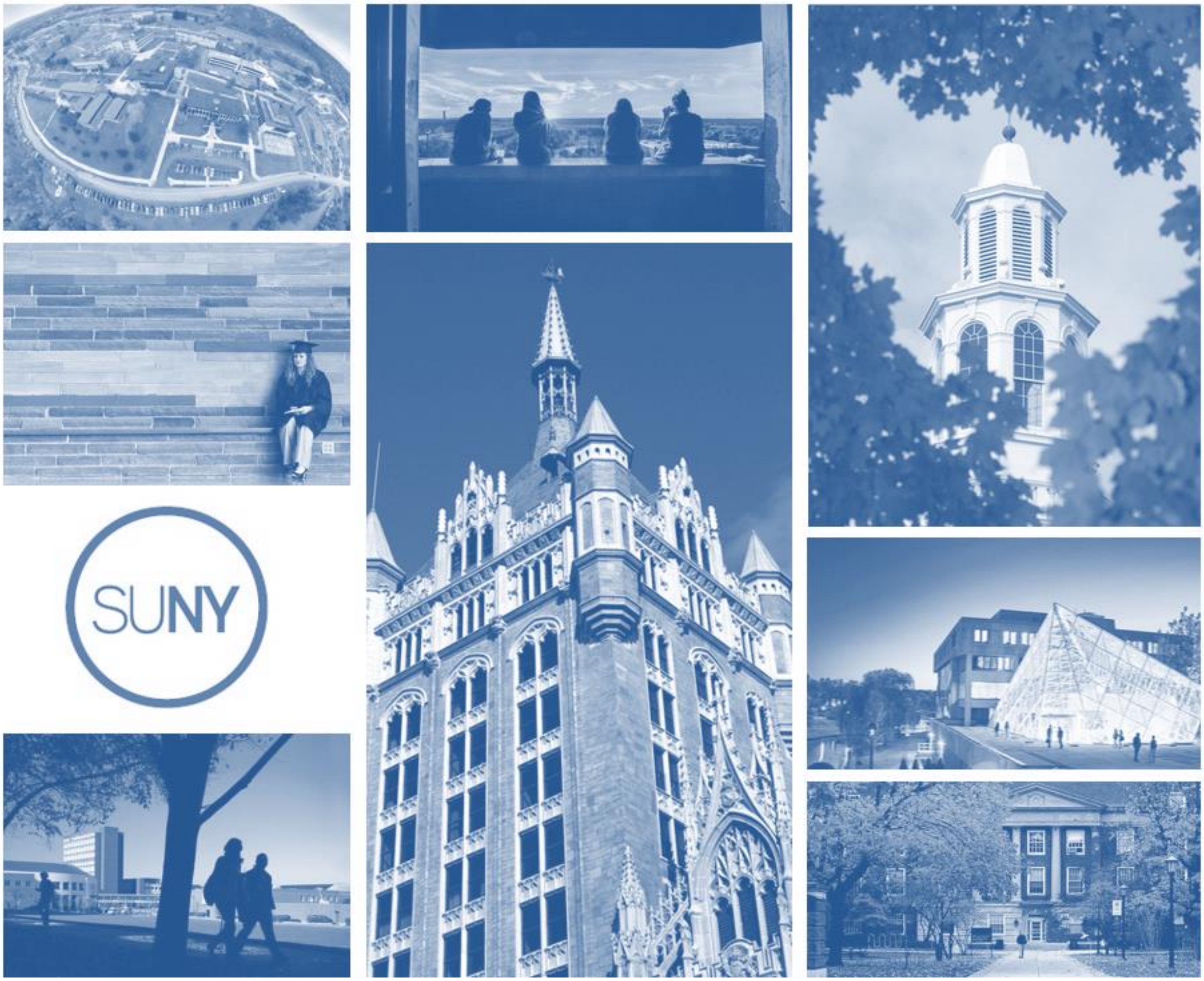
SUNY Email Retention Guidance

Prepared by the SUNY Compliance Office and the Office of General Counsel

> ***"Retention policies are best applied to information by subject, not by the medium on which it is stored. That's why we don't have retention policies for paper."***



Published April 2014, updated August 2015

Executive Summary

At the SUNY Office of General Counsel, the question "How long should we retain email?" is a frequent inquiry from our campuses. The answer is that email is simply a medium. Retention policies are best applied to information by subject, not by the medium on which it is stored. That is why we do not have retention policies for paper or CDs, or any other medium that contains information. The purpose of the following guidance is to shed light on what SUNY campuses should be doing with regard to retention of emails.

Contents

What is a record on SUNY campuses? 2

Are emails records? 2

Why don't we have a set retention period for all emails? 2

What does SUNY Records Retention Policy 6609 say about email? 2

What does the State Archives General Retention and Disposition Schedule say about email? . 3

How should emails that are records be retained? 3

Why should emails that are not records be deleted in a timely way? 3

What about retention of instant messaging system messages? 4

What are the costs and risks related to storing emails? 4

How do we manage and reduce email volume? Adopt a policy. 5

What elements should an email policy contain/ include/ address? 6

For more information on records retention and disposition at SUNY, visit the SUNY Compliance website and the topic pages about records management and e-discovery.

What is a record on SUNY campuses?

A "record" possess all of the following *three* elements:

- Documentary material,
- Transmitted or stored by a campus, and
- Has legal or operational, or historical value.

The SUNY Records Retention Policy Doc. No. 6609 defines a record as follows:

> *"Records - all books, papers, microforms, computer-readable tapes, discs or other media, maps, photographs, film, video and sound recordings, or other documentary materials, regardless of physical form or characteristics, made or received by State University of New York or its campuses in pursuance of law or in connection with the transaction of University business and retained by the University as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities. Library or museum materials made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of blank forms shall not be deemed to constitute records."*

Are emails records?

Most emails are NOT records. Most emails are simply ESI (Electronically Stored Information) without a lasting legal, operational, or historic value. Only emails that serve a legal, operational, or historical value are records, and the rest should be deleted accordingly.

Why don't we have a set retention period for all emails?

Email is simply a medium. Retention periods are best tied to the information in a record, not the medium on which it is stored. This is why we do not have retention policies for paper, videotapes, Word, Excel, .PDF, or any other materials that we use to store information.

What does SUNY Records Retention Policy 6609 say about email?

The SUNY Records Retention Policy Doc. No. 6609 addresses email in the Introduction section (available in the appendices to the Policy). The introduction says the following with regard to email:

> *"Generally, records transmitted through email systems have the same retention periods as records in other formats that are related to the same function or activity. Email records should be scheduled for disposition in conjunction with any other records related to that function or activity. Campus and University officials may delete, purge, or destroy email records if the records have been retained for the minimum retention period established in the RR&D Schedule and are not being retained for a legal action or otherwise subject to a litigation hold or for an audit. Transitory messages may be destroyed when no longer needed. For further guidance on the disposition of e-mail messages and attachments, see item 90369 in the State Archives' General Retention and Disposition Schedule for New York State*

> *Government Records (available through a page on the State Archives website where the schedule is published)."*

What does the State Archives General Retention and Disposition Schedule say about email?

The New York State Records schedule, titled the State Archives' General Retention and Disposition Schedule for New York State Government Records, directly addresses email in its schedule also. The schedule states the following with regard to email:

> ***90369 E-Mail Messages --** Incoming and outgoing e-mail communications, including attachments, used to distribute information and documents, announce or schedule meetings, and conduct formal and informal communications.*
> ***Minimum Retention and Disposition: Destroy after messages and attachments are opened and records have been saved in appropriate electronic or paper file.***
> ***Justification:** Many e-mail communications are not records and are therefore suitable for immediate destruction. Those messages and attachments which are records should be maintained in appropriate electronic or paper files and disposed consistent with applicable authorizations for those records.*

How should emails that are records be retained?

SUNY's email retention approach is to classify emails that are records by determining the subject matter and purpose of the email. The content of the email will determine what, if any, classification of records the email falls under, and retention of the email will then be in accordance with the SUNY Records Schedules based on the type of record it is. Emails that fall into a specific categories of records on the two records schedules that apply to SUNY should be kept in accordance with the corresponding schedule item. The schedules applicable to SUNY are available via the SUNY Policy Doc. No. 6609 Records Retention and Disposition (with schedule appendices that cover activities related to SUNY-specific business), and the State Archives' General Retention and Disposition Schedule for New York State Government Records schedule that covers records common to all state agencies – such as financial and employment records. Emails that do not fall into a category of records identified on either the SUNY schedule or the State schedule are likely not records, and should be deleted permanently unless they serve an important operational value to the employee or are subject to a legal hold.

An example: If the email represents part of an individual student's conduct record—a charge notice for instance—it should be kept in accordance with the SUNY schedule item on student conduct records and retention of such records. If an email is an invitation to a meeting, it probably has no value after it has been read (or maybe after the meeting has taken place) and should be deleted.

Why should emails that are not records be deleted in a timely way?

Emails that are not records, and are just ESI with no legal, operational or historic value, convert to a record when the following "trigger" scenarios occur:

- Relevant to a legal action that is reasonable anticipated as per counsel’s instructions
- Subject to an audit by University Audit or an oversight agency
- Subject to a public information (FOIL/FOIA) request

Only ESI that exists at moment of a "trigger" can convert to a record. But the events above will serve to convert existing email that previously served no legal, operational, or historic value into a record, which triggers our legal obligation to preserve.

What about retention of instant messaging system messages?

Keeping records of instant messages is akin to recording every conversation in every hallway and office on your campus and retaining those recordings for responding to future FOIL requests and litigation holds. People use instant messaging in a conversational way and do not intend those messages to be stored for future use or misuse. The more data you keep, the more records you will have to sort through for any number of audits, information requests, litigation holds, etc. So, if you have no obligation to keep something like instant messages that are generally useless, get rid of them!

What are the costs and risks related to storing emails?

The costs and risks associated with storing email long term go beyond simple storage and server costs. Retaining thousands of unnecessary emails creates legal and administrative e-discovery costs and greatly increases regulatory burdens. While data storage costs can be clear and predictable (i.e., cheap cloud storage systems that allow vast amounts of email data), the costs associated with e-discovery can vary based on the amount of information that must be identified, organized, and reviewed. One thing regarding e-discovery is predictable: the more information that an institution retains, the more information it must process when it is subject to a litigation hold or demand.

SUNY campuses are even further at risk in this respect because, as a public institution in New York State where Freedom of Information Laws (FOIL) are broad, SUNY is legally required to review and produce documents and data, including email, at the public’s request regardless of the purpose of the request or the nature of the document/data. This leaves use vulnerable to harassment and ill-intentioned requests for useless data that must nevertheless be processed. In addition, SUNY campuses are subject to reviews by any number of agencies charged with enforcing certain legal and compliance obligations. The scope and burdens of such reviews can be greatly increased when campuses keep more information than required.

The risks are clear: When a litigation hold, discovery request, or a public request for information occurs, the more documents/records/data we have to sort through, the more disruptive the request will be to the normal operation of a campus. In today’s climate, many people simply retain any and all emails forever, but without knowledge of how retaining all those emails could negatively impact them and the organization. The SUNY Records Retention and Disposition policy 6609, along with the New York State schedule, clearly describe that most emails are not records, and should be deleted accordingly. Even the United States Supreme Court has endorsed the idea that unnecessary email should not be retained, in the case of Arthur Andersen LLP v. United States, 544 U.S. 696 (2005).

This is not a matter of purging damaging information or eluding regulators; it is simply a matter of placing reasonable limits on the resources we devote to information storage and processing. Remember, all that we are deleting is material without legal, operational, or historical value.

In addition, we must not forget about data breaches. Having more documents/data/records, especially in electronic format, creates more risk for breaches of the information contained in them. Further, the more information in question that could be breached, the higher the cost will be to conform to the New York State Breach Notification laws, which require notice to those whose data has been compromised. Data breaches are costly and unavoidable. The surest way to reduce the risk is to reduce the amount of breachable data.

How do we manage and reduce email volume? Adopt a policy.

Campuses can and should develop email retention policies and defensible disposition programs to reduce the costs of storage and e-discovery while maintaining regulatory and legal obligations.

The best way to reduce email volume and manage email may be to set a policy whereby email is deleted after a certain period of time by default unless it is intentionally saved by a user. If an email program, such as Outlook, is set to automatically delete email that is left in a default folder, it will reduce the volume of emails, which most of the time (per the State schedule) are not records that should be retained. Logistically, the setting should act whereby any email that needs to be retained for record retention purposes, or because it has an operative value, can be retained by actively placing the email into a specific folder within the email account, or saving it as a PDF to a hard drive or network drive. Emails that are simply left in default folders such as "inbox," "sent" or "trash," should be automatically destroyed after the user has had time to move them into a longer-duration folder or medium—usually 30–90 days.

Note that if you implement something like an auto-delete feature on emails, you need to be sure to tell your campus—everyone needs to be aware of the setting so that they manage their email effectively. If the auto-delete setting is not effectively communicated, then you may have a lot of angry people at your campuses wondering why their emails are disappearing—and requests to IT to retain back-up tapes so that they can get the email back. You may also be at risk for **spoliation** (the intentional or negligent withholding, hiding, altering, or destroying of evidence relevant to a legal proceeding). See below What elements should an email policy contain (#8), for more information on spoliation and how to prevent it within your policy.

Document management systems can (and should) be used to enable organization and categorization of the emails. Outlook is one example of a document management system, and allows for rapid categorization and "bucketing" of emails into folders specified by the organization. Email archiving solutions, in which emails are housed in the vendor's archiving program, can be helpful because it allows for a single individual to manage litigation holds and run searches directly in the program. Drawbacks to the archiving model include cost (they are not cheap) and enabling the problem of "bloat" in the email system, where employees are retaining more than they should be in the first place. Before campuses look into an archive option for email, they should evaluate why the "bloat" exists in the first place (usually lethargy or a tendency toward e-hoarding), and how the problem of excess records could be handled prior to the installing of any archive feature.

What elements should an email policy contain/ include/ address?

Aside from the auto-deletion features that your policy should set out as described in the previous section, what else should an email policy (and corresponding procedure) include?

1. **REQUIRE USE OF UNIVERSITY-ISSUED EMAIL ACCOUNT**
   The policy should require that employees of the campus MUST use their University-issued email account for University business, and MAY NOT use personal email accounts for University business.

2. **RETAIN EMAILS THAT ARE RECORDS BY SUBJECT MATTER IN ACCORDANCE WITH SUNY'S SCHEDULE**
   The policy should establish that, although most emails are not records, those that are should be maintained in accordance with the applicable records retention schedule by a designated custodian according to the subject matter concerned, as described in the section of this document covering How Emails that are Records be Retained.

3. **CLEARLY IDENTIFY POLICY SCOPE: WHO IS COVERED BY THE POLICY**
   The policy should be applicable to all employees (including volunteers) who create, send or receive email messages and attachments.

4. **REFERENCE THE UNIVERSITY'S EXISTING ACCEPTABLE USE POLICY**
   The email policy should refer to your campus' Acceptable Use Policy regarding what is an appropriate use of a University email account. If the campus does not have such a policy, they should develop one in conjunction with the email policy.

5. **EXPLAIN MECHANISM FOR RETAINING EMAIL RECORDS THAT ARE RECORDS**
   The policy should state how users can create folders locally, or on their email account, with varying retention parameters to store files that should be retained.

6. **SET PRIVACY EXPECTATIONS FOR THE EMAIL USER**
   The policy should address data privacy and expectations of privacy by the user. It should be made clear that employees using campus email systems should not have a strong expectation of privacy when using campus information technology resources. To this end, it is much more effective to specify the reasons that email privacy will be intruded by the campus, rather than to simply say there is "no expectation of privacy." Legitimate reasons that accounts could be subject to unilateral access by the campus administration should include discovery proceedings, audit inquiries, freedom of information requests, policy enforcement and other legal actions.

7. **DESCRIBE LOCAL PROCEDURES FOR EMAIL RETENTION FOR THE INDIVIDUAL USER**
   The policy should identify where email records will be managed, stored, and retained within the infrastructure of the campus, and how the employees should retain their own emails that are actual records locally within their campus email management system (such as Outlook or Gmail).

8. SET PROCEDURES FOR EXCEPTIONS TO THE AUTO-DELETION PROTOCOLS

The policy should explain how IT handles exceptions to the retention settings if auto-delete options are put in place. This part should make clear *how* an employee would retain the emails that *must* be retained under SUNY's Legal Proceedings Preparation (E-Discovery) Procedure. A clear process must be outlined in order to prevent any charge of **spoliation** (the intentional or negligent withholding, hiding, altering, or destroying of evidence relevant to a legal proceeding).

9. POLICY TRAINING AND EDUCATION

The policy should discuss how managers and users will be trained on the policy. Even the best policy has limited value if it is not publicized and enforced.

10. MANDATE COMPLIANCE WITH POLICY

The policy must be mandatory for all employees, and include compliance measures to ensure that the policy is followed. It should be established that Internal Audit or other campus oversight measures have the authority to review and assess compliance with the policy as necessary and that disciplinary procedures may be initiated to address noncompliance.

11. REQUIRE PERIODIC REVIEW OF POLICY TO ENSURE IT IS CURRENT

The policy should be reviewed annually, or on some other regular cycle, to ensure compliance with other SUNY and State policies, any new laws or regulations. It should also be reviewed when IT Systems change (i.e. a new email, document management, or e-discovery system is put in place) to ensure that the new system is set up with protocols to ensure compliance under the email policy. In addition, it must be understood that any new systems will once again require user training to make sure employees are aware of how to ensure preservation of emails that are actually records.

12. IDENTIFY TWO INDIVIDUALS WHO WILL BE CHARGED WITH ENSURING CAMPUS COMPLIANCE WITH THE POLICY

The policy should identify two people responsible for ensuring compliance with the email retention policy. The campus Records Management Officer, who is already charged with ensuring compliance with the records retention schedules, should be charged with ensuring compliance with the policy in the individual offices, and offering trainings to make sure that employees are aware of how to appropriately use their email and how to retain emails when necessary and appropriate. The second person responsible should be someone in IT, who has an intricate understanding of the systems and servers where email is stored, so that they can better control how the IT side handles and stores the emails. These two people must work together to ensure that the protocols are set up appropriately on the systems and that the policy is communicated to those whom it impacts. It is advisable that these are the same individuals who are designated as members of the campuses' e-discovery response team.