**Memorandum**

To: Division Heads (to be shared with your departments)

From: Thomas V. Flynn
 General Counsel

Date: 9/13/2013

Re: Retention and Destruction of Electronically Stored Information

Policy E1.3 Retention discusses the “efficient and effective retention of Stonehill College records.” The policy applies to records in both “electronic [and] paper form.” The following memorandum provides information regarding College requirements for the retention and destruction of electronically stored information (“ESI”) and is intended to provide a deeper explanation of Policy E1.3’s application to ESI.

Document Defined. Document management is the process by which we as College employees store, classify, search, share, retrieve, and eventually destroy our documents. For purposes of this memo, a “document” is an electronic, digital container of information (a file). A document may be a word processing file, a graphic image, or any other discrete, identifiable information unit that can exist within a computer system.

Saving Documents. Effective January 31, 2014 all departments should begin the process of creating internal procedures which ensure that documents are saved based on their subject matter and not by individual user (employee) accounts. The practice of saving documents on local user hard drives should be discontinued. All files should be saved in a central location as designated by Information Technology.

File Naming Conventions. Effective January 31, 2014 all users, when manually saving documents within systems which allow for user-determined file names, should save documents so that the file name starts with the date the document was created in year-month-day format (example: 2013-08-15). While not required, departments are encouraged to also begin the process of renaming existing files to coincide with this naming convention. It is recommended that this “back-dating” process be completed by all departments by June 30, 2014.

Cloud Storage. The use of any third party storage, for example Googledocs, Dropbox, Zipcloud, without prior division head approval is prohibited. If your office is currently using such a system, you should phase out such use and transfer all files to a central location as designated by Information Technology.

Email. Many emails and their attachments are covered by the retention policy under various categories of documents. Store these emails and attachments in the appropriate folders and preserve them as directed by the retention schedule(s). Emails not covered by any category other than temporary should be destroyed after they have served their intended purpose. This specifically includes, but is not limited to, emails which contain the automated transcription of voicemail messages.

Employees should not use personal or third party email for work-related activities unless such use is approved by IT. In the event that use of a third party email system is required or necessitated by special circumstances (for example, access to the College’s email is not available and the employee uses his or her personal Google account to send a communication to a colleague), the employee should retain paper copies of all such documents consistent with the applicable retention schedules.

Document Destruction. Document destruction forms must contain information regarding the disposition of all ESI. ESI may not be kept longer than the time periods specified in a College-wide, Divisional, or Departmental retention schedule (in other words, if you destroy a physical copy of a document you must simultaneously destroy the electronic version of the document).

Every department on campus is responsible for purging its ESI on a regular basis consistent with its document retention schedule. Purging is the act of separating active from inactive records in a filing system or database.

The Office of the General Counsel oversees all destruction of documents. Documents, other than temporary documents as defined in Policy E1.3, should not be destroyed without the permission of the Office of the General Counsel. The following are the acceptable methods of destruction for Stonehill College:

* Paper: burning, shredding, pulping, pulverizing
* Microfilm: pulverizing
* Electronically Stored Information: electronic data shredding, degaussing
* DVD’s, CD’s, Laser Discs: shredding, pulverizing

Policy Compliance. Departments shall ensure that:

1. Electronic records are kept for the same length of time as paper records would be kept with similar content, as directed by the College’s retention policy.
2. Primary responsibility for each electronic record rests upon its owner. The “owner” of an electronic record is defined as the originator or author of the record. If a record has more than one author, each is considered an owner with “joint and several” primary responsibility for it.
3. For each electronic record, the owner, in consultation with his or her department’s document retention liaison, must determine the disposal date in accordance with the applicable retention schedule, check to ensure that no cessation of records destruction has been issued, and then properly maintain/dispose of the record as called for.
4. The owner is responsible for assuring that all records are properly authenticated and for preserving “contextual” information such as the date and time the record was created, origin and purpose of the record, recipients of the record, etc. in order to validate the authenticity of the document in question.
5. All ESI must be stored so as to be retrievable by authorized company personnel throughout the applicable retention period.
6. When a computer or device is retired or assigned to a new owner, IT shall be contacted before any data or files of any kind are altered or removed so that proper retention, transfer, or removal of documents is achieved.
7. Records with similar preservation periods should be stored together on the same medium, whenever possible.
8. When retiring a software application, take appropriate measures to ensure that the associated record is retained in a retrievable, usable, format for the preservation period associated with that record. If the preservation period for a particular electronic record is more than three years, and if the program that produced the data is not widely accessible (i.e., other than Word, Excel, PowerPoint, Adobe PDF, etc.), then either print and save a hard copy instead of the electronic record, or convert the electronic record into a more widely used format. If neither of these alternatives is sufficient, then make arrangements with IT for keeping and properly storing necessary hardware and software (such as computers, tape or CD drives, operating systems, and programs) so that the data can be read and printed. Document which hardware and software is being retained for the purpose of these records, and where it is located. This should include training materials and setup and configuration for the hardware, operating system and programs, as well as instructions on how to restore and access data (i.e., user’s guide).
9. Electronic records sent to an offsite storage facility must have a destruction date set in consultation with the Office of the General Counsel. This includes archived tapes sent to long-term storage.

At least annually, every department should conduct an electronic systems survey to identify where and how ESI is maintained by the department. Such a survey should indentify which applications are being used, which management methods are in place, and the strengths and weaknesses of those methods. It is recommended that each department create a flowchart to specify the existing record flow. The survey should also include an internal audit of the department’s compliance with the College’s data security policy.

Training. The Office of the General Counsel will be providing a comprehensive training for all departmental liaisons on January 29, 2014 from 9 AM to 1 PM in the Cleary Dining Room. Lunch will be provided. All departments should make every attempt to free up their liasion’s schedules that day to attend the training.