FSCOT Agenda
Tuesday, November 17, 2020, 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. See policies in Teams files

      ii. Update on last meetings discussion?

   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, and **Ryan Leimkuehler**, CA, DAS, University Records Manager, Assistant Professor Morse Department of Special Collections, Kansas State University Libraries

      i. General introduction to Record and Retention Committee

      ii. See Attachment # 1: Bring Your Own Device (BYOD) Policy Draft

         1. No Action – Just information and discussion

      iii. See Attachment # 2: University Email Policy 3455

         1. No Action – Just information and discussion

      iv. See Attachment # 3: University Data Storage Guidelines

         1. No Action – Just information and discussion

5.) Old Business (Business from Previous Meetings)

a. First December meeting, Exec was moved from Fall break to December 1 – **Brett**

    i. Action from FSCOT – determine if we want to have a December meeting and if so, date and time

b. Zoom Cloud Retention Recommendation – **Scott Finkeldei**, Director of Academic and Student Technology, Information Technology Services and FSCOT Liaison for Chief Information Officer

    i. Status Report

c. Teams Retention Policy – **Don Crawford**, Information Technology Manager, Architecture, Planning & Design, FSCOT Member:

    i. Attachment # 4: Email from Don

    ii. Action from FSCOT – Do we want to discuss this at a future meeting?

d. Academic Technology Tools committee, feedback from special meeting of October 20 – **Brett**

    i. Status Report – Presented to Faculty Senate Leadership and Mindy Markham, Faculty Senate President will present to Provost for next steps

6.) New Business

a. General review and reminder of K-State Policies on Records Retention Policies – **Ryan Leimkuehler**, CA, DAS, University Records Manager, Assistant Professor Morse Department of Special Collections, Kansas State University Libraries

7.) Other Items – **Group**

8.) Adjourn meeting—**Brett**

Future Meetings and Agenda:

TBD

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:

- Ryan Leimkuehler, CA, DAS, University Records Manager, Assistant Professor Morse Department of Special Collections, Kansas State University Libraries
-
-
-

Attachments # 1:

All items below are in reference to university devices, university records, and university systems:

Bring Your Own Device (BYOD) Policy Draft:

Policy Statement:

The purpose of this policy is to define the controls when using mobile devices. It mitigates the following risks:

- Loss or theft of mobile devices, including the data on them
- Compromise of protected (?) information such as: CUI, FERPA, or KORA through observation by the public
- Introduction of viruses and malware to the network
- Damage to reputation

It is important that the controls set out in this policy are observed at all times in the use and transport of mobile devices.

Scope and Applicability

This policy applies to the University Community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the University's information assets, and protects the interest of the University, its customers, personnel, and business partners.

Policy

Mobile computing is an increasing part of everyday life, as devices become smaller and more powerful, the number and complexity of tasks that can be achieved away from the office grows. As the capabilities increase so, too, do the risks. Security controls that have evolved to protect the static desktop environment are easily bypassed when using a mobile device outside of the confines of a building.

Mobile devices include items such as:

- Laptops
- Notebooks
- Tablet devices
- Smart phones
- Smart watches

Unless specifically authorized, only mobile devices provided by Kansas State University may be used to hold or process University records. Use of personal devices may open the device/account to litigation in the case of a Kansas Open Records Request (See PPM 3060)

Risks, Liabilities, Disclaimers

Employees who elect to participate in BYOD accept the following risks, liabilities, and disclaimers:

- At no time does the University accept liability for the maintenance, backup, or loss of data on a personal device. It is the responsibility of the equipment owner to backup all software and data to other appropriate backup storage systems before requesting assistance from IT. (see PPM 3090 and PPM 3433)

- Persons violating this policy may also be held personally liable for resulting damages and civil or criminal charges. Kansas State University will comply with any applicable laws regarding data loss or breach notification and may also refer suspected violations of applicable laws to appropriate law enforcement agencies.
- The University shall not be liable for the loss, theft, or damage of personal devices. This includes, but is not limited to, when the device is being used for University business, on University time, or during business travel.
- Kansas State University Information Technology reserves the right to implement technology such as mobile device management to enable the removal of Kansas State University owned data.
- Personal devices are not a University maintained space for storage and does open up personal accounts to review to determine whether those accounts contain documents subject to the Kansas Open Records Act.

(How is this conducted now? How should this change to better fit KSU practice?) If an employee is required to make use of mobile equipment, the employee is provided with an appropriate device which is configured to comply with the University's policies. Support provided by the IT Department may at times require access to the employee's device for problem resolution and maintenance purposes. Kansas State University has implemented security measures to protect its critical information during mobile device usages.

Definitions

The following are the definitions relevant to the policy:

- Computing resources: All University information processing resources including all University owned, licensed, or managed computing services, hardware, software, and use of the University network via physical or wireless connection regardless of the ownership of the computer or device connected to the network.
- Institutional Data: All data owned or licensed by the University.
- University Community: Includes faculty, administrators, staff, student workers, graduate/technical assistants, alumni, interns, guests or agents of the administration, external individuals and organizations accessing University network services, and other authorized users.

Compliance

The University reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy. Instances of non-compliance must be presented and reviewed and approved by the Director of Information Security, or equivalent officer.

All breaches of information security, actual or suspected, must be reported to and investigated by the Director of Information Security, or equivalent officer.

Those who violate security policies, standards, or security procedures are subject to disciplinary action up to and including loss of computer access and appropriate disciplinary actions as determined by the University.

Related Policies, Standards, and Regulations:

- PPM 3030
- PPM 3090
- PPM 3060
- PPM 3433
- Others?

Attachments # 2:

University Email Policy 3455

Kansas State University Email Policy

Every KSU employee is individually responsible for handling and maintaining records (including University email and other electronic records) in accordance with University policy and requirements. Emails are records which may contain evidence of official University actions, decisions, approvals, or transactions. Email is subject to statutes of the State of Kansas, KSA 45-401 through 45-414, which applies to the preservation and destruction of records.

Email Records FAQ

1: How Long Do I Keep Email Messages I Have Received and Sent?

Email You Can Delete

Most received and sent emails have a very transitory value. They have no administrative, legal, fiscal, or archival retention requirements and can therefore be deleted as soon as they have fulfilled their reference purpose. Examples of such email messages include:

- Preliminary drafts
- Routine replies/requests for information
- Emails sent as reference or for informational distribution
- Emails used to set-up or accept meetings
- Announcements
- Acknowledgements

Email You Must Keep

All other email messages, both sent and received, must be retained for a designated amount of time (retention period). Retention periods are listed on a Records Retention Schedule. The retention period is based on the content of each individual email.

Emails that contain the following types of information have specific retention periods:

- Policy and procedure directives
- Substantive decisions regarding matters of University business
- Legal, discipline, or audit issues
- Approvals for purchases, HR decisions, and other actions to be taken
- Financial records including invoices and receipts
- Final reports or recommendations
- Student advising files
- Documentation of departmental/office actions, decisions, operations and responsibilities

2: How Do I Delete My Email Messages?

Deleting an email is the first step toward eliminating information that does not require further retention.

Delete emails in your Inbox, Sent Mail, and other folders that are not required to be retained or have passed their retention periods.

If you save a message that is the last in a thread of emails, you may be inadvertently saving content that you do not want or need as part of the previous messages in the string. Try to save only the information that is pertinent to a subject and not parts of a string that are unrelated.

Each email system has its unique way of storing email. You need to know how your system works to ensure all email messages that should be deleted actually are deleted. If you are using a client other than Outlook or Gmail, your instructions may be different.

Outlook	Gmail (This will change) until official
In Microsoft Outlook, the Deleted Items folder stores the messages you have deleted. To completely delete these messages, you must empty the Deleted Items folder. Right click on the Deleted Items folder and click Empty Folder to permanently delete emails. (Outlook 2016) Be sure to regularly check your Junk Email and Clutter folders for emails that can be deleted.	In Gmail, the Trash folder stores the messages you have deleted. To completely delete these messages, you must empty the Trash folder. On the left side of the page, click More and then Trash. To delete a single message, open the message and click Delete forever. To delete all messages in your trash, click Empty Trash now. Be sure to regularly check your Junk folders for emails that can be deleted.

3: When Creating a Message, What Can I Do to Help Ensure It Will Be Properly Managed?

Do You Need It?

Before creating an email message, consider whether it needs to be created:

- Can other modes of communication be used more efficiently or effectively?
- Is it necessary to create and send “information only” emails?
- Could this information be shared on a collaborative workspace such as SharePoint or Slack?
- Is it necessary to CC all of the listed recipients?
- Do you need to reply? Avoid replying to messages you receive unless a reply is actually required.

Be Objective

Be objective in the content of your email. Remember that email is subject to public information requests and may be accessed during litigation or audits. Create each email as if it were being published on the front page of the local newspaper.

One Subject Per Message

Try to limit the content in each email message to one subject. If there are several unrelated subjects to discuss, send individual emails for each subject. The messages will be easier to track, find, use, and eventually delete.

Subject Line

It is important to be objective and accurate in choosing the subject heading. Subject lines should be clear, concise, and closely articulate the purpose or action requested in your email.

Stick to the Subject When Forwarding

When forwarding email, review the original subject line and ensure it applies to your response. Too often, people continue to use a string of email messages with the same subject line, even though the topic of the messages has changed. This makes it difficult to properly categorize email messages for deletion.

When replying or forwarding messages, you can choose to not include the original message. At the top of your email inbox click File > Options > Mail > Replies and Forwards to see options. (Outlook 2016)

4: What Do I Do with All My Email?

Once you open an email message, decide what you are going to do with it before you close it.

Delete It

Can the information be found elsewhere, such as on an internal/external website, collaborative web tool, or network drive? Is it a newsletter, acknowledgement, notification, or alert? Does the email request or provide routine information? All of these types of emails can be deleted as soon as you no longer need it for reference. For most KSU employees, 70-80% of emails meet these criteria and do not need to be kept beyond reference purpose.

Do It

If you can respond or take specific action in two minutes or less – do it. File it in a folder, respond, make a call, etc.

Delegate It

Email messages requesting information or an action are not always directed to the appropriate person. After reading a message, determine whether you need to respond to it or whether you should delegate it to someone who is better placed to respond to it.

Defer It

If a response or specific action will take more than two minutes of dedicated time – defer it. If you use Outlook, you have the ability to flag emails for follow-up, label them, and add them to your Tasks list. These tools can help you find them later so that you can determine whether action is still required.

File It

Create folders that are logically aligned with the way in which business is conducted for your office such as projects, transactions, standing meetings, budgets, and employees.

5: How Do I Manage the Email I Have to Keep?

Manage Emails by Folders

Email folder titles should be clear, concise, and relate directly to the emails that will reside in the folder. Once the project or function is completed, you may add the retention period to the folder title for easy future cleanup.

Create a folder for each project or standing meeting:

- Make a folder for each project and/or standing meeting and put all email related to this project into this single folder. Use your email client's search function to check both your inbox

and sent mail folder for these emails. When the project is complete, note the date of the termination of the records retention period and retain the entire folder until that time.

Create a folder for specific functions or transactions:

- Create a folder for specific functions, transactions, or processes. For example, if you approve purchases for your office, you can create an Approvals folder for each fiscal year.

Use subfolders:

- Creating subfolders is a very useful way to easily find information. For example, a Budget Files folder can have subfolders named for each budget with which you work.

Create a folder for archival emails:

- Archive folders can be created for groups of emails related to the same topic or function that have been designated archival on the General Records Retention Schedule. Archival emails should be transferred to the University Archivist at the end of their retention period.

Separate Transitory Email

In order to keep your inbox clean, delete transitory messages as soon as you no longer need them for reference. Any transitory emails you may need to keep for a limited amount of time can be moved to a folder that is purged regularly.

Use Search and Sort Functions

Search and sort functions are useful for locating and grouping specific messages that have characteristics in common. You can search for emails to or from an individual, by date, subject, and keywords in the body.

To search in Outlook, click on the folder you would like to search, enter the search term in the search box and press Enter. Outlook's search options also allow you to search all folders and include the Deleted Items folder in your search. You can access more options by clicking the Search tab at the top of your screen.

Don't Use Email - Collaborate Via the Web

Consider utilizing an online collaboration tool such as Microsoft Teams, Groups, or OneDrive for projects/meetings rather than using email. These tools compile all the information, written and received, by its users in one location. All notes, drafts, conversation, and meeting minutes may be stored on the tool. Remember that information stored on web collaboration tools are subject to public records requests, audits, and litigation and must be retained and later deleted as per an approved retention schedule.

6: What are My Responsibilities as a Manager?

If You Are a Manager:

- Schedule a quarterly or yearly records cleanup time for your office.
- Include records management responsibilities in your office's new employee checklist.
- Establish an office procedure for setting up email accounts that allows access to email by other(s) in the office in case of absence.
- Establish general email protocols which ensure that everyone in the office is managing their email in the same way.

When an Employee Separates from Employment:

In accordance with KSU policy, managers and/or administrators are responsible for managing records associated with separated employees - this includes email. (I could not confirm if this was true or not)

- The employee and their manager or administrator should develop a plan for determining which emails must be kept and which may be deleted.
- Email that must be kept should be transferred to another employee or stored in a centralized location, such a network drive or SharePoint site.

To allow time for the department to appropriately transfer ownership or dispose of the records, systems administrators must ensure that email and other electronic records associated with a separated employee are not automatically deleted until at least one year after separation.

Attachments # 3:

University Data Storage Guidelines

General Records Management Statement:

Kansas State University, as an agency of the State of Kansas, is governed by state statutes defining records retention requirements. State law provides that all government records are public property and shall not be destroyed or otherwise disposed of except as authorized by law or applicable retention and disposition schedules (see Kansas Statutes Annotated (K.S.A.) 45-403). The University Archives is designated as the official repository for the preservation of all Kansas State University non-current government records with enduring value. The University Archives also has responsibility for advising on the management of current records, primarily through the efforts of the University Records Manager. The University Records Manager serves as the liaison between the University Archives and Kansas State University offices to develop and maintain records retention and disposition schedules. The University Records Manager also provides training on records management topics and acts as an advisor on policies.

Retention of Records Policy: PPM 3090

Management Proposals:

1. Future Teams training will include a section/handout for attendees that includes the records management site, retention schedule, and information for records manager and training opportunities.
2. Is there a way to establish rules for student created Teams vs. employee/university endorsed Teams? Student groups could have a much shorter retention period since they will likely be more for personal, study, or coursework. Employee/University endorsed Teams will likely have records in them and may have longer retention periods based on the types of records the group creates and stores in Teams.
3. Is it possible to lock Teams creation behind a training requirement or ticketing system where the creators fill out what the team will be used for and how the team will be classified?
    a. Central IT would have to implement: likely limited to IT staff or department admin creation external and internal solutions

Key Concepts to Keep in Mind:

Office 365 tools are acceptable repositories for retaining university records if they are deployed properly and actively managed, taking into consideration the following points:

- University records and information must be managed no matter where they are kept. Do not allow any system or repository to become a dumping ground for files.
- The University's records retention schedules must be applied to all university records regardless of where they are maintained no matter the format. Premature or otherwise inappropriate destruction of university records is unacceptable and violates State statute.
- When using Office 365 tools, access must be actively managed and reviewed on an ongoing basis. Updating access when changes to unit staffing occur is critical.
- DO NOT USE: Dropbox, Google Drive, etc. is not a University maintained space for storage and does open up personal accounts to review to determine whether those accounts contain documents subject to the Kansas Open Records Act.

Office 365 and University Data Storage Guidelines:

Chat/Instant Messaging: A private, synchronous exchange of messages between parties over a computer network. All messages should be short-term conversational communication. All policy or business function communication should be conducted through a more permanent medium such as email. (link to routine and policy correspondence) (~~include link to data security def.~~) See also Data Classification and Security Policy 3433

[include chat guidelines]

- Basic information on how chat is used, what kind of things should be kept, what is subject to request. Chats are between individuals and not conversation in channels. Definitions needed. Transactional records vs. Long term records, reference retention decision for chat logs.

Managed Network Drive Formerly Catfiles/W:Drive: This drive is for information that needs to be shared across the unit/organization. [This space will be phased out or foot print drastically reduced]

Y: Drive: These are created for each user and accessible only to the user. Types of files that could exist in this environment would be working documents/drafts, meeting notes, personnel records, etc. [This space is no longer created for new employees] In the process of going away use OneDrive space for this.

Microsoft Teams: Teams are cloud-based virtual workspaces that can be created by faculty and staff to facilitate collaborative work. Team sites can be made using a variety of Office 365 applications including Outlook, Teams, Yammer, and Planner. Team sites are intended to be accessed by a group of people who are working on a common project or task where rapid, remote, or simultaneous access is anticipated or desired.

When the project or task has been completed, the team site owners should determine which files, if any, are to be retained and transferred to longer term record storage or the University Archives. Once the files have been transferred, the owner should delete them from the Team site to prevent duplication and potential over-retention. ITS will keep a Team one year past the date it becomes dormant/inactive. Before a Team is deleted permanently, all archival/permanent/long term records will be migrated out of the Team structure to longer term storage or transfer to archives. [See KSU retention schedule website for guidance]

OneDrive: OneDrive is a cloud-based storage provided to individual faculty and staff to store university information and materials related to your work at Kansas State University. It is similar to your local hard drive, and it is intended for retaining work files while they are still being drafted. This space is not intended for personal, non-university-related files. It is best used as a short-term location to store files relevant to your job that you are actively working on. It is recommended that OneDrive not be used for long-term storage of university records because accessing these departmental files/university records can be difficult once an employee leaves Kansas State University.

[Do we need to address Groups here?]

SharePoint Online Communication Sites: Communication sites when deployed and properly configured, are cloud-based repositories intended for storage and sharing of university records and information. Communication sites are intended to be accessed by a group of people who need the unit's documents and where rapid, remote, or simultaneous access is beneficial. Communication sites can act as a unit's long-term records repository for digital files because they are not subject to the same expiration rules as Team sites or OneDrive for Business document libraries, and they avoid creating silos of university information and records. Note that the university records with a final deposition of Archives need to be transferred to the Kansas State University Archives once their period of retention has been met; it is not appropriate to retain these files in your unit's records repository indefinitely.

Department Intranets: A computer network that is restricted to users within a specific organization, especially network services intended for disseminating information within the organization through the use of web

technology. An intranet is distinguished from the internet, in that it is not generally accessible to the public. These areas can be used to store longer term records as they are more secure, but it should be noted this is not a preservation environment. Permanent or Archival records should be managed in a system that will check the authenticity, integrity, and accessibility of the record over time.

Department-Specific Record Systems: This could apply to a variety of vendor or homegrown systems used at the university. These record systems may be designed specifically for certain types of records such as financial, flight data, or research data. Plans should be in place to monitor and manage records in these environments and that the records are destroyed or transferred as appropriate for the system. Note that some systems create additional records that you may want to track and manage such as critical metadata associated with records in the system. [Slack], [Zoom], Others?

Email: **Email is a record**. Whenever an email message is sent in the course of University business that email becomes an official record of the University. Such records can be subject to disclosure in response to an open records request or subject to subpoena by courts. So it is important that you take care when sending emails for a business. [See Also PPM 3455 and link to https://www.k-state.edu/policies/ppm/3400/3455.html]

In today's world, we all have multiple email accounts. Some are personal (such as Gmail, etc.), and some will be institutional (such as your KSU employee account). Always use your KSU employee email account for University business. Also, try to avoid using your KSU employee email account for personal communication; that is best for personal accounts.

If you use a non-KSU employee account to create, respond to, or store work-related information you are increasing the risk of causing an inadvertent privacy breach by using a non-authorized service provider. In addition, those emails are still subject to open records requests and subpoena so you run the risk that your own personal emails will be drawn into an open records request. For these reasons, it is important that you keep your personal and work-related correspondence separate.

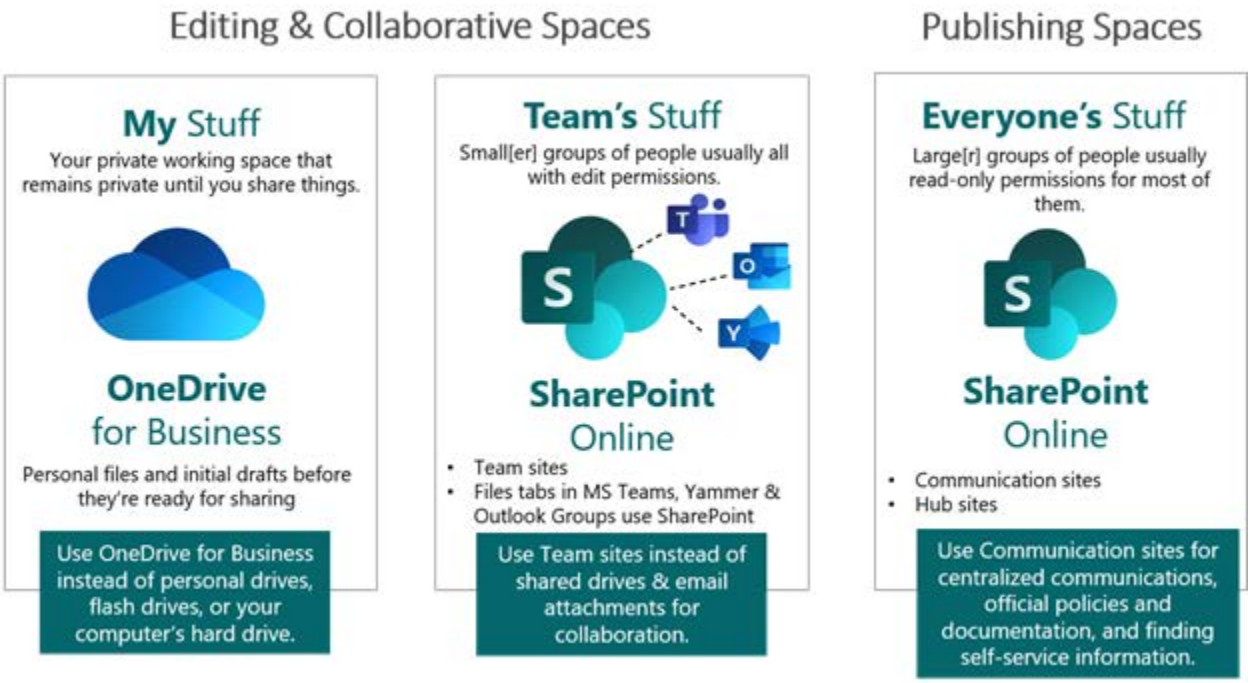
Be sure to keep and file email records appropriately. Retain messages that are sent and received only if they relate to University business; all other messages can be treated as transitory and deleted. (See also Email Records Management FAQ)

- When retaining a series of replies or forwards, keep only the last message as long as the thread is complete and has not been changed in the course of the exchange.
- Make sure to retain information in the header regarding the sender, recipients, date and time; this helps preserve the context of the message.
- *Note* The email system is not a recordkeeping system. A recordkeeping system organizes records according to a file plan, provides shared access to those who need it, and applies retention and disposition rules. So, it is best practice to implement a file/folder structure for your email account.

Bring Your Own Device (BYOD): [see attached document]

Infographics:

These infographics were taken from the University of Washington and we have permission to take or change as much as we would like. I propose we work with DCM and ITS to develop infographics that work for our needs and publicize them at training, K-State Today, and other areas as needed.



Glossary of Terms:

Long term: the length of time needed to retain a record to satisfy the minimum retention period of a record. Retention periods can range from one year to several decades.

Record:

1. A written or printed work of a legal or official nature that may be used as evidence or proof; a document.

2. Data or information that has been fixed on some medium; that has content, context, and structure; and that is used as an extension of human memory or to demonstrate accountability.

3. Data or information in a fixed form that is created or received in the course of individual or institutional activity and set aside (preserved) as evidence of that activity for future reference.

4. An instrument filed for public notice (constructive notice); see recordation.

5. Audiovisual Records: A phonograph record.

6. Computing: A collection of related data elements treated as a unit, such as the fields in a row in a database table.

7. Description: An entry describing a work in a catalog; a catalog record.

Retention schedule: A document that identifies and describes an organization's records, usually at the series level, and provides instructions for the disposition of records throughout their life cycle.

Short term: the length of time needed to retain a record to complete a task or project. Lasting from days to years.

Transitory record: a record that has little to no documentary or evidential value and that need not be set aside for future use. Examples of transitory records include correspondence that requires no administrative action, policy decision, or special handling; and non-record copies of quasi-official notices, such as memoranda, that are not used as the basis of an administrative or program action or decision.

Attachment # 4:

From: Donald Crawford
Sent: Monday, November 2, 2020 2:26 PM
To: FSCOT <fscot@KSUemailProd.onmicrosoft.com>; tech-comm@listserv.ksu.edu
Subject: Discussion about Microsoft Teams message retention schedule

Good afternoon colleagues.

I received an email today regarding the Microsoft Teams message retention schedule. I would like to share the message as I suspect others may be having similar discussions within your respective constituency.

"*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.service-now.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?

Appreciate your time and your thoughts!

—

Donald P. Crawford, MCSE, MCP+I, A+
Information Technology Manager
Architecture, Planning & Design
Kansas State University
Manhattan, KS 66506

APDESIGN THE COLLEGE of ARCHITECTURE, PLANNING & DESIGN // K-STATE