

FSCOT Agenda
January 19, 2021, 3:00 pm
Note: Guests join at 3:30 pm

Zoom Connection: <https://ksu.zoom.us/j/7855322637>
Phone Connection: +1 669 900 6833 or +1 646 876 9923

- 1.) Turn on recording and announce disclaimer
- 2.) Call meeting to order – **Brett**
- 3.) Approve agenda (additions) – **Brett**
- 4.) Reports:
 - a. Extended IT Leadership Group – Brett & Michael
 - i. No Report
 - b. IT Policy Review Team – Don Crawford, Information Technology Manager, Architecture, Planning & Design, FSCOT Member
 - i. Attachment # 1 (page 5): Review of PPM 3450 K-State eID policy (First Reading)
 1. Action Needed:
 - a. Approve or send back more feedback
 - c. Office 365 Governance Group – Michael
 - i. No Report
 - d. Project Governance Group – **Brett**
 - e. Record and Retention Committee – **Lisa Shappee**, Library Director/Associate Professor, K-State Polytechnic, FSCOT Member
- 5.) Old Business (Business from Previous Meetings)
 - a. Discussion of Policies and the Technical, Legal, and Retention components
 - i. Introduce guests
 - ii. Attachment # 2 (page 14): Legal/Security Questions for the Guests
 - iii. Attachment # 3 (page 16): Review of PPM 3455 Electronic Mail Policy
 - iv. Attachment # 4 (page 27): Review of PPM 3460 Official Electronic Correspondence
 - v. Attachment # 5 (page 31): Revised Process for Policy Review

6.) New Business

a. Select topic for next meeting: February 2, 2021, 3:30 pm

i. See topics under Future Meetings and Agenda Items

7.) Other Items – **Group**

8.) Adjourn meeting—**Brett**

Future Meetings and Agenda Items:

- Accessibility of scanned documents for on line educational materials – presented by Jason Maseberg-Tomlinson, General University, Director, Student Access Center
- Use of YouTube for instructional materials – What is University’s policy for publishing educational materials on YouTube
- SPARK Funded Laptop/A/V equipment program – General update from IT – Scott or Gary
- Zoom Stats – General Zoom stats update – Scott

Continued discussion of FSCOT’s role in IT policy approval

Attendance:

- Aryan Tayal, Student Representative
- Be Stoney, Education (18-22)
- Bill Zhang, Engineering (20-23)
- Bob Larson, Veterinary Medicine (18-21)
- Brett DePaola, Arts and Sciences (17-22) Co-Chair
- Colby Moorberg, Agriculture (20-22)
- Don Crawford, Architecture, Planning, and Design (20-22)
- Ignacio Ciampitti, Extension (20-22)
- Jason Maseberg-Tomlinson, General University (20-23)
 - Jim Bach, General University alternate (20-23)
- Lisa Shappee, Technology & Aviation K-State Polytechnic (15-21)
- Martin Seay, Health and Human Sciences (20-21)
- Michael Raine, Business Administration (07-20) Co-Chair
- Ryan Otto, K-State Libraries (17-20)

Non-voting Attendees:

- Gary Pratt, CIO
- Debbie Webb, Liaison for University Support Staff
- Scott Finkeldei, Liaison for Chief Information Officer

Guests:

- Mr. Chad Currier, IT Chief Operations Officer/Deputy CIO for Enterprise Technology, Chief Security Officer
- Ms. Shari Crittendon, General Counsel, Office of General Counsel
- Ms. Kelley Brundage, University Registrar, Office of the Registrar

Mr. Ryan Leimkuehler, University Records Manager, University Archives

Attachment # 1:

PROPOSED REVISIONS: K-State Electronic Identifier (eID) Policy

Chapter 3450

Revised January 9, 2012

Table of Contents

- [.010 Purpose](#)
- [.020 Scope](#)
- [.030 Effective Date](#)
- [.0540 Policy](#)
- [.0650 Definitions](#)
- [.0760 Roles and Responsibilities](#)
- [.0870 Implementing Procedures](#)
- [.0980 Related Laws, Regulations, or Policies](#)
- [.1090 Questions/Waivers](#)

.010 Purpose

The K-State eID is the electronic identifier that when used in conjunction with a password enables authorized access to centrally managed University IT resources. This policy defines the requirements for the eligibility, creation, usage, maintenance, and duration of the eID.

This policy defines the requirements for the eligibility, creation, usage, maintenance, and duration of the electronic identifier (eID). The K-State eID is the electronic identifier that when used in conjunction with a password enables authorized access to centrally managed University IT resources.

.020 Scope

This policy applies to all students, faculty, staff, and individuals affiliated with the University with a legitimate need for access to University information technology resources in support of the teaching, research, and service mission of Kansas State University.

For this policy, "students, faculty, and staff" refers to existing and incoming students, faculty, and staff who have been issued a K-State eID.

A person or entity (user) may be granted a K-State University user account and access to information technology resources if such access supports the mission of the University.

.030 Effective Date

2004

Revised: November 2011

Revised: January 9, 2012

Revised: December 2020

.0540 Policy

Students, faculty, staff, and others affiliated with the University (including those in program, contract, or license relationships with the campus) are required to have a unique electronic

identifier (eID) and a valid password in order to obtain authorized access to centrally-managed IT University resources.

In some cases, a group eID may be required to facilitate shared access to centrally-managed IT University resources by a group of students, faculty, staff, and/or affiliated individuals with valid individual K-State eIDs.

An eID ~~is~~ only a means to verify a campus identity. It is not the sole means of determining permission to access specific services. Authorization to access any campus service shall be determined by the provider of each service through appropriate authorizing mechanisms.

.0650 Definitions

Authentication

Process of verifying one's digital identity. For example, when someone ~~logs~~ signs into a workstation or application with their eID, the password verifies that the person ~~logging~~ signing in is the owner of the eID. ~~The verification process is called authentication.~~

Authorization

Granting access to resources only to those authorized to use them.

K-State eID

The electronic identifier or user_name allocated to an individual affiliated with Kansas State University that when used in conjunction with a password enables authorized access to centrally-managed ~~University~~ [University](#) IT resources. eID's become part of K-State email addresses (e.g., [eID@k-state.edu](#)).

K-State Group eID

The electronic identifier allocated to a group of faculty, staff, students, and/or affiliated individuals that when used in conjunction with a password enables shared authorized access to centrally-managed ~~u~~University IT resources such as email.

Special Access eID

The electronic identifier or username allocated to an individual who is not a current student ~~or employee~~ [or employee](#), but is affiliated with the university with a legitimate need for access to ~~U~~university ~~IT~~ resources.

.0760 Roles and Responsibilities

It is the role of individual students, faculty, staff, or affiliated individuals to request the allocation of an eID. The authentication and activation of the eID is the responsibility of **the Division of** Information Technology Services-(ITS) personnel.

.0870 Implementing Procedures

1. Eligibility - All students, faculty and staff, and individuals with a legitimate need for access to university IT resources are eligible for an eID. Eligible users are included in one of the following categories:

The following groups are eligible for an eID:

Applicants: eIDs are necessary to begin using some K-State services before enrolling in classes.

Students: All undergraduate and graduate students.

Faculty: Full time, part-time and adjunct faculty are required to have an eID.

Staff: Full time and part-time staff are required to have an eID.

Post-doctoral fellows, interns, residents, visiting professors and sponsored researches: All are eligible for an eID if they have been entered into the HR database. If they are not in the database, they are considered temporary employees and visitors.

Retirees

- ~~1. **Students** - All Currently enrolled students and students admitted for the next semester will be enabled for access to University IT resources. Students are verified through the university's student information system (KSIS). Student access remains active over the summer semester.~~
- ~~2. **Faculty and Staff** - All Faculty, staff, adjunct faculty, adjunct staff, and retired employees will be enabled for access to University IT resources. Employment is verified through the Human Resources employee database (HRIS).~~

Affiliated Individuals - Individuals who are affiliated with the university with a legitimate need for access to University IT resources in order to fulfill their obligations or further the mission of the university may be eligible for a K-State eID as a special access account. A unit sponsor is required.

Special Access Accounts - The following types of affiliations may qualify individuals for a special access accounts.

- i. Previous students who have been granted additional time to complete coursework are eligible to have their K-State eID enabled for the access necessary to complete that work.
- ii. Employees of affiliated organizations are eligible for a K-State eID with access to only those services required for their work for K-State.
- iii. Individuals who serve as liaisons for building community among students may be eligible for a K-State eID enabled for email access only.
- iv. Other individuals may be eligible for a K-State eID and access to centrally-managed IT University resources if such access is necessary in order to fulfill

the requesting person's obligations to K-State and the special account will be used ONLY for purposes directly related to the association with K-State. Personal use is not permitted.

7. **Creating or Changing an eID**—University students, faculty, staff, and others must register to select an eID and password. The eID must be 3–20 characters long, with letters "a–z" and/or numerals from "0–9". The first character must be a letter of the alphabet. eID assignments are made on a first-come, first-serve basis. eID's may be changed for a fee. Fees are waived in cases of legal name changes.

For detailed information on requesting, creating, changing, or reactivating K-State eIDs (including Special Access eIDs), see the [eID FAQs page](#). This should be part of the procedures identified in the eID creation process.

~~HYPERLINK "https://www.k-state.edu/its/eid/"~~

2. **Duration**- eIDs remain assigned to eligible individuals for life. Access to IT resources will remain enabled as long as the individual meets the eligibility requirements and has a valid password. All electronic data solely controlled and owned by an eID stored on central servers will be deleted 240 days after eligibility to access this data ceases. Access to University resources is based on roles and responsibilities and will be removed once the holder of the eID no longer has a legitimate need.

Administrators **The unit head** may request deprovisioning a former employee's services accessed via an eID, if that former employee was under their supervision while employed; or, in the case of students, the Vice President for Office of Student Life or the Assistant Vice President of Student Life may request deprovisioning of a former student's services accessed via an eID. The request must come to the Chief Information Officer (CIO) or to their designee.

3. **Group Accounts** - A Group eID may be allocated in such circumstances as 1) departments, units, or organizations need shared access to email, files, or project space, 2) two or more staff need to handle an email account, and 3) a department, unit, or organization needs an official email address. For information on how to request a Group eID, see the [K-State eID and password page](#). This should be part of the eID creation procedures.

~~HYPERLINK "https://www.k-state.edu/its/eid/"~~

4. **Electronic Signature through eID** - All students, faculty, and staff with eIDs ~~may~~ may provide their binding, legally enforceable electronic signature, in their individual capacities, on contracts or other transactions with the University by signing in with their eID, and while signed in, indicating agreement to the terms. Agreement through this process has the same force and effect as a regular physical signature. The person providing an

electronic signature agrees to conduct that contract or other transaction_ by electronic means.

.0980 Related Laws, Regulations, or Policies

E. [K-State's Information Technology Usage Policy](#)

[K-State's Access Controls Security Policy](#)

[K-State's Operations and Management Security Policy](#)

[K-State's Electronic Mail Policy](#)

~~[K-State's Official Electronic Correspondence with Faculty, Staff, and Students](#)~~

[K.S.A. § 16-1605: Use of electronic records and electronic signatures](#)

.100 .090 Questions/Waivers

The [Chief Information Officer](#) (CIO) is responsible for this policy. The CIO or designee must approve any exception to this policy or related procedures. Questions should be directed to the [Chief Information Security Officer](#).

Draft without Markup: Electronic Identifier (eID) Policy

Table of Contents

.010 [Purpose](#)

.020 [Scope](#)

.030 [Effective Date](#)

.040 [Policy](#)

.050 [Definitions](#)

.060 [Roles and Responsibilities](#)

.070 [Implementing Procedures](#)

.080 [Related Laws, Regulations, or Policies](#)

.090 [Questions/Waivers](#)

.010 Purpose

This policy defines the requirements for the eligibility, creation, usage, maintenance, and duration of the electronic identifier (eID).The K-State eID is the electronic identifier that when used in conjunction with a password enables authorized access to University resources.

.020 Scope

This policy applies to all students, faculty, staff, and individuals affiliated with the University with a legitimate need for access to University resources in support of the teaching, research, and service mission of Kansas State University.

.030 Effective Date

2004

Revised: November 2011

Revised: January 9, 2012

Revised: December 2020

.040 Policy

Students, faculty, staff, and others affiliated with the University (including those in program, contract, or license relationships with the campus) are required to have a unique electronic identifier (eID) and a valid password in order to obtain authorized access to University resources.

In some cases, a group eID may be required to facilitate shared access to University resources by a group of students, faculty, staff, and/or affiliated individuals with valid individual K-State eIDs.

An eID is only a means to verify a campus identity. It is not the sole means of determining permission to access specific services. Authorization to access any campus service shall be determined by the provider of each service through appropriate authorizing mechanisms.

.050 Definitions

Authentication

Process of verifying one's digital identity. For example, when someone signs into a workstation or application with their eID, the password verifies that the person signing in is the owner of the eID.

Authorization

Granting access to resources only to those authorized to use them.

K-State eID

The electronic identifier or user name allocated to an individual affiliated with Kansas State University that when used in conjunction with a password enables authorized access to University IT resources. eID's become part of K-State email addresses (e.g., eID@k-state.edu).

K-State Group eID

The electronic identifier allocated to a group of faculty, staff, students, and/or affiliated individuals that when used in conjunction with a password enables shared authorized access to University resources such as email.

Special Access eID

The electronic identifier or username allocated to an individual who is not a current student or employee, but is affiliated with the university with a legitimate need for access to University resources.

.060 Roles and Responsibilities

It is the role of individual students, faculty, staff, or affiliated individuals to request the allocation of an eID. The authentication and activation of the eID is the responsibility of the Division of Information Technology (IT).

.070 Implementing Procedures

Eligibility

The following groups are eligible for an eID:

- Applicants: eIDs are necessary to begin using some K-State services before enrolling in classes.
- Students: All undergraduate and graduate students.
- Faculty: Full time, part-time and adjunct faculty are required to have an eID.
- Staff: Full time and part-time staff are required to have an eID.
- Post-doctoral fellows, interns, residents, visiting professors and sponsored researchers: All are eligible for an eID if they have been entered into the HR database. If they are not in the database, they are considered temporary employees and visitors.
- Retirees
- **Affiliated Individuals** - Individuals who are affiliated with the university with a legitimate need for access to University resources to fulfill their obligations or further the mission of the university may be eligible for a K-State eID as a special access account. A unit sponsor is required.

Special Access Accounts - The following types of affiliations may qualify individuals for a special access accounts.

- Previous students who have been granted additional time to complete coursework are eligible to have their K-State eID enabled for the access necessary to complete that work.
- Employees of affiliated organizations are eligible for a K-State eID with access to only those services required for their work for K-State.

- Individuals who serve as liaisons for building community among students may be eligible for a K-State eID enabled for email access only.
 - Other individuals may be eligible for a K-State eID and access to University resources if such access is necessary to fulfill the requesting person's obligations to K-State and the special account will be used ONLY for purposes directly related to the association with K-State. Personal use is not permitted.
5. **Duration** - eIDs remain assigned to eligible individuals for life. Access to University resources is based on roles and responsibilities and will be removed once the holder of the eID no longer has a legitimate need.

The unit head may request deprovisioning a former employee's services accessed via an eID, if that former employee was under their supervision while employed; or, in the case of students, the Office of Student Life may request deprovisioning of a former student's services accessed via an eID. The request must come to the Chief Information Officer (CIO) or to their designee.

6. **Group Accounts** - A Group eID may be allocated in such circumstances as 1) departments, units, or organizations need shared access to email, files, or project space, 2) two or more staff need to handle an email account, and 3) a department, unit, or organization needs an official email address.
7. **Electronic Signature through eID** - All students, faculty, and staff with eIDs may provide their binding, legally enforceable electronic signature, in their individual capacities, on contracts or other transactions with the University by signing in with their eID, and while signed in, indicating agreement to the terms. Agreement through this process has the same force and effect as a regular physical signature. The person providing an electronic signature agrees to conduct that contract or other transaction by electronic means.

.080 Related Laws, Regulations, or Policies

- [K-State's Information Technology Usage Policy](#)
- [K-State's Access Controls Security Policy](#)
- [K-State's Operations and Management Security Policy](#)
- [K-State's Electronic Mail Policy](#)
- [K.S.A. § 16-1605: Use of electronic records and electronic signatures](#)

.090 Questions/Waivers

The [Chief Information Officer](#) (CIO) is responsible for this policy. The CIO or designee must approve any exception to this policy or related procedures. Questions should be directed to the [Chief Information Security Officer](#).

Attachment # 2

Legal/Security Questions for the Guests

Please note that there may be additional questions/concerns based upon discussion of the policy review of Chapter 3450, Electronic Identifier (eID) Policy.

General Questions:

- How can we determine what points in a policy are mandated by law or other higher authority vs what are recommendations by OGC or IT Leadership?
- What is the difference between Policy and procedures and how are each documented, vetted, approved, communicated, and published?

PPM 3455 Electronic Mail Policy

0.20 University Official Emails

1. What about “official” university emails to non-university persons (eg. Offer letters)?
2. Need definition of “Sanctioned email”

A. Proper Usage

3. Is it FERPA violation to include grade information in an email to a student?
 - Faculty member was told to not use K-State email for communicating grade information to students – what method of communication can a faculty member use for this purpose?

B. Ownership of Email Data

4. Does this overrule other IP rules?
5. Does this include the physics email domain?

C. Forwarding

- Can we manually forward? (We think the answer is yes.)
- What about retired or former students – How those grandfathered in access their email?

D. Publication of Email Addresses

- We can't put email contact even on departmental web pages?
- If we can't post email addresses, how will our (potential) colleagues contact us?
- How can Ag-Extension users contact us?
- If someone files with the Registrar to not have their email addresses posted, how will we know that at the departmental level (for the departmental web pages)?

E. Retention

- Manually moving emails to files is extremely time-intensive
- Files are not as easily searched on many keys as our email search tools
- Can we have a convenient “tool” to do this, if we are required to move these files?

F. Expiration

- There will be lots of opposition with existing policy – and the proposed policies are even more problematic. What does legal *require*?
- Where are the “The guidelines regarding those privileges are outlined in email deprovisioning guidelines” posted?

0.40 Confidentiality and Privacy

6. Where are the details for the PPM describing the report the CIO provides to Faculty Senate regarding cases dealt with that year?

Email Deprovisioning Guidelines

- Emeritus status should be defined somewhere in the policy

- How do we accommodate faculty and staff who continue to have a role with the University but are not employees? – See F. Expiration above

Microsoft Teams Retention Policies – See excerpt from an email sent to FSCOT

“I'm writing to make a request for Chats and Posts on Teams be retained for 5 years (typical of K-State records) instead of the current schedule. https://kstate.servicenow.com/its?id=kb_article&sys_id=9d49287ddb5e905044619e26db96196c”

The current Teams retention policy is having a very negative impact on our department. We did what the university urged and got on board with Teams. Unfortunately, it didn't occur to me that the retention policy would be different from what we have with folders in Outlook. Team's really is a great platform--if our communications don't disappear. I do not want to abandon the work we've done to set up an effective Teams framework and get everyone invested in using it. We've set it up for the department, special projects, and individual faculty development (annual evaluations, grant management, furlough plans, etc.). I especially don't want to have to undo it and send yet another message to the faculty that the university doesn't value their time and effort. It's hard to understand why the university is making things more difficult in an already difficult time.”

What separates Teams messages from email messages regarding retention policy? Is our retention policy based on Regents or other governance, or do we have some flexibility? Is this a topic worthy of a discussion?

What is Official Policy Creating and Approval Process (i.e. Zoom Policy Settings Released January, K-State Today)

- How and where were the Zoom Security Settings vetted through Shared Governance and where is that policy listed?

Attachment # 3

November 25, 2020

To: Consultant groups

From: IT Policy Review team

Re: PPM 3455 Electronic Mail Policy

The IT Policy Review Team reviewed [PPM 3455 Electronic Mail policy](#) and are recommending the changes provided in the proposed revisions that begin on page 2. Proposed revisions without markups are found on page 7. Changes included setting specific timelines for deprovisioning of email that are procedures and not listed in the policy, reorganizing information under 0.20 Policy with appropriate subheadings, removing similar language to the Information Technology Usage Policy, include the word “sanctioned” since other entities have email systems (Vet Med, Physics). Under .030, the paragraphs with state statute and KBOR language were removed. Units consulted on the changes to the policy include FSCOT, Registrar, Office of Student Life, CAPP, the IDM team and the Division of Communications and Marketing.

The policy team is requesting general comments on the policy as opposed to wordsmithing. Table 1 provides a listing of policies from other universities that were reviewed.

We would appreciate your feedback using this [form](#) by December 14.

Table 1. University policies reviewed

University	URL
KU March 1998	Electronic Mail - https://bit.ly/3gWwPt8
Auburn April 2019	Employee and Student Email Policy - https://sites.auburn.edu/admin/universitypolicies/Policies/EmployeeandStudentEmailPolicy.pdf
Harvard	Email Policies - https://www.hsph.harvard.edu/information-technology/resources/policies/email-policies/
Indiana University August 2011	Use of Electronic Mail - https://bit.ly/2EU2qyL
Iowa State University	Email, University Communications - https://bit.ly/2QMGc4b
LSU	Use of Electronic Mail - https://www.lsu.edu/policies/ps/ps_6.15.pdf

August 2007	
NC State Feb 2015	Institutional Email - https://ncstatecollege.edu/documents/President/PoliciesProcedures/PolicyManual/Final%20PDFs/19-22.pdf
Oklahoma State University March 2017	Appropriate Use Policy - https://adminfinance.okstate.edu/site-files/documents/policies/appropriate-use-policy.pdf
Texas A&M 2003	Student email - https://bit.ly/2ExTgao
University of Wisconsin August 2004	Email Address Requirements - https://registrar.wisc.edu/email/
Washingto n State University Oct 2015	Electronic Communication Policy - https://policies.wsu.edu/prf/index/manuals/executive-policy-manual-contents/ep4-electronic-communication-policy/

Proposed REVISIONS: Electronic Mail Policy

Chapter 3455

Revised September 2, 2010, September 2020

Table of Contents

[.010 Introduction](#)

[.020 Policy](#)

[.030 Confidentiality and Privacy](#)

[.040 Sanctions](#)

[.050 Related Kansas Law and Board of Regents Policy](#)

[.060 Questions](#)

.010 Introduction

~~This Policy clarifies the applicability of law and certain other University policies to electronic mail. Users are reminded that all usage of K-State's information technology resources including electronic mail is subject to all University policies including [K-State's Information Technology Usage Policy](#).~~

Kansas State University provides email accounts for all students, faculty and staff. The University reserves the right to place constraints on the use of email to protect its legal position to respect copyright, telecommunications, anti-discrimination and contractual law to ensure the confidentiality of communications, and the protection of privacy and to comply with record retention requirements.

.020 Policy

~~The University encourages the use of electronic mail and respects the privacy of users. Nonetheless, electronic mail and data stored on the University's network of computers may be accessed by the University for the following purposes:~~

~~For items A-G, the extent of the access will be limited to what is reasonably necessary to acquire the information and/or resolve the issue.~~

- ~~1. troubleshooting hardware and software problems,~~
- ~~2. preventing unauthorized access and system misuse,~~
- ~~3. retrieving University business related information,*~~
- ~~4. investigating reports of alleged violation of University policy or local, state or federal law,*~~
- ~~5. complying with legal requests (e.g.; court orders) for information,*~~
- ~~6. rerouting or disposing of undeliverable mail,~~
- ~~7. addressing safety or security issues.~~

~~* The system administrator will need written approval, including email, indicating the extent of access that has been authorized from the Chief Information Officer (CIO) or the CIO's designee, to access specific mail and data for these purposes.~~

Official communication for Kansas State University students and employees should be made through the K-State email system (eID@ksu.edu or eID@k-state.edu). The use of non-K-State email for sending confidential and sensitive information is prohibited. For purposes of this policy, "email" includes all offerings encompassing email, calendaring, contacts and contact management, and mailing lists and list management.

~~To the greatest extent possible in a public setting individuals' privacy should be preserved. However, there is no expectation of privacy or confidentiality for documents and messages stored on University-owned equipment.~~

~~Users of electronic mail systems should be aware that, in addition to being subject to authorized access, electronic mail in its present form cannot be secured and is, therefore, vulnerable to unauthorized access and modification by third parties. Receivers of electronic mail documents should check with the purported sender if there is any doubt about the identity of the sender or the authenticity of the contents, as they would with print documents. Users of electronic mail services should be aware that even though the sender and recipient have discarded their copies of an electronic mail record, there may be back-up copies of such electronic mail that can be retrieved.~~

.030 Confidentiality and Privacy

Kansas State University does not guarantee privacy in anything stored, sent or received on the University's email system. Students and employees have no expectation of privacy in email messages sent through University email accounts as outlined in the Information Technology Usage policy. <https://www.k-state.edu/policies/ppm/3400/3420.htm> .

~~University electronic mail services may, subject to the foregoing, be used for incidental personal purposes provided such use does not interfere with University operation of information technologies including electronic mail services, burden the University with incremental costs, or interfere with the user's employment or other obligations to the University.~~

Incidental personal use is permitted as long as it does not have negative effects on other email accounts, jeopardize the email system, get in the way of fulfilling job responsibilities, or violate the law or the [Information Technology Usage Policy](#) or of any other policy or guideline of the University.

~~Registered student and campus organizations such as the College Republican Club or the Young Democrats may use their membership listservs to notify members of meetings, speeches, or rallies. Faculty members may use electronic systems for course-related discussions of political topics. Individuals may use email to exchange ideas and opinions, including those dealing with political issues. The latter is generally considered an incidental use of the email system. However, University information technology resources, including email, may not be used to support partisan political candidates or party fundraising. This statement is consistent with Kansas law and Board of Regents policy on political activity. (See Kansas law and Board of Regents policy printed at the end of this policy.)~~

A. Proper Usage

Email must be consistent with Kansas State University policies, meet ethical conduct and safety standards, and comply with applicable laws and proper business practice. State law prohibits the use of public resources in support of political candidates.

~~Electronic mail may constitute a public record like other documents subject to disclosure under the Kansas Open Records Act or other laws, or as a result of litigation. However, prior to such disclosure, the University evaluates all requests for information submitted by the public for compliance with the provisions of the Act or other applicable law. In addition, electronic mail may constitute University records subject to the University's Retention of Records Policy (PPM, Chapter 3090). As such, they may need to be retained for longer than an email system is capable of retaining them. It is the responsibility of the sender/recipient to determine if a particular email message constitutes a university record.~~

~~If an email message is a university record (as defined in PPM, Chapter 3090) it is subject to the same retention period as the paper equivalent. Email messages which require long-term retention should be either retained electronically on retrievable media or printed, including all header and transmission information, and filed with their electronic or paper equivalents by the sender/recipient. K-Staters should not consider back-up media on the central system as permanent archival storage (email back-up media are only available for 30 days).~~

~~Incidental personal electronic mail which is not subject to the Retention of Records Policy may be destroyed at the user's discretion.~~

F. Record Retention

Electronic mail may constitute a public record like other documents subject to disclosure under the Kansas Open Records Act or other laws, or as a result of litigation. Prior to such disclosure, the University evaluates all requests for information submitted by the public for compliance with the provisions of the Act or other applicable law.

Electronic mail may constitute University records subject to the University's Retention of Records Policy (PPM, Chapter 3090). As such, they may need to be retained for longer than an email system is capable of retaining them. It is the responsibility of the sender/recipient to determine if a particular email message constitutes a university record. If an email message is a university record (as defined in PPM, Chapter 3090) it is subject to the same retention period as the paper equivalent. Email messages which require long-term retention should be either retained electronically on retrievable media or printed, including all header and transmission information, and filed with their electronic or paper equivalents by the sender/recipient. ~~K-Staters should not consider back-up media on the central system as permanent archival storage (email back-up media are only available for 30 days).~~

Incidental personal electronic mail which is not subject to the Retention of Records Policy may be destroyed at the user's discretion.

~~Faculty, unclassified professionals, and classified employees may not suppress publication of (e.g., unlist) their University Computing ID in the online white pages, K-State Phone Book or other official publication of Kansas State University. Exceptions for special circumstances must be approved by the Chief Information Officer or official designee.~~

D. Publication of Email Addresses

Email addresses are classified as directory information under the Family Educational Rights and Privacy Act of 1974 (FERPA) and will be listed in the Kansas State University electronic directory unless the **student** desires to withhold this information by filling out a Hold Directory Information form available in the Records section of the Office of the Registrar. Email distribution in bulk or via the class roster mechanism will be for official University business only.

~~Email is considered a formal communication by the University with faculty, staff and students. Faculty, staff and students are expected to check their email on a frequent and consistent basis in order to stay current with University and/or faculty-student related communications. For more information regarding official correspondence see [K-State's Official Electronic Correspondence with Faculty, Staff and Students Policy](#).~~

.030 Confidentiality and Privacy

Kansas State University does not guarantee privacy in anything stored, sent or received on the University's email system. Students and employees have no expectation of privacy in email messages sent through University email accounts as outlined in the Information Technology Usage policy. <https://www.k-state.edu/policies/ppm/3400/3420.htm>

In January of each year the Chief Information Officer will report to the Faculty Senate regarding cases dealt with that year. For privacy purposes all names will be omitted.

.040 Sanctions

Violations of University policies governing the use of University electronic mail services may result in restriction of access to University information technology resources in addition to any disciplinary action that may be applicable under other University policies, guidelines or implementing procedures, up to and including dismissal.

~~.030~~ .050 Related Kansas Law and Board Of Regents Policy

[Kansas Statutes Annotated \(K.S.A.\) 25-4169a](#). Use of public funds, vehicles, machinery, equipment and supplies and time of certain officers and employees to influence nomination or election of candidate prohibited; exceptions; misdemeanor. **(This has been updated, recommending leaving the link to the policy and remove the paragraph)**

- ~~3. No officer or employee of the State of Kansas, any county, any unified school district having 35,000 or more pupils regularly enrolled, any city of the first class or the board of public utilities of the city of Kansas City, Kansas, shall use or authorize the use of public funds or public vehicles, machinery, equipment or supplies of any such governmental agency or the time of any officer or employee of any such governmental agency, for which the officer or employee is compensated by such governmental agency, to expressly advocate the nomination, election or defeat of a clearly identified candidate to state office or local office. The provisions of this section prohibiting the use of time of any officer or employee for such~~

~~purposes shall not apply to an incumbent officer campaigning for nomination or reelection to a succeeding term to such office or to members of the personal staff of any elected officer.~~

(a) (1) No officer or employee of the state of Kansas, or any municipality, shall use or authorize the use of public funds or public vehicles, machinery, equipment or supplies of any such governmental agency or the time of any officer or employee of any such governmental agency, for which the officer or employee is compensated by such governmental agency, to expressly advocate the nomination, election or defeat of a clearly identified candidate to state office or local office. The provisions of this section prohibiting the use of time of any officer or employee for such purposes shall not apply to an incumbent officer campaigning for nomination or reelection to a succeeding term to such office or to members of the personal staff of any elected officer. The provisions of this section shall not apply to the statutory duties of the commission on judicial performance pursuant to article 32 of chapter 20 of the Kansas Statutes Annotated, and amendments thereto.

(b) Any person violating the provisions of this section shall be guilty of a class C misdemeanor.

B. Any person violating the provisions of this section shall be guilty of a class C misdemeanor.

~~Kansas Board of Regents Policy and Procedures Manual (15F, section d): In the interest of the fullest participation in public affairs, personnel are free to express opinions speaking or writing as an individual in signed advertisements, pamphlets and related material in support of or opposition to parties and causes. There will be the commensurate responsibility of making plain that each person so doing is acting for himself and not in behalf of an institution supported by tax funds drawn from citizens of varying political and economic views.~~

Kansas Board of Regents Policy and Procedures Manual (Chapter 2, 13, section d)

[https://www.kansasregents.org/about/policies-by-laws-](https://www.kansasregents.org/about/policies-by-laws-missions/board_policy_manual_2/chapter_ii_governance_state_universities_2/chapter_ii_full_text)

[missions/board_policy_manual_2/chapter_ii_governance_state_universities_2/chapter_ii_full_text](https://www.kansasregents.org/about/policies-by-laws-missions/board_policy_manual_2/chapter_ii_governance_state_universities_2/chapter_ii_full_text)): In

the interest of the fullest participation in public affairs, personnel are free to express opinions speaking or writing as an individual in their personal capacity and not as a representative of the institution in signed advertisements, pamphlets and related material in support of or opposition to parties and causes. There shall be the commensurate responsibility of making plain that each person so doing is acting for himself or herself and not on behalf of an institution supported by tax funds drawn from citizens of varying political and economic views. This responsibility includes avoiding the use of university letterhead and stationery and other official university designations. Employees testifying before the Legislature on behalf of outside entities shall notify their institution's designated representative prior to such testimony.

This has been updated, recommending leaving the link to the policy and remove the paragraph)

.040 .060 Questions

Questions regarding this policy should be sent to the [Chief Information Officer](#) (CIO).

Proposed Revisions without Markup: Electronic Mail Policy

Chapter 3455

Table of Contents

.010 [Introduction](#)

.020 [Policy](#)

.030 Effective Date

.030 Confidentiality and Privacy

.040 Sanctions

.050 [Related Kansas Law and Board of Regents Policy](#)

.060 [Questions](#)

.010 Introduction

Kansas State University provides email accounts for all students, faculty, and staff. The University reserves the right to place constraints on the use of email to protect its legal position to respect copyright, telecommunications, anti-discrimination, and contractual law to ensure the confidentiality of communications, and the protection of privacy, and to comply with record retention requirements.

.020 Policy

Official communication for Kansas State University students and employees should be made through the K-State **sanctioned email** addresses. The use of non-K-State email for sending confidential and sensitive information is prohibited. For purposes of this policy, "email" includes all offerings encompassing email, calendaring, contacts, and contact management, and mailing lists and list management.

A. Proper Usage

Email must be consistent with Kansas State University policies, meet ethical conduct and safety standards, and comply with applicable laws and proper business practice. State law prohibits the use of public resources in support of political candidates.

Incidental personal use is permitted as long as it does not have negative effects other email accounts, jeopardize the email system, get in the way of fulfilling job responsibilities, or violate the law or the [Information Technology Usage Policy](#) or of any other policy or guideline of the University.

B. Ownership of Email Data

The University owns all K-State email accounts. Subject to underlying copyright and intellectual property rights under applicable laws and University policies. The University also owns data transmitted or stored using University email accounts and is not be used or redistributed for non-business purposes.

C. Forwarding

Students and employees are prohibited from automatically forwarding Kansas State University email to a third-party system.

D. Publication of Email Addresses

Email addresses are classified as directory information under the Family Educational Rights and Privacy Act of 1974 (FERPA) and will be listed in the Kansas State University electronic directory unless the student desires to withhold this information by filling out a Hold Directory Information form available in the Records section of the Office of the Registrar. Email distribution in bulk or via the class roster mechanism will be for official University business only. (DRIVEN by other decisions eID/password)

E. Records Retention

Electronic mail may constitute a public record like other documents subject to disclosure under the Kansas Open Records Act or other laws, or as a result of litigation. Prior to such disclosure, the University evaluates all requests for information submitted by the public for compliance with the provisions of the Act or other applicable law.

Electronic mail may constitute University records subject to the University's Retention of Records Policy (PPM, Chapter 3090). As such, they may need to be retained for longer than an email system retains them. It is the responsibility of the sender/recipient to determine if a particular email message constitutes a university record. If an email message is a university record (as defined in PPM, Chapter 3090) it is subject to the same retention period as the paper equivalent. Email messages which require long-term retention should be either retained electronically on retrievable media or printed, including all header and transmission information, and filed with their electronic or paper equivalents by the sender/recipient.

Incidental personal electronic mail which is not subject to the Retention of Records Policy may be destroyed at the user's discretion.

F. Expiration of Email Accounts

Individuals may leave the University for a variety of reasons, which gives rise to differing situations regarding the length of time email privileges or expiration of accounts. The guidelines regarding those privileges are outlined in email deprovisioning guidelines. Notwithstanding the deprovisioning guidelines, the University (K-State, President, Provost, Deans, or General Counsel) reserves the right to revoke email privileges at any time. Any email account that has not been accessed within 12 months will be deleted or suspended.

.030 Effective Date

Revised: Sept 2, 2010

Revised: December 2020

.040 Confidentiality and Privacy

Kansas State University does not guarantee privacy in anything stored, sent or received on the University's email system. Students and employees have no expectation of privacy in email messages sent through University email accounts as outlined in the [Information Technology Usage Policy](#).

In January of each year the Chief Information Officer will report to the Faculty Senate regarding cases dealt with that year. For privacy purposes all names will be omitted.

.050 Sanctions

Violations of University policies governing the use of University electronic mail services may result in restriction of access to University information technology resources in addition to any disciplinary

action that may be applicable under other University policies, guidelines or implementing procedures, up to and including dismissal.

.060 Related Kansas Law and Board of Regents Policy

- [Kansas Statutes Annotated \(K.S.A.\) 25-4169a](#) Use of public funds, vehicles, machinery, equipment and supplies and time of certain officers and employees to influence nomination or election of candidate prohibited; exceptions; misdemeanor.
- [Kansas Board of Regents Policy and Procedures Manual](#) (Chapter 2, 13, section d)

.070 Questions

Questions regarding this policy should be sent to the [Chief Information Officer](#) (CIO).

Email Deprovisioning Guidelines (to be posted on a separate web page or in the knowledge base).

Individuals may leave the University for a variety of reasons, which gives rise to differing situations regarding the length of time email privileges or expiration of accounts. The guidelines regarding those privileges are outlined in email deprovisioning guidelines below. Notwithstanding the deprovisioning guidelines, the University (K-State, President, Provost, Deans, or General Counsel) reserves the right to revoke email privileges at any time.

Any email account that has not been accessed within 12 months will be deleted or suspended.

STUDENT ROLE

- Students no longer enrolled at K-State will lose access 365 days after enrollment ceases.
- Persons who are admitted but do not enroll will lose access 30 days after they are no longer identified in the system as affiliated (this usually takes 365 days).
- Students whose potential access to K-State email may not be in the best interests of the University (based on access to confidential information or other liability protection) may immediately lose access to email at the request of the Director of Student Life. The request is made to the CIO.
- Additionally, students' access to email may be immediately terminated without notice for those accounts/access that is through a second or shared eID or other policy violations.

EMPLOYEE ROLE

- The default rule is that separated employees will have access to email for 30 days after their termination date. NOTE: Employees with emeritus status are exempt from this default rule and may maintain their email access so long as the exception below does not apply. Retired and emeritus faculty and staff who currently have email will be grandfathered in.
- Employees who are terminated for cause or who separated and whose potential access to confidential information may not be in the best interests of the University may immediately lose access to email at the request of their supervisor. The request is made to the CIO.
- When a person is both an employee and a student at the time of separation from employment, the student role will take precedence. To further clarify, if the person is no longer

enrolled as a student at the time of their employment separation, the employee role will take precedence.

- Faculty who are retiring and who have students with incompletes will be able to request one extension of up to 90 days, subject to the approval of the applicable department head.

ADJUNCT ROLE

- Adjunct faculty, coded as temporary faculty/staff, will have access to email for 180 days following the end of their employment at K-State. If these employees do not return to service within those 180 days, they will lose access to email (Question: Immediately or with a grace period).

Attachment # 4:

November 25, 2020

To: Consultant groups

From: IT Policy Review team

Re: PPM 3460 Official electronic correspondence with faculty, staff and students

The IT Policy Review Team reviewed [PPM 3460](#) *Official electronic correspondence with faculty, staff and students* (see page 2) and are recommending that the policy be retired and the premise of the policy be incorporated into [PPM 3455](#) *Electronic Mail Policy*, where appropriate [PPM 3450](#) K-State eID policy. Units consulted on the policy include FSCOT, Registrar, CAPP, VP Student Success, Division of Communications and Marketing, K-State Alerts committee, HCS and Business Intelligence. The policy team is requesting general comments on the policy as opposed to wordsmithing. Table 2 provides a listing of similar policies from other universities that were reviewed to arrive at the above recommendation. Many universities incorporate the “official” communication channel into a broader policy. NC State documents on a website that “All official email from NC State is sent only to your university email address”.

We would appreciate your feedback in this [form](#) by December 14.

Table 1. University policies reviewed

University	URL
Auburn Revised - April 19, 2019	Employee and Student Email policy https://sites.auburn.edu/admin/universitypolicies/Policies/EmployeeandStudentEmailPolicy.pdf
Clemson Approved – May 2013	Email communications policy http://www.clemson.edu/studentaffairs/student-handbook/general-policies/email-communications.html
Colorado State University Revised – March 2018	Electronic communications to students http://policylibrary.colostate.edu/policy.aspx?id=489
KU Revised – Feb 2017	Electronic mail policy https://policy.ku.edu/provost/electronic-mail-policy
Indiana University No date (2020 on website)	Email is an official method of communication https://studentcentral.indiana.edu/policies/email.html#:~:text=Email%20is%20an%20official%20method,available%20for%20all%20registered%20students.

Iowa State University Revised – Nov 2012	Email, University communications https://www.policy.iastate.edu/policy/email
LSU Aug 2007	Use of electronic mail https://www.lsu.edu/policies/ps/ps_6.15.pdf
NC State No date (2020 on website)	Official university email https://oit.ncsu.edu/my-it/email-calendaring/official-university-email/
Oklahoma State University May 2017	Appropriate use policy https://adminfinance.okstate.edu/site-files/documents/policies/appropriate-use-policy.pdf
Texas A & M University New: 2003	Student e-mail https://student-rules.tamu.edu/rule61/#:~:text=1%20E%2Dmail%20Use%20E,Computing%20(Revised%2C%201996).
University of Wisconsin August 2004	Email address requirements https://registrar.wisc.edu/email/
University of Texas No date	Use of e-mail for official correspondence to students https://catalog.utexas.edu/general-information/appendices/appendix-m/

Original: Official Electronic Correspondence with Faculty, Staff and Students

Chapter 3460

Revised September 2, 2010

Table of Contents

.010 [Introduction](#)

.020 [Policy](#)

.030 [Forwarding of Email](#)

.040 [Communicating Confidential Information](#)

.050 [Questions](#)

.010 Introduction

There is an increasing need for efficient communication with and among faculty, staff, and students in order to conduct official business at Kansas State University. All faculty, staff, and students are issued a K-State eID and an email account for use throughout the time they are a student or an employee. The definition of an official University email address is eID@ksu.edu or eID@k-state.edu. Although email is not the only form of formal communication, email is an appropriate mechanism for formal communication by the University with faculty, staff and students. If faculty, staff, or students choose to forward their mail to another email address (AOL, Hotmail, departmental server, etc.), their primary campus email address remains the official destination for official university correspondence.

.020 Policy

Email shall be considered an appropriate mechanism for official communication by Kansas State University with faculty, staff, and students. Email shall also be considered an appropriate mechanism for official communication by faculty with students. The University has the right to send official communications via email to faculty, staff, and students with the full expectation that those communications will be received and read in a timely fashion. The same expectation may be held for faculty communicating via email with students.

Official communications will be sent to the recipients' official University email addresses. Faculty, staff, and students are expected to check their email on a frequent and consistent basis in order to stay current with University and/or faculty-student related communications.

Faculty, staff and students receiving official email communication must insure that there is sufficient space in their accounts to allow for email to be delivered. It should be recognized that certain communications may be time-critical. Faculty, staff, and students will not be held responsible for an interruption in their ability to access an email

message due to a system-related problem that may prevent the timely delivery or access to the message (power outages, system viruses, etc.).

.030 Forwarding of Email

Faculty, staff, and students who choose to have their email forwarded to a private, unofficial email address (e.g., aol.com, yahoo.com, hotmail.com, cox.net) outside the official university network address (ksu.edu) do so at their own risk. The University is not responsible for any difficulties that may occur in the proper or timely transmission or access of email forwarded to any unofficial email address.

.040 Communicating Confidential Information

Users of electronic mail systems should be aware that, in addition to being subject to authorized access, electronic mail in its present form is not secure and is, therefore, vulnerable to unauthorized access and modification by third parties. Confidential information, such as student grades, should not be sent to a student with a private, unofficial, non-K-State email account (i.e., aol.com, yahoo.com, hotmail.com, cox.net, etc.). Faculty may require students to provide their official K-State email address (eID@ksu.edu) to receive a reply. A recommended step is to provide generic replies only, directing students to University tools that require authentication, such as K-State Online and Blackboard.

.050 Questions

Questions regarding this policy should be sent to the [Chief Information Officer](#) (CIO).

Attachment # 5:

Revised Process for Policy Review

Updated June 18, 2020

1. Develop or review existing policies
IT Communications Team works with a subject matter expert(s) to draft or edit (policy showing markup). This is shared with the Policy Review Team (a subset of IT Extended Leadership) who review, edit, and prepare for routing to appropriate stakeholders. The intake process might be a new/proposed policy, changes to a service, or a recommendation to review IT policies brought forward by the campus community.
2. Policy Review Team routes proposed or edited policy through appropriate review channels such as System Administrators, governance groups, administrative units, President's Cabinet (this will vary with the policy). The Office of General Counsel is notified that the policy is under review. This ensures a timely review period and that stakeholders have been consulted. The team summarizes the information and makes edits to the policy in response to comments. The consulting period should be no longer than two months. NOTE: Consultation groups and subject matter experts will vary with the policy under review.
3. Policy Review Team brings revised policy along with comments to the Office of General Counsel.
4. The final draft is shared and reviewed by IT Extended Leadership.
5. The CIO notifies the campus community that the policy has been finalized.
6. The policy is also included in the [K-State Policy and Procedures Manual](#) with appropriate links to the IT Policies section of the ITS website.
7. Policies are reviewed annually.

NOTE: The process above was reviewed by the Office of General Council in June 18, 2020.

RACI Model for rethinking purposes only, will not be part of the policy review process.

Task	Communications Team/Subject Matter Expert	Policy Review Team	Extended Leadership	System Administrators	Governance groups*+	Administrative Units	President's Cabinet	Office of General Counsel	CIO
Develop policy or review policies	<i>R</i>	-	-	-	-	-	-	-	<i>A</i>
Route policy to appropriate review channels and send to Office of General Counsel	<i>I</i>	<i>R</i>	<i>C</i>	<i>C</i>	<i>C</i>	<i>C</i>	<i>C</i>	<i>C</i>	<i>A</i>
Final draft is shared and reviewed	<i>R</i>	<i>R</i>	<i>C</i>	<i>I</i>	<i>I</i>	<i>I</i>	<i>I</i>	<i>I</i>	<i>A</i>
Notification of campus community of policy	<i>I</i>	<i>I</i>	<i>I</i>	<i>I</i>	<i>I</i>	<i>I</i>	<i>I</i>	<i>I</i>	<i>A/R</i>

A - Accountable – delegates work and is the last one to review the task or deliverable before it is deemed complete. There is only 1.

C - Consulted - review and consultation from more stakeholders and use of data/information to improve policy.

I - Informed - kept in the loop on the progress

R - Responsible - does the work

*Governance groups – FSCOT, USS, Faculty Senate, PGG, DGG, SGA, etc.

+Governance groups and subject matter experts vary with each policy.