOVERNANCE & SECURITY

APPROVALS

FINAL APPROVAL

SENIOR VICE PRESIDENT FOR ADMINISTRATION & FINANCE

SEE EMAIL ATTACHMENT — 7/2/2016
Signature — **Date**

Sue Hodges Moore
Printed Name

PRESIDENTIAL APPROVAL

PRESIDENT

SEE EMAIL ATTACHMENT — 7/2/2016
Signature — **Date**

Geoffrey S. Mearns
Printed Name

BOARD OF REGENTS APPROVAL

BOARD OF REGENTS (IF FORWARDED BY PRESIDENT)

☒ **This policy WAS NOT forwarded to the Board of Regents.**
☐ **This policy WAS forwarded to the Board of Regents.**

☐ **The Board of Regents approved this policy on _____/_____/_____.**
(Attach a copy of Board of Regents meeting minutes showing approval of policy.)

☐ **The Board of Regents rejected this policy on _____/_____/_____.**
(Attach a copy of Board of Regents meeting minutes showing rejection of policy.)

POLICY COORDINATOR

7/2/2016
Signature — **Date**

Justin M. Duncan
Printed Name

Justin Duncan

From: Geoffrey Mearns
Sent: Saturday, July 02, 2016 11:23 AM
To: Sue Hodges Moore
Cc: Justin Duncan
Subject: Re: Data Policies for ET Review

Yes.

Geoffrey S. Mearns
President
Northern Kentucky University

> On Jul 1, 2016, at 9:04 AM, Sue Hodges Moore <moores4@nku.edu> wrote:
>
> Geoff, these policies have gone through the policy approval process and were thoroughly vetted by all of the necessary players. Do you approve? They take effect today.
>
> Thanks,
>
> Sue
>
> Sue Hodges Moore
> Senior Vice President for Administration and Finance Northern Kentucky
> University
> 836 Lucas Administrative Center
> Nunn Drive
> Highland Heights, KY 41099
> Office # 859-572-5349
[redacted]
>
[redacted]

[redacted]

>
> Colleagues,
>
> Attached are four draft policies:
>
>
> • Information Security
>
> • Information Security Incident Response
>
> • Data Governance & Security
>
> • Electronic Signature
>
> These policies have been through the open comment period and subsequently reviewed by each policy's drafting team. These policies are tentatively scheduled to take effect July 1. Please review the attached policies and provide feedback at your earliest convenience.
>
> -Sue
>
>
>
> Justin M. Duncan
> Coordinator, Institutional Effectiveness Division of Administration &
> Finance Northern Kentucky University AC 812
> O: (859) 572-7704
[redacted]
> duncanj6@nku.edu<mailto:duncanj6@nku.edu>
>
>
> <ETReviewDraft_DataGovernance6-24-16.docx>
> <ETReviewDraft_ElectronicSignature6-24-16.docx>
> <ETReviewDraft_InformationSecurity6-23-16.docx>
> <ETReviewDraft_ITIncidentResponse6-24-16.docx>

ELECTRONIC SIGNATURE

POLICY NUMBER: RESERVED FOR FUTURE USE
POLICY TYPE: ADMINISTRATIVE
RESPONSIBLE OFFICIAL TITLE: SENIOR VICE PRESIDENT, ADMINISTRATION & FINANCE
RESPONSIBLE OFFICE: DIVISION OF ADMINISTRATION & FINANCE
EFFECTIVE DATE:7/2/2016
NEXT REVIEW DATE: 6/1/2017
SUPERSEDES POLICY DATED: N/A
REQUIRES LEGAL/COMPLIANCE REVIEW:
(PER SECTION V. OF THE APPROVED POLICY REQUEST FORM) ☒YES ☐NO
REQUIRES I.T. POLICY COUNCIL REVIEW:
(PER SECTION V. OF THE APPROVED POLICY REQUEST FORM) ☒YES ☐NO
REQUIRES PROFESSIONAL CONCERNS COMMITTEE REVIEW:
(PER SECTION V. OF THE APPROVED POLICY REQUEST FORM) ☐YES ☒NO
REQUIRES HUMAN RESOURCES REVIEW:
(PER SECTION V. OF THE APPROVED POLICY REQUEST FORM) ☐YES ☒NO
REQUIRES BOARD OF REGENTS APPROVAL:
(PER SECTION V. OF THE APPROVED POLICY REQUEST FORM) ☐YES ☒NO

I. POLICY STATEMENT

To increase the efficiency of internal transactions that require authorization, the University may require that members of the University community use electronic signatures to conduct certain transactions that previously required handwritten signatures and approvals on paper documents.

This regulation establishes the policies and procedures by which the University designates University transactions for which e-signatures are required and recognizes and authenticates e-signatures.

This regulation also identifies University requirements for the use of electronic signatures, electronic transactions, and electronic records in conducting University transactions.

II. ENTITIES AFFECTED

This regulation applies to all units of the University and all members of the University community. Members of the University community include students and employees, prospective students and employees, business partners, and other individuals who are associated with the University.

III. DEFINITIONS

Define any terms within the policy that would help in the understanding or interpretation of the policy.

A. Agreement

Agreement means the bargain of the parties in fact, as found in their language or inferred from other circumstances and from rules, regulations and procedures that are given the effect of agreements under laws otherwise applicable to a particular transaction. (KRS 369.102(1))

B. Authentication

Authentication means the process of securely verifying the identity of an individual prior to allowing access to an electronic University service. Authentication ensures that the user who attempts to perform the function of an electronic signature is in fact who they say they are and is authorized to “sign.”

C. Authorization

Authorization means verifying that an authenticated user has permission to access specific electronic University services and/or perform certain operations.

D. Electronic

Electronic means relating to technology that has electrical, digital, magnetic, wireless, optical or electromagnetic capabilities or similar capabilities.

E. Electronic record or e-record

Electronic record or e-record means a record of information that is created, generated, sent, communicated, received or stored electronically.

F. Electronic signature or e-signature

Electronic signature or e-signature means an electronic sound, symbol or process that is attached to or logically associated with a record and that is executed or adopted with the intent to sign the record.

G. Electronic transaction or e-transaction

Electronic transaction or e-transaction means an action or set of actions that is conducted or performed, in whole or in part, electronically or via electronic records.

H. Information

Information means data, text, images, sounds, codes, computer programs, software, databases or similar items.

I. Non-Repudiation

Non-Repudiation means the inability of either party in a voluntary transaction to reject, disown, or disclaim the validity of that transaction.

J. Record

Record means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and that is retrievable in perceivable form.

K. Repudiation

Repudiation means the willful act of either party in a voluntary transaction to reject, disown, or disclaim the validity of that transaction.

L. Security Procedure

Security Procedure means a procedure that is used to verify that an electronic signature, record, or performance is that of a specific person; to determine that the person is authorized to sign the document; and, to detect changes or errors in the information in an electronic record. This includes a procedure that requires

the use of algorithms or other codes, identifying words or numbers or encryption, callback or other acknowledgment procedures.

M. Transaction

Transaction means an action or set of actions occurring between two (2) or more persons relating to the conduct of business, commercial, or governmental affairs.

N. Unit

Unit means the University organization conducting business by means of an e-signature such as a college, department, auxiliary, or administrative division.

O. University Transaction

A University Transaction means a transaction conducted in support of the University's teaching, research, or service mission.

IV. E-SIGNATURE TRANSACTION APPROVAL AND RESPONSIBILITIES

Provide the position titles, departments, or divisions that are responsible for implementing the policy. Next to each entity, enumerate the responsibilities necessary to implement and enforce the policy.

All electronic signature transactions shall follow guidelines and policy set forth under Kentucky Public Records law (KRS 171.410-171.740), the Kentucky Uniform Electronic Transactions Act [UETA] (KRS 369.101-369.120.) and The Health Insurance Portability & Accountability Act of 1996 [HIPAA] (Public Law 104-191).

A. For enterprise-level transactions, the principal University administrators, data custodians, and enterprise application system owners shall assess the potential for replacing a manual process/signature with an electronic process/signature and propose joint recommendations for implementation of automation, subject to approval by the senior vice president, executive vice president or vice president. Joint recommendations under this paragraph are subject to formal authorization by the relevant executive data custodian. Once a process for a University transaction is approved and automated, it is automatically subject to the provisions of this policy.

B. For all other transactions, the transaction to be enabled by e-signatures shall be evaluated by the unit, in conjunction with the office of Information Technology. (This includes any existing implied or explicit e-signatures in use prior to the adoption of this policy.) For risk assessment and review purposes, similar types of transactions may be grouped together under one agreement. Implemented e-signatures shall be reviewed periodically for appropriateness, and continued applicability.

V. POLICIES ON ELECTRONIC SIGNATURE USE

A. To the fullest extent permitted by law, the University accepts e-signatures as legally binding and equivalent to handwritten signatures to signify an agreement.

B. Students shall use electronic signatures to authorize all designated internal records and transactions. Examples include but are not limited to: registering for courses, accepting financial aid awards, paying student bills, obtaining unofficial transcripts, completing electronic forms, etc.

C. Employees shall use electronic signatures to authorize all designated internal documents. Examples include but are not limited to: submitting grades; viewing personal payroll data; accessing protected data through the administrative computing system and web applications provided by the unit; signing off on timesheets, etc.

D. Other members of the University Community, upon mutual agreement with the University may use electronic signatures to conduct designated University transactions and to formally acknowledge their agreement to University transactions in which they are parties by affixing an e-signature.

E. The University's right or option to conduct a University transaction on paper or in non-electronic form shall not affect the University's right, option, or obligation to have documents provided or made available in paper format.

VI. IMPLEMENTATION AND SECURITY PROCEDURES

A. Electronic signatures may be implemented using various methodologies depending on the risks associated with the transaction, and all relevant state, federal, and university regulations. Examples of transaction risks include: fraud, non-repudiation, and financial loss. The quality and security of the electronic signature method shall be commensurate with the risk and needed assurance of the authenticity of the signer.

B. The e-signature methodology shall be commensurate to the assurances needed for the risks identified. In addition, specifications for recording, documenting, and/or auditing the electronic signature as required for non-repudiation and other legal requirements shall also be determined by the unit.

C. The University shall adopt security procedures for e-signatures, e-transactions and e-records that are practical, secure, and balance risk and cost. It is not the intent of this regulation to eliminate all risk, but rather to provide a process for undertaking an appropriate analysis prior to approving the use of e-signatures, e-transactions or e-records for specific University transactions; and, based on such analysis, to designate those University transactions in which e-signatures, e-transactions and e-records shall be required in place of handwritten documents.

D. The security requirements for a University transaction include, but are not limited to Acceptable Use Policy, Security Policy, Web Accessibility Policy, Discretionary Expenditure Policy, and other relevant policies deemed appropriate by Senior Leadership.

VII. VIOLATIONS AND SANCTIONS

A. It is a violation of this regulation for an individual to sign a University transaction on behalf of another individual, unless he or she has been granted specific authority by that individual.

B. Individuals shall report any suspect or fraudulent activities related to electronic signatures immediately to any manager or supervisor in the appropriate department, college, or division.

C. Employees who falsify electronic signatures or otherwise violate this regulation are subject to disciplinary action, up to and including termination of employment and criminal prosecution under applicable federal and state laws.

D. Students who falsify electronic signatures or otherwise violate this regulation are subject to disciplinary action under the Student Code of Conduct and criminal prosecution under applicable federal and state laws.

E. Other members of the University community who falsify electronic signatures or otherwise violate this regulation are subject to appropriate sanctions, including but not limited to termination of the relationship and criminal prosecution under applicable federal and state laws.

VIII. REFERENCES AND RELATED MATERIALS

REFERENCES & FORMS

The Electronic Signatures Act: 15 USC Chapter 96 ; http://www.gpo.gov/fdsys/pkg/PLAW-106publ229/content-detail.html
Family Educational Rights and Privacy Act (FERPA): 34 CFE Part 99; Final Rule;
http://www2.ed.gov/legislation/FedRegister/finrule/2004-2/042104a.pdf
E-authentication Guidance for Federal Agencies: OMB M04-04;
http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
The Kentucky Uniform Electronic Transactions Act: KRS 369.101-120; http://www.lrc.ky.gov/KRS/369-00/CHAPTER.HTM
Kentucky State Electronic Signature Recordkeeping Guidelines;
http://kdla.ky.gov/records/Documents/Electronic%20Signature%20Recommendation%20Version%201.pdf
NIST Electronic Authentication Guidelines: 800-63; http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

RELATED POLICIES

REVISION HISTORY

REVISION TYPE	MONTH/YEAR APPROVED
New Policy	07/2016
Choose an item.	
Choose an item.	
Choose an item.	
Choose an item.	
Choose an item.	
Choose an item.	

ELECTRONIC SIGNATURE

APPROVALS

FINAL APPROVAL

SENIOR VICE PRESIDENT FOR ADMINISTRATION & FINANCE

SEE EMAIL ATTACHMENT — 7/2/2016
Signature — **Date**

Sue Hodges Moore
Printed Name

PRESIDENTIAL APPROVAL

PRESIDENT

SEE EMAIL ATTACHMENT — 7/2/2016
Signature — **Date**

Geoffrey S. Mearns
Printed Name

BOARD OF REGENTS APPROVAL

BOARD OF REGENTS (IF FORWARDED BY PRESIDENT)

☒ **This policy WAS NOT forwarded to the Board of Regents.**
☐ **This policy WAS forwarded to the Board of Regents.**

☐ **The Board of Regents approved this policy on _____/_____/_____.**
(Attach a copy of Board of Regents meeting minutes showing approval of policy.)

☐ **The Board of Regents rejected this policy on _____/_____/_____.**
(Attach a copy of Board of Regents meeting minutes showing rejection of policy.)

POLICY COORDINATOR

7/2/2016
Signature — **Date**

Justin M. Duncan
Printed Name

Justin Duncan

From: Geoffrey Mearns
Sent: Saturday, July 02, 2016 11:23 AM
To: Sue Hodges Moore
Cc: Justin Duncan
Subject: Re: Data Policies for ET Review

Yes.

Geoffrey S. Mearns
President
Northern Kentucky University

> On Jul 1, 2016, at 9:04 AM, Sue Hodges Moore <moores4@nku.edu> wrote:
>
> Geoff, these policies have gone through the policy approval process and were thoroughly vetted by all of the necessary players. Do you approve? They take effect today.
>
> Thanks,
>
> Sue
>
> Sue Hodges Moore
> Senior Vice President for Administration and Finance Northern Kentucky
> University
> 836 Lucas Administrative Center
> Nunn Drive
> Highland Heights, KY 41099
> Office # 859-572-5349
[redacted]
>
[redacted]

[redacted]

>
> Colleagues,
>
> Attached are four draft policies:
>
>
> • Information Security
>
> • Information Security Incident Response
>
> • Data Governance & Security
>
> • Electronic Signature
>
> These policies have been through the open comment period and subsequently reviewed by each policy's drafting team. These policies are tentatively scheduled to take effect July 1. Please review the attached policies and provide feedback at your earliest convenience.
>
> -Sue
>
>
>
> Justin M. Duncan
> Coordinator, Institutional Effectiveness Division of Administration &
> Finance Northern Kentucky University AC 812
> O: (859) 572-7704
[redacted]
> duncanj6@nku.edu<mailto:duncanj6@nku.edu>
>
>
> <ETReviewDraft_DataGovernance6-24-16.docx>
> <ETReviewDraft_ElectronicSignature6-24-16.docx>
> <ETReviewDraft_InformationSecurity6-23-16.docx>
> <ETReviewDraft_ITIncidentResponse6-24-16.docx>

To: Chief Information Officer, Office of Information Technology
From: Prof. Ken Katkin, PCC Chair
Re: NKU Policy on "Electronic Signature Policy"
Filed: June 6, 2016

I am the Chair of the Professional Concerns Committee (PCC) of the NKU Faculty Senate. Neither the PCC nor the Faculty Senate meet over the summer. I have not conferred with any other member of the PCC before filing these comments. Accordingly, the following comments represent only my own views. However, I intend to disseminate these comments to the incoming PCC Members in advance of our first meeting in Fall 2016.

I offer the following comment on the draft Policy proposal entitled "Electronic Signature Policy."

Section VI.C of the draft Policy states that "Employees shall use electronic signatures to authorize all designated internal documents. Examples include but are not limited to: submitting grades. . . . " The application of this policy to "submitting grades" seems inconsistent with the policy statement at the beginning of the draft document, which states that the purpose of the policy is to facilitate the use of electronic signatures "to conduct certain transactions that previously required handwritten signatures and approvals on paper documents."

At present, the submission of grades does not generally require handwritten signatures and approvals on paper documents. Rather, NKU faculty members routinely enter grades directly into Web Sites such as MyNKU or Blackboard. In the Chase College of Law, where most grading is anonymous, faculty members routinely email grades (identified by student number) to the Chase Registrar from the faculty members' nku email addresses.

From a faculty perspective, it is important that the reference to "submitting grades" be deleted because Section VIII.C of the draft regulation states that "Employees who . . . otherwise violate this regulation are subject to disciplinary action, up to and including termination of employment and criminal prosecution under applicable federal and state laws." Seemingly, this means that a faculty member who continues to submit grades via MyNKU or Blackboard—or who emails grades to a registrar—would potentially be subject to disciplinary action, up to and including termination of employment. While a move to replace hand-signatures with electronic signatures in the University's business operations seems unobjectionable, the transition should not create new traps for unwary faculty members.

MEMORANDUM

To: PCC
From: Prof. Ken Katkin, PCC Chair
Re: Proposed NKU Policy on "Retired Faculty Participation on Sponsored Projects"
Date: Aug 25, 2016

Comments in NKU Policy Proceeding Due: Sept 29, 2016

On Aug 15, 2016, NKU initiated a notice-and-comment proceeding to solicit comment on a proposed policy on "Retired Faculty Participation on Sponsored Projects." If adopted as drafted, this policy would effectively downgrade the status of emeritus faculty members, and would make it harder for emeriti to being paid for work performed in furtherance of externally-funded research.

In this Memorandum, I raise several concerns about the proposal. Other PCC members may have other concerns, as well. After considering these and any other concerns raised by PCC members, PCC should consider whether it would like to file comments in this proceeding. These are my concerns:

(1) Throughout the current draft policy proposal, emeritus faculty members are repeatedly and tendentiously referred to as "retired" or "former" faculty members. This word-choice disparages the status of emeritus faculty and misleadingly connotes that emeriti no longer hold rank, title, or affiliation with the university. In fact, the NKU Faculty Handbook makes clear that "[e]meritus faculty are tenured faculty or administrators who hold faculty rank, who, upon retirement, . . . have been conferred emeritus status by the Board of Regents. Such persons hold the title and rank held immediately prior to their retirement, followed by the title 'emeritus.' " NKU Faculty Handbook § 1.7.1 (emphasis added). In order to avoid belittling our emeritus faculty, throughout the document the words "former" and "retired" should everywhere be replaced with the word "emeritus."

(2) The current draft policy creates ambiguity about the classification of faculty members going through phased retirement. Many such faculty members might carry less-than-full-time workloads during the phase period. Do such faculty members nonetheless qualify as "full-time" and "permanent" faculty members under this policy? Should they? Should a sentence be added to clarify that: "irrespective of teaching load, tenured faculty members undergoing phased retirement shall qualify as full-time permanent faculty members for purposes of this policy."

(3) The current draft policy proposal states that "[c]redentialing by the Office of the Provost is required if the [emeritus] faculty member supervises students who are receiving academic credit for the research experience." It is not clear whether such credentialing is currently required when emeritus faculty members teach ordinary courses at NKU. Should PCC consider recommending that the same

credentialing process that applies when emeritus faculty teach courses should also apply when emeritus faculty members supervise student research?

(4) The current draft policy proposal states that when an emeritus faculty member seeks appointment as a senior research scientist/scholar on the sponsored project of a full-time faculty member at NKU, the emeritus faculty member "will be given the additional title of senior research scientist/scholar, to be held during the period of the sponsored." Although the grant of an additional title seems unobjectionable, the perceived need for such a title might possibly reflect insufficient appreciation that the rank and title of emeritus professor would already be held by anyone affected by this policy. For that reason, perhaps this sentence should be amended to read:

> When an emeritus faculty member seeks to participate in work on a sponsored research project at NKU, the emeritus faculty member will be given pre- and post-award administrative support and may also be given the additional title of senior research scientist/scholar, to be held during the period of the sponsored project. This designation requires the approval of the department chair, dean and Vice Provost for Graduate Education, Research, and Outreach.

These thoughts are offered as a starting point for PCC's consideration of this issue.

Retired Faculty Participation on Sponsored Projects

Policy Number:	**Reserved for future use**
Policy Link:	
Responsible Official:	**Provost**
Responsible Office:	**Provost**
Effective date:	**Click here to enter a date.**
Next review date:	**Click here to enter a date.**
Supersedes policy dated:	**N/A**
Approved by:	**Choose an item.**

I. Policy Statement

Several important considerations determine whether NKU will sponsor, totally or in part, retired faculty members' participation on sponsored projects, and whether it will authorize research appointments for retired faculty members. In making its decision NKU must take into account the contribution of the proposed research to the NKU community, its demand upon physical and administrative facilities, pre- and post-award administrative support, and its direct and indirect effects upon other research and programs of the university.

Only full-time permanent faculty and staff may apply as primary investigators or project directors for sponsored projects at NKU. Full-time members of faculty may participate in a sponsored project beyond their retirement date, but upon that date the project must transition to a new full-time NKU Primary Investigator. Once retired, a former faculty member may participate on a sponsored project as a Co-Primary Investigator or other personnel, subject to approval by the appropriate chair, dean, and Vice Provost for Graduate Education, Research, and Outreach. A retired faculty member serving as a Co-Primary Investigator on a sponsored project may supervise students with approval from the department chair and dean. Credentialing by the Office of the Provost is required if the retired faculty member supervises students who are receiving academic credit for the research experience.

At the discretion of the department chair and dean, and based on the availability of resources, retired faculty participating on sponsored projects may be provided office space, office support, mailing privileges, and laboratory space, when used for professional purposes in support of NKU's mission and the grant objectives.

When a retired faculty member seeks appointment as a senior research scientist/scholar on the sponsored project of a full-time faculty member at NKU, he/she will be given pre-and post-award administrative support and the additional title of senior research scientist/scholar, to be held during the period of the sponsored project. This designation requires the approval of the department chair, dean and Vice Provost for Graduate Education, Research, and Outreach.

A retired faculty member who is appointed as senior research scientist/scholar under the above conditions may be compensated for effort from the sponsored project on a part-time or full-time basis as a contractor, but not as an employee. The contractor rate will be set at the rate of compensation at the time of retirement, consistent with the OMB Circular A-21 guidelines (see below). Retired faculty may not work more than 30 hours/week. Fringe benefits will not be paid

to a contractor. In no case may compensation exceed the available funding from the sponsored project.
OMB Circular A-21, 10.d.(1)(e) states that institutions must follow their own policies and salaries are to be consistent with those paid by the institution.
http://www.whitehouse.gov/omb/circulars/a021/a21_2004.html

II. Entities Affected

Faculty, Deans, Provost, Office of Research, Grants & Contracts, Vice Provost for Graduate Education, Research and Outreach, Department Charis, Human Resources and Office of the Comptroller

III. Authority

Chair, Dean, Vice Provost for Graduate Education, Research and Outreach, and Provost

IV. Definitions

V. Responsibilities

Department Chairs, Deans, and Vice Provost for Graduate Education, Research and Outreach must approve requests. Credentialing requires approve by Provost if student supervision involved.

VI. Committee

VII. Procedures

VIII. Reporting Requirements

IX. Exceptions

X. Training

XI. Communications

References and Related Materials

References:
Related Policies:
Related Forms:
Revision History:

INFORMATION SECURITY

POLICY NUMBER: RESERVED FOR FUTURE USE
POLICY TYPE: ADMINISTRATIVE
RESPONSIBLE OFFICIAL TITLE: CHIEF INFORMATION OFFICER
RESPONSIBLE OFFICE: OFFICE OF INFORMATION TECHNOLOGY
EFFECTIVE DATE:7/2/2016
NEXT REVIEW DATE: 6/1/2017
SUPERSEDES POLICY DATED: N/A
REQUIRES LEGAL/COMPLIANCE REVIEW:
(PER SECTION V. OF THE APPROVED POLICY REQUEST FORM) ☒YES ☐NO
REQUIRES I.T. POLICY COUNCIL REVIEW:
(PER SECTION V. OF THE APPROVED POLICY REQUEST FORM) ☒YES ☐NO
REQUIRES PROFESSIONAL CONCERNS COMMITTEE REVIEW:
(PER SECTION V. OF THE APPROVED POLICY REQUEST FORM) ☐YES ☒NO
REQUIRES HUMAN RESOURCES REVIEW:
(PER SECTION V. OF THE APPROVED POLICY REQUEST FORM) ☐YES ☒NO
REQUIRES BOARD OF REGENTS APPROVAL:
(PER SECTION V. OF THE APPROVED POLICY REQUEST FORM) ☐YES ☒NO

I. POLICY STATEMENT

Northern Kentucky University recognizes the obligation to protect confidentiality, maintain the integrity, and ensure appropriate availability of information regarding students, faculty, staff, alumni, and customers, and to provide proper administrative, technical and physical safeguards to protect university information assets per NKU's data classification categories (see below).

The NKU Information Security Policy covers:

- information and data that are acquired, transmitted, processed, managed, transferred, stored, and/or maintained by NKU organizations;
- security of passwords, decryption, and encryption processes
- all data systems and equipment including departmental, divisional and other ancillary systems, as well as information residing on these systems and equipment;
- work/home/personal electronic and mobile devices of NKU faculty, staff, alumni, and administrators which access information technology information and data;

Each member of the NKU campus community is personally responsible for the security and protection of NKU information and data resources over which he or she has access, use, and/or control, and must adhere to the Acceptable Use Policy. Resources to be protected include data stored on any laptops, desktops, mobile devices (iPads, tablets, cell phones, etc.), any data which are accessed, transferred or stored, regardless of format (text, graphic, audio), passwords, decryption and encryption processes. The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, inappropriate or unsafe transmission or storage of confidential data, inappropriate release of confidential or private information (whether accidental or intentional) or inadvertent compromise, such as theft or loss.

It is the policy of NKU to:

- safeguard personal and confidential information of NKU students, faculty, staff, alumni, and customers, regardless of format or medium;
- protect against anticipated threats or hazards to the physical security or integrity of NKU information and data assets, including data files and hardware equipment;
- ensure campus compliance with federal and state laws, regulations, NKU policies, procedures, and standards regarding information security, privacy and prevention of threats, breaches, and intrusions;
- ensure employees, departments, and organizations operate in compliance with state and federal laws for access, usage, and transmission of electronic data (FERPA, HIPAA, etc). Compliance with state law includes following the State University Model Records Retention Schedule and NKU Records Management Policy for the retention and disposal of electronic records
- ensure departments and organizations are held responsible for implementing appropriate managerial, operational, physical, and technical controls for access, usage, transmission, storage, and disposal of NKU data in compliance with this policy.

II. ENTITIES AFFECTED

This policy applies to all individuals who access, use, or control NKU information or data resources. Those individuals covered include, but are not limited to faculty, staff, students, contractors, alumni, and individuals authorized by affiliated institutions or organizations.

III. DEFINITIONS

Classification Definitions and Examples

The table on the next page clarifies the nature of each data category and provides criteria for determining which classification is appropriate for a particular set of data.

	Confidential Data *(highest, most sensitive)*	**Private Data** *(moderate level of sensitivity)*	**Public Data** *(low level of sensitivity)*
Legal Requirements	Protection of data is required by law (i.e. HIPAA, FERPA, GLBA, etc.)	NKU has a contractual obligation to protect the data	Governed by the Kentucky Open Records Act, K.R.S. §§ 61.870 to 61.884
Reputation Risk	High	Medium	Low
Other Institutional Risks	Information which provides access to resources, physical or virtual	Smaller subsets of protected data from a school or department	General university information
Access	Only those individuals designated with approved access, signed non- disclosure agreements, and a need-to-know	NKU employees and non-employees who have a business need-to-know	Unrestricted
Examples	• Student education records • Individual health records and information • Human subjects research data that identifies individuals • Prospective students • Personally Identifiable Financial Information • Campus Security Systems and Details • Credit card numbers • Certain management information • Social Security Numbers • Government restricted and/or classified information • Financial transactions of students and employees • Personnel records (Although certain records contained within employee personnel files may be “public records” subject to disclosure, personnel files should be maintained as confidential data and disclosure of “public records” shall only be made after a case-by- case determination.)	• Information resources with access to confidential data • Research data or results that are not confidential data • Information covered by non-disclosure agreements • Materials for performance of official duties • Proprietary information of NKU or others contained within proposals, contracts, or license agreements	• Campus maps • Directory information (e.g. Contact Information, Find It) • Departmental Websites • Academic course descriptions • News • Information posted on university website • Budgets • Purchase Orders • All institutional data made available to the general public by the Open Records Act

IV. RESPONSIBILITIES

All employees working with NKU data are responsible for properly protecting that data. The following protective measures should be used as a foundation for your due diligence in keeping data secure.

DO:

- Understand NKU's Data Classification Categories (see addendum):
- The NKU Data Classification categories will be used as reference in defining Confidential, Private, and Public data
- Confidential and Private data are to be protected from disclosure, breaches, unauthorized alteration, and data loss.
    - Examples of Confidential data include, but are not limited to social security numbers, drivers license numbers, credit card or banking information, student academic information such as grades or GPA, etc.
    - Examples of Private data include but are not limited to academic reports, research data, technical reporting such as system logs, faculty tenure evaluations, etc.
    - Public data items include campus promotional materials, class schedules, catalog information, annual reports, press releases, directory information, etc.
- For a more comprehensive list of examples and legal requirements, please visit: http://datagovernance.nku.edu/content/dam/DataGovernance/docs/Data%20Classification.pdf
- Follow FERPA guidelines: The Family Educational Rights and Privacy Act (FERPA) guidelines are maintained and must be adhered to for student rights and controlled disclosures of their records. For information regarding NKU and FERPA guidelines, see http://www.nku.edu/~registrar
- Use Encryption for Laptops: All NKU owned laptops will be encrypted. NKU IT personnel will assist in providing encryption services. NKU employees are not permitted to remove encryption from laptops, and exceptions will only be permitted with VP and CIO approval.
- Store Data within NKU Networks: Data that is classified as Confidential or Private should be stored within the NKU file server network ("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. IT can assist if you require storage quotas that exceeds currently allocated amounts.
- Use Virtual Private Network (VPN) to access data when not on campus (home, travel, etc.) Our VPN technology provides security when used from remote locations. See http://oit.nku.edu/vpn.html
- Only access confidential and/or private data through encrypted or secure networks when on campus
- A secured login must be used when leaving your device unattended. (i.e. When leaving your computer unattended, you must lock your screen and require login to re-access)
- Do dispose of non-permanent confidential and private data as soon as possible according to the State University Model Records Retention Schedule to reduce risk and potential liability.
- Do report any breaches, inappropriate disclosures, abuses, data loss, or unauthorized alterations to abuse@nku.edu
- Do require personnel handling confidential or private data to sign non-disclosure statements.
- If a personally owned device is lost or stolen and has been used to access confidential or private information, it is the individual's responsibility to report this to abuse@nku.edu

DO NOT:

- Store Confidential or Private data within Cloud and Third Party Data Services: The use of individual "cloud" based storage services such as Google Docs, Drop Box, Amazon, iCloud, or other external storage for NKU Confidential or Private data is prohibited. (Microsoft OneDrive, provided through NKU, is the only cloud based storage service approved for storage of NKU confidential or private data.) Third party contracts that require data collection, distribution, or interfaces with NKU systems will require Legal, IT, and Procurement approval.
- Store Confidential or Private data on portable or mobile storage devices: "Flash" or "Thumb" drives are prohibited when storing NKU Confidential or Private Data, unless the device and/or data has been properly encrypted. For assistance with encryption of mobile and portable devices, please call the IT Service Center.
- Share Passwords: Sharing or using weak passwords may put NKU data at risk. Even in the safest environment, a password disclosure by unauthorized personnel or hackers could result in a data breach. Use strong passwords, and do not share with friends, co-workers or family.
- Email Messages: Do not send Confidential or Private data through email. Even internal email messages are vulnerable to possible attack.
- Do not mix NKU confidential or private data with individual personal records.

V. VIOLATIONS

Any university employee, student or non-university individual who stores university data outside NKU networks and secure servers without proper permissions and protection measures is in violation of this policy and will be subject to appropriate disciplinary action, including possible dismissal and/or legal action.

Depending upon the nature and seriousness of the infraction, any faculty, staff, student, contractor, alumni, or other user within the university network found to have violated this policy may be:

- removed from the network
- subject to disciplinary action, up to and including termination of employment or expulsion
- held personally responsible for any fees, charges or other costs to recover from incidents, including fraud protection for breach of information
- subject to legal actions from internal and external agencies.

Please see the Acceptable Use Policy for additional details on IT Usage and Policy enforcement, and contact the IT Help Desk or (x6911) for assistance with security needs.

VI. EXCEPTIONS

Exceptions are limited in regards to data and information protection measures. If an individual is required to store highly sensitive, Confidential or Private data for a business need that are outside NKU managed networks, that individual must obtain permission from the Chief Information Officer and the area Vice President.

VII. REFERENCES AND RELATED MATERIALS

REFERENCES & FORMS

RELATED POLICIES

REVISION HISTORY

REVISION TYPE	MONTH/YEAR APPROVED
New Policy	07/2016
Choose an item.	
Choose an item.	
Choose an item.	
Choose an item.	
Choose an item.	
Choose an item.	

INFORMATION SECURITY

APPROVALS

FINAL APPROVAL

SENIOR VICE PRESIDENT FOR ADMINISTRATION & FINANCE

SEE EMAIL ATTACHMENT — 7/2/2016
Signature — **Date**

Sue Hodges Moore
Printed Name

PRESIDENTIAL APPROVAL

PRESIDENT

SEE EMAIL ATTACHMENT — 7/2/2016
Signature — **Date**

Geoffrey S. Mearns
Printed Name

BOARD OF REGENTS APPROVAL

BOARD OF REGENTS (IF FORWARDED BY PRESIDENT)

☒ **This policy WAS NOT forwarded to the Board of Regents.**
☐ **This policy WAS forwarded to the Board of Regents.**

☐ **The Board of Regents approved this policy on _____/_____/_____.**
(Attach a copy of Board of Regents meeting minutes showing approval of policy.)

☐ **The Board of Regents rejected this policy on _____/_____/_____.**
(Attach a copy of Board of Regents meeting minutes showing rejection of policy.)

POLICY COORDINATOR

7/2/2016
Signature — **Date**

Justin M. Duncan
Printed Name

Justin Duncan

From: Geoffrey Mearns
Sent: Saturday, July 02, 2016 11:23 AM
To: Sue Hodges Moore
Cc: Justin Duncan
Subject: Re: Data Policies for ET Review

Yes.

Geoffrey S. Mearns
President
Northern Kentucky University

> On Jul 1, 2016, at 9:04 AM, Sue Hodges Moore <moores4@nku.edu> wrote:
>
> Geoff, these policies have gone through the policy approval process and were thoroughly vetted by all of the necessary players. Do you approve? They take effect today.
>
> Thanks,
>
> Sue
>
> Sue Hodges Moore
> Senior Vice President for Administration and Finance Northern Kentucky
> University
> 836 Lucas Administrative Center
> Nunn Drive
> Highland Heights, KY 41099
> Office # 859-572-5349
[redacted]
>
[redacted]

[redacted]

>
> Colleagues,
>
> Attached are four draft policies:
>
>
> • Information Security
>
> • Information Security Incident Response
>
> • Data Governance & Security
>
> • Electronic Signature
>
> These policies have been through the open comment period and subsequently reviewed by each policy's drafting team. These policies are tentatively scheduled to take effect July 1. Please review the attached policies and provide feedback at your earliest convenience.
>
> -Sue
>
>
>
> Justin M. Duncan
> Coordinator, Institutional Effectiveness Division of Administration &
> Finance Northern Kentucky University AC 812
> O: (859) 572-7704
[redacted]
> duncanj6@nku.edu<mailto:duncanj6@nku.edu>
>
>
> <ETReviewDraft_DataGovernance6-24-16.docx>
> <ETReviewDraft_ElectronicSignature6-24-16.docx>
> <ETReviewDraft_InformationSecurity6-23-16.docx>
> <ETReviewDraft_ITIncidentResponse6-24-16.docx>

To: Chief Information Officer, Office of Information Technology
From: Prof. Ken Katkin, PCC Chair
Re: NKU Policy on "Information Security Policy"
Filed: June 6, 2016

I am the Chair of the Professional Concerns Committee (PCC) of the NKU Faculty Senate. Neither the PCC nor the Faculty Senate meet over the summer. I have not conferred with any other member of the PCC before filing these comments. Accordingly, the following comments represent only my own views. However, I intend to disseminate these comments to the incoming PCC Members in advance of our first meeting in Fall 2016.

I offer the following comments on the draft Policy proposal entitled "Information Security Policy."

(1) On Page One and Page Five, the draft policy cross-references another NKU Policy entitled "Acceptable Use Policy." However, the hyperlink in the cross-reference is dead, making it difficult for the reader to locate the "Acceptable Use Policy" being cross-referenced.

(2) On Page Two, the second bullet point contains a reference to "HIPPA." This reference probably refers to the Health Insurance Portability and Accountability Act of 1996, which is properly abbreviated "HIPAA."

(3) On Page Three, the data classification table adopts a definition of "public data" that places excessive and undesirable restrictions on the use and dissemination of such data. In order to preserve the open information sharing requirements of NKU's academic culture, to protect the freedom of speech of all NKU community members, and to comply with the letter and spirit of Kentucky's Open Records Act, the following revisions to the draft language in the "public data" column are needed.

(a) In the current draft, "access" to "public data" is limited only to "NKU affiliates and general public with a need-to-know." This language raises the possibility that an NKU community member could be disciplined for sharing public data with someone who does not have a "need-to-know." By definition, "public data" should be available to the public, without any threshold need to demonstrate any need-to-know. See Ky. Rev. Stat. § 61.872(2) ("Any person shall have the right to inspect public records."). The language describing who is entitled to have "access" to "public data" should therefore be amended to simply read: "unrestricted."

(b) In the current draft, the language describing "legal requirements" of "public data" seems not to comply with the presumption of openness set forth in the Kentucky Open Records Act and in the University's own stated commitment to preserve the open information sharing requirements of NKU's academic culture. As drafted, this policy language states that protection of public data "is at the discretion of the owner or custodian" of the data. This language seems to imply that the owner or custodian of public data has discretion to withhold public data from the public. The Kentucky Open Records Act, in contrast, codifies into Kentucky law the policy "that free and open examination of public records is in the public interest and the exceptions provided for by KRS 61.878 or otherwise provided by law shall be strictly construed, even though such examination may cause inconvenience or embarrassment to public officials or others." Ky. Rev. Stat. § 61.871. In most instances, therefore, if an NKU owner or custodian were to exercise "discretion" to deny access to public data, such an exercise

would violate the Kentucky Open Records Act. To resolve this problem, the language describing the "legal requirements" of "public data" should be amended to read: "is governed by the Kentucky Open Records Act, KRS §§ 61.870 to 61.884."

(c) In the current draft, the list of "examples" of "public data" seems misleadingly restrictive, in that all but one example concerns material that the University voluntarily publicizes through its Web Site. In fact, however, the category of "public data" includes all institutional data that is not "confidential data" or "private data," including a great deal of data (such as salary data) that is not routinely or voluntarily posted on University Web Sites. The Kentucky Open Records Act defines "public records" as "all books, papers, maps, photographs, cards, tapes, discs, diskettes, recordings, software, or other documentation regardless of physical form or characteristics, which are prepared, owned, used, in the possession of or retained by a public agency," Ky. Rev. Stat. § 61.870(2), except those that fall within a specific exception set forth at Ky. Rev. Stat. § 61.878. To avoid creating the misleading impression that "public data" is limited only to categories of information that the University chooses voluntarily to publicize, an additional bullet point should be added to the list of examples, which would read: "all institutional data made available to the general public by the Kentucky Open Records Act."

(4) On Page Three, the three sub-bullet points at the bottom of the page each contain misleading, unclear, or unhelpful examples. In particular:

(a) In the draft policy, examples of "confidential data" include "student academic information such as grades or GPA, etc." Under the Kentucky statute on Personal Information Security and Breach Investigations being implemented by this policy, in contrast, such "personal information" is confidential only where it includes unique individual identifying information such as "an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image." Ky. Rev. Stat. § 61.931(6); see also Ky. Rev. Stat. § 61.878(2) ("No exemption in [the Kentucky Open Records Act] shall be construed to prohibit disclosure of statistical information not descriptive of any readily identifiable person."). At NKU, it is relatively common practice for summary grading data to be disseminated in ways that identify the professor and the course, but not the students. Such information dissemination is valuable, is not prohibited by Kentucky law, and should not be discouraged by this policy.

(b) In the draft policy, examples of "private data" include "academic reports, research data, technical reporting such as system logs, faculty tenure evaluations, etc." As discussed above, most items on this list are properly classified as "public records" unless some specific exception to the Kentucky Open Records applies.

(c) In the draft policy, examples of "public data" include "campus promotional materials, class schedules, catalog information, annual reports, press releases, directory information, etc." Because every item on this list is a form of institutional data that the University voluntarily chooses to disseminate, the list creates the misleading and false impression that no institutional data can qualify as "public data" unless the University voluntarily decides to disseminate such data. As discussed above, the Kentucky Open Records Act provides a much larger and more inclusive definition of "public information" that specifically includes information whose dissemination "may cause inconvenience or embarrassment to public officials or others." Ky. Rev. Stat. § 61.871.

Because these three bullet points are both misleading and unnecessary, I recommend that they simply be deleted. The reader can rely on the Table that appears on the same page for examples, if necessary.

(5) It is unclear whether the data security "do's and don'ts" set forth on Pages Four and Five of the draft policy are intended to apply to the process of calculating student grades that is routinely performed by individual faculty members. Such application would be burdensome and cumbersome for many faculty members, and is not contemplated by FERPA or by Kentucky Law. Indeed, neither FERPA, nor the US Department of Education regulations that implement FERPA, require any data security standards whatsoever. See 20 U.S.C. § 1232g; 34 C.F.R. Part 99. Rather, FERPA requires only that NKU must not have "a policy or practice of permitting the release of education records . . . without the written consent of their parents. . . . " 20 U.S.C. § 1232g(b)(1). Similarly, the US Department of Education regulations that implement FERPA require only that "[a]n educational agency or institution that does not use physical or technological access controls must ensure that its administrative policy for controlling access to education records is effective. . . . " 34 C.F.R. § 99.31(a)(1)(ii). In addition, the Kentucky statute on Personal Information Security and Breach Investigations that is being implemented by this policy specifically EXCLUDES educational records from its coverage. See Ky. Rev. Stat. §61.931(6)(f) ("Personal information" means an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with . . . individually identifiable health information . . . EXCEPT FOR EDUCATION RECORDS COVERED BY the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g.") (emphasis added).

Moreover, professors' gradebooks—including electronic gradebooks saved as files in programs such as MS EXCEL—are not "education records" under FERPA. See 34 C.F.R. § 99.3(b)(1) ("The term 'education records' does not include: Records that are kept in the sole possession of the maker, are used only as a personal memory aid, and are not accessible or revealed to any other person except a temporary substitute for the maker of the record."). Rather, as the United States Supreme Court explained in 2002, students' grades first become "education records" only when they are submitted to the registrar, and not earlier:

> FERPA requires "a record" of access for each pupil. This single record must be kept "with the education records." This suggests Congress contemplated that education records would be kept in one place with a single record of access. By describing a "school official" and "his assistants" as the personnel responsible for the custody of the records, FERPA implies that education records are institutional records kept by a single central custodian, such as a registrar, not individual assignments handled by many student graders in their separate classrooms.

Owasso Independent School Dist. No. I-011 v. Falvo, 534 U.S. 426, 434-35 (2002).

As drafted, the data security "DO'S & DON'TS" set forth on Pages Four and Five of the draft policy might be construed to prohibit NKU faculty members from calculating student grades for particular assignments on their own home computers, or from using email or a flash drive to transfer worksheets containing such calculations back to their office computers. While ideally all NKU faculty members will one day receive training and technology that will facilitate the use of more secure solutions at all times, this is not the case today. Accordingly, the draft policy should be revised to clarify that professors' individual gradebooks or grading worksheets are not covered by the policy unless they are also covered by FERPA.

(6) On Page Five, 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, I recommend adding language clarifying that:

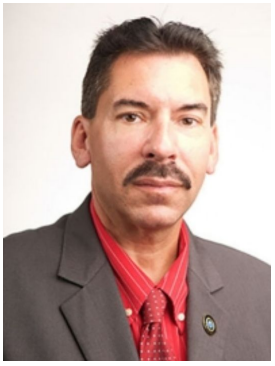
> Such penalties shall be levied through ordinary disciplinary procedures set forth in other official University personnel policy documents, such as the NKU Personnel Policies and Procedure Manual, the NKU Faculty Policies and Procedures (the "Faculty Handbook"), or the Chase College of Law Faculty Policies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

What did former NKU top cop do about possible rape confession?

James Pilcher, jpilcher@enquirer.com *5:40 p.m. EDT August 14, 2016*



(Photo: Provided/Northern Kentucky University)

Update, 3:20 p.m. Sunday: Northern Kentucky University's president issued a public statement addressed to colleagues about The Enquirer's article Sunday, saying that NKU "has robust policies and procedures dealing with sexual misconduct in all forms, including sexual assault."

Geoffrey S. Mearns declared parts of the article "misleading," but did not elaborate in his statement (http://president.nku.edu/campuscommunication/campussafety.html).

Mearns declined multiple interview requests from The Enquirer through an NKU spokeswoman.

Previous reporting: HIGHLAND HEIGHTS - In 2013, a newly minted freshman arrived at Northern Kentucky University on a full academic scholarship.

Within a few months, she says she was raped by a fellow freshman.

But instead of pressing criminal charges, the woman kept it to herself for several months. After eventually seeking counseling, she decided to take the case through the school's internal administrative discipline system. Her would-be attacker was found to have probably assaulted her even as he claimed innocence. His punishment: a possible suspension if he broke any more rules and orders to stay away from the woman and out of certain areas on campus.

Yet she continually ran across her accused attacker on campus, in possible violation of those sanctions. After several such incidents and a perception that the school didn't enforce those sanctions and treated her badly, she sued the school in federal court under Title IX, the federal law that covers sexual equality, harassment and assault on college campuses. That treatment, according to the lawsuit, included an email from NKU's police chief that faculty members and other students saw as accusing the woman of slandering the male student.

The email, written last September, said the female complainant "has been publicly slandering the male student." This came even after the administrative process ruled against the male student, although the police chief later said it was in reference to possible allegations by the alleged victim that the male student was dealing drugs.

And now, The Enquirer has learned the former police chief acknowledged in a deposition that two unidentified friends of the woman's alleged attacker told him that the man confessed to the attack just prior to sending that email.

Furthermore, former chief Les Kachurek testified under oath last month that he didn't pass that information on to his supervisors, acknowledging that the new information might have changed the punishment for the accused attacker.

In the deposition, Kachurek never gave a reason for not passing on the possible confession. And Kachurek acknowledged that he learned the information even before he sent that controversial email later the same day.

He also said in the deposition that the case was handled through the administrative process and therefore had "been adjudicated" and that the woman's accused attacker "had been held responsible." The accused attacker never faced any criminal charges.

Furthermore, Kachurek testified that he was not given enough information by school administrators to enforce those sanctions against the male student or anyone else found in violation of the school's policy against sexual harassment or assault.

"I did not have those documents," Kachurek said during the July 12 deposition, referring to a list of the sanctions or a picture of the male student.

Kachurek also remained unapologetic about that email. He only said he should have used the word "allegedly" in front of slander.

The transcript of the deposition was filed in federal court late last month and obtained by The Enquirer from the courthouse. Kachurek recently left NKU after about a year in the post - he was not at the school when the alleged attack took place, but handled much of the fallout. In the deposition, Kachurek said he left of his own accord, but was frustrated with the scrutiny by faculty and a lack of resources.

"Mr. Kachurek's testimony described NKU's behavior perfectly - appalling," said Kevin Murphy, the Fort Mitchell lawyer representing the woman named

as Jane Doe in the lawsuit. "I was personally shocked to hear what he had to say, but I was thankful he told the truth."

The woman filed the suit against the school in January, claiming that NKU administrators did not do enough to protect her and keep her alleged attacker away from her as they both attended class. The suit also claims administrators were indifferent and possibly even hostile to her pleas for help. It names the school as well as top administrators, including President Geoff Mearns and even Kachurek as co-defendants. No specific damages are specified.

NKU spokeswoman Amanda Nageleisen declined comment on the suit and the deposition, saying the university cannot comment on pending litigation and would not discuss the sanctions citing student privacy concerns.

In court documents, however, outside lawyers hired by NKU denied any wrongdoing by the school, arguing that all procedures and applicable laws were followed. The school has hired a Lexington-based law firm to defend the case.

'I wasn't strong enough'

The suit comes as universities across the country have struggled with what to do about sexual assaults on campus. New regulations released by the Department of Education in 2011 required schools to create an internal administrative process for dealing with violations of the federal law known as Title IX which covers sexual discrimination and assaults on campuses. These systems are separate from the criminal system, which is also available to would-be victims.

According to NKU data, there have been 30 reports of assaults/offenses to the school or the NKU police between 2010-2015, including 19 in 2014-15 alone. School officials have previously said that increase may be due to possible victims being comfortable reporting such incidents instead of an actual rise in sexual assaults.

By comparison, there were 47 "forcible sex" crimes reported to the University of Cincinnati police alone between 2012-2014, the last year data was available for that school. And there were 20 rapes reported at Ohio State University's main campus in 2014 alone.

One such report at NKU included the one by the woman about the 2013 incident. In the suit, the woman says a fellow student raped her in her dorm room in her first semester of her freshman year. In a separate interview with The Enquirer, she says she wasn't drunk and had not been drinking, and that she had just thought she would be talking to the male student whom she had just met recently.

In the interview, the woman known as "Jane Doe" in the suit says she did not pursue criminal charges because she was ashamed and didn't want her parents to know. But after several months of keeping it to herself, she finally told her mother and sought counseling on campus.

"It was eating me up inside," said the woman, still a student at the school. The Enquirer is withholding her name by request because she said she is afraid of retribution from school administrators and fellow students. "I had been an athlete and thought I was strong. But I couldn't accept to myself that I wasn't strong enough to stop what happened or deal with it afterward."

So in the spring of 2014, she told her mother and went to counselors on campus. That led her to school administrators who she says pressured her to keep the complaint within the internal disciplinary system. She also acknowledges that filing criminal charges would have been futile since at least several months has passed since the alleged attack.

The woman went through Norse Violence Prevention Center, which had just been formed. That led to her going through the process that oversees NKU's internal discipline system for sexual assault that includes hearings in front of an administrative panel made up of a student, a faculty member and a staff member. Such a panel ruled in June 2014 that it was more likely than not that sexual misconduct had occurred and the discipline was then handed down.

He was not suspended and was ordered to stay away from the woman. There was a suspension issued, but it was held "in abeyance" or the equivalent of being on probation.

"They never told me until after the fact that expulsion was never seen as an option," the woman said. "My mom and I were completely confused and thought there would be no way that he could do something like that and basically nothing be done about it."

Yet according to the woman and her lawyer Murphy, the male student continually violated those sanctions, showing up in her cafeteria or even her dormitory with little to no warning from administrators. She said she called the police several times yet nothing was done. She also said that she would be confronted by her would-be attacker, only to find out afterward he had been given permission to be in that area. At one point, he was even hired to check all IDs entering the school's activity center.

"When I saw him again (at the school cafeteria), it was like reliving the whole thing over again," the woman said. "And befor%lon' , his friends and people who knew him were yelling at me for as much as an hour, calling me a slut or a whore."

In the deposition, Kachurek said he didn't think allowing a would-be attacker to have contact with his alleged victim was a "best practice" and that he would not have allowed such a person to be hired at the gym. He also said such a finding would probably have meant expulsion at Alfred State University in New York where he last worked.

Kachurek also acknowledged that the school's administration was technically responsible for enforcing the administrative sanctions. But he said would-be victims called the police department after hours to help remove the person potentially violating sanctions. Kachurek also said he had asked the administration that the police department be notified of such sanctions, yet that hadn't happened as of his departure from the school last month.

Kachurek also said he had no way to identify such a possible violator because there was nothing on file at the department. The school notified Kachurek's predecessor of the sanctions in a brief email that identified the male student by name.

In a separate interview, the woman's lawyer Murphy echoed those sentiments.

"Are those folks in the ivory tower in their cars at night, checking to see if the person under sanctions is staying away from her," Murphy said. "Do they get in their cars and patrol the areas where the person under sanctions is prohibited from? The answer to that is no."

The Enquirer is also not naming her alleged attacker but did try to contact him for comment. He did not respond to several emails. In the deposition, he is described as a well-known and popular figure on campus.

Not apologetic for email

The woman’s lawyer Murphy said that NKU’s handling of the case was “disgraceful,” saying all she asked for initially was counseling and a scholarship to transfer to another Kentucky public university to get away from her alleged attacker.

Kachurek left the school late last month after about a year as chief of the 22-member department. He declined comment when reached through his current employer the Malvern, Pa.-based FBI-Law Enforcement Executive Development Association, a non-profit law enforcement training agency (it has no ties to the Federal Bureau of Investigation).

In the deposition, Kachurek described protesting to supervisors that he worked in a "hostile" environment because of the scrutiny over his decisions by NKU's faculty senate (there were several motions and inquiries into the email as well as other incidents on campus involving the NKU police). Kachurek also said he was never given full resources to do the job he was hired for, and that when he arrived his staff had never been trained on Title IX issues. He also said the school routinely declined to enact his suggestions to improve on-campus safety, including instituting a full-time sign-in process at the dormitories.

"Residential housing personnel felt that their procedures were adequate and were not willing to entertain our suggestions for improvement," Kachurek said.

Kachurek came under fire last fall after sending that email that intimated that the woman was slandering her alleged attacker. In his deposition he said that other school administrators used the word slander, and that they said the woman was accusing the man of dealing drugs.

Still, the email, which was sent to his supervisor and internally within the police department, went campus-wide. Several faculty members viewed it as being insensitive to a possible victim of sexual assault, and it led to an inquiry by the faculty senate. In fact, Kachurek is named in the suit in part for sending that email.

In the deposition, Kachurek said he should have put the word "allegedly" in front of the word slander and that he was referring to the possibility that the woman had accused her accused attacker of selling drugs. He said he was not willing to apologize for the email.

"I believe anyone who reads it certainly is entitled to their own interpretation," he said.

Kachurek also expressed frustration that his recommended changes to improve security were not implemented to his knowledge.

"Changes have been proposed, but to the best of my knowledge, have not been enacted," Kachurek said.

NKU spokesman Nageleisen declined comment on the proposed changes although NKU's lawyers argued in court documents that the dormitory security had been improved.

Toward the end of his deposition, the woman's lawyer asked Kachurek about the case overall, "Chief, don't you find this appalling?"

"Yes," Kachurek answered.

Sexual Assaults/Offenses at NKU

Here are the number of sexual assaults or offenses reported to Northern Kentucky University administration or police between 2010-2015

2010	**1**
2011	2
2012	5
2013	3
2014	10
2015	9

Source: NKU

Read or Share this story: http://cin.ci/2bqPe4c