Nichols College

Policy on Data, Records, and E-mail Retention

Background

Staff and faculty rely heavily on the records generated as a result of the business and operation of Nichols College. These records help the college in meeting its goals and objectives, assist management in its decision making, and acts as an archive of the college's history.

A records retention policy helps the college to improve office efficiency, facilitate administrative access to records, ensures the consistent maintenance of records, decreases operational costs, increases staff productivity and assists the college in meeting its legal and regulatory requirements.

Purpose

This policy serves as an overarching description of the types of data being stored, and a policy for the retention and destruction of data after its useful life. This policy is intended to coexist with other policies on campus, and comply with legal and regulatory requirements.

It is important to note that this policy applies to all data that is maintained at the college, both paper-based as well as electronic. In the realm of electronic records, it is important to note that e-mail messages are subject to the same data classification and retention requirements as any other data maintained in the student information system, Excel spreadsheets, Word documents, and similar formats.

Data Classification

Data at Nichols College should be classified into one of the following categories:

1) Confidential – Nichols College Confidential data are data that contain personally identifiable information concerning any individual; is regulated by local, state, or federal privacy regulations or any voluntary industry standards; or best practices concerning protection of personally identifiable information that the college chooses to follow. Any paper or electronic data that contain this information must be classified as Nichols College Confidential data by default.

   Regulations may include, but are not limited to:

   - Health Insurance Portability and Accountability Act (HIPAA)
   - Family Educational Rights and Privacy Act (FERPA)
   - Payment Card Industry Data Security Standards (PCI DSS)

- MA Office of Consumer Affairs and Business Regulation 201 CMR 17.00

Examples of Confidential data include, but are not limited to:

- Social security numbers
- Credit and debit card numbers
- Bank account numbers
- Drivers license numbers

2) Operational Use Only – Nichols College Operational Use data are data whose loss, corruption, or unauthorized disclosure would not necessarily result in any business, financial, or legal loss, but which the college has determined is critical to its business and requires a higher degree of handling than unclassified data.

   Examples of Operational Use data include, but is not limited to:

   - Academic advising records
   - Admissions files
   - Student education records
   - Student account data
   - Budgets
   - Salary information

3) Unclassified – Nichols College Unclassified data are data that does not fall into any other data classification.

   Examples of Unclassified data include, but is not limited to:

   - Department faculty lists
   - Press releases
   - Nichols College web site content
   - General, or informational, e-mails

Data Retention - Designations

In order to determine what the retention requirements are for specific sets of data, it is important to insure that data has been categorized according to the classifications above. Each department should have published policies and procedures on retention requirements. These retention requirements should be identified using the following designations:

- **Permanent** – Records that must be kept indefinitely. This designation would be used primarily for confidential and operational data. It is expected that most unclassified data will <u>not</u> fall under this designation.

- **Specific** – Records that will be kept for a specific number of years. Each department must have explicit retention policies regarding records that fall under this category, the reason for retention, and the specific number of years to retain them.
- **Temporary** – Records that need to be retained for a short period of time, and do not fall under the other record retention designations. These records should be disposed of after 6 months from the last date of entry on the record or, in the case of e-mail, date of receipt.
- **Transient** – Records that do not need to be retained because they are used to create other retained records or whose content has no importance or relevance to the college's business or history. These records are of such an extremely short term or irrelevant nature that they are not included in the record retention and disposition schedules and should be immediately be disposed of.

E-mail Messages – Classification

All e-mail messages must be classified using the descriptions above for Confidential, Operational Use, and Unclassified. Per the "Nichols Data Security Policy", "Confidential" data cannot be transmitted via e-mail. Therefore all e-mail messages would fall under the classifications of either "Operational Use" or "Unclassified."

E-mail Message Retention and Management – Clarification of Policy

Nichols staff and faculty currently have four locations to store electronic data on campus:

1) Microsoft Outlook inbox or subfolders
2) Personal "H" drive, OneDrive, and department mapped/shared drives
3) Local "C" drive on PC
4) Removable storage devices, such as a USB key/thumb drive, external hard drive, or CD/DVD

Per the "Nichols Data Security Policy", "Confidential" data must not be stored in any location except mapped/shared drives on a Nichols College server. It is good business practice to apply this same level of security to "Operational Use" data as well, when possible.

A common practice on the part of some staff and faculty is to create a "personal" Outlook folder (i.e. a "pst" file) on their "H" drives and then move e-mail messages to this folder. Some people do this in order to stay below their e-mail quotas, and avoid the task of cleaning out their inbox of unneeded messages to free up space. From a server utilization perspective, this practice creates no savings or benefits. The server storage load has just been transferred from one physical server to another. From a business operations perspective, this practice serves to complicate the retrieval of

important data, in the event that the person storing the data is not available. Therefore the creation of a personal folder that is stored on a network drive is not allowed. It should also be obvious that a personal folder stored on the “C” drive of a PC is not recommended due to issues with security and risk of data loss, since the “C” drive is not backed up.

The only time a “personal” outlook folder should be created is in the case of “Operational” data (e-mail messages) that is going to be burned to a CD/DVD or USB key/thumb drive, with the messages subsequently deleted. The expectation is that the CD/DVD or USB key/thumb drive will then be secured in a locked cabinet or safe, adhering to the security requirements for this type of data.

Also, per the acceptable use policy, users are not allowed to use their Nichols e-mail account for storage of personal e-mails and/or attachments.

--- END ---