

<b>Policy Name:</b>	Data Management Policy		
<b>Policy No:</b>	6.10	<b>Approval Authority:</b>	Senior Management Team
<b>Volume:</b>	6, Computer Services	<b>Responsible Executive:</b>	Director, Computer Services
<b>Chapter:</b>	10, Data Management	<b>Responsible Office:</b>	Computer Services
<b>Originally issued:</b>	March 2019	<b>Revisions:</b>	

### Policy Statement

All employees who collect, store or handle institutional data must follow the directives and guidelines in this policy to manage the data assets of the University effectively and efficiently.

### Reason for Policy

This policy provides guidance and direction on the management of institutional data throughout the information lifecycle.

### Policy Applies to

- All institutional data.

### Who Should Read this Policy?

- All employees of NSCAD University, who collect, store or handle institutional data.

### Contacts

Please direct any question on policy meaning or application to the Director, Computer Services, 902-444-7203 or [computer@nscad.ca](mailto:computer@nscad.ca).

## Definitions

**Employees:** All faculty, staff and administrators of NSCAD University.

**Institutional Data:** Data is the representation of facts as text, numbers, graphics, images, sound or video. Institutional data captured through the operation of the University. It can include, but is not restricted to staff data, student data, financial data, facilities data, curriculum data, etc.

**Personal data:** Personal data is data where a person's identity is apparent, or can be reasonably ascertained. Note that a person's name is not necessary for data to be personal.

**Reference data:** Data used to classify or categorize other data. It can include, but is not restricted to, status codes, state abbreviations, demographic fields, etc.

**The University:** NSCAD University

## The Policy

1. Institutional data should be collected only when known and documented uses and value exist.
2. Collection of accurate and complete data is expected, even when elements are required by a department of the University which is different to the department undertaking the collection.
3. The University collects and uses personal data about its students, staff and others in order to operate effectively. Personal data held by the University is protected under the Nova Scotia Freedom of Information Act and Protection of Privacy Act (FOIPOP a copy is posted on NSCAD's Computer Services web page) and the Nova Scotia Personal Information International Disclosure Protection Act (PIIDPA).
4. For accountability and stewardship, all data must have a defined Data Steward responsible for accuracy, integrity, and security of data. Data Stewards are responsible for ensuring that all legal, regulatory, and policy requirements are met in relation to specific data assets. A list of data stewards is provided in this policy.
5. Whilst data re-use is encouraged, data duplication is discouraged. For integrity, data should be entered only once, and any duplication of the collection or storage of data needs approval of the relevant Data Steward and reported to the Director, Computer Services. Staff should collaborate to prevent the storage of duplicate data assets, wherever possible referring to an organizational single source of truth rather than saving a local department copies.
6. The timely destruction of data is essential for effective management. Institutional records are destroyed after fulfilling the minimum retention period prescribed by the Government of Nova Scotia and the Government of Canada. Retention periods in records authorities consider business, legal and government requirements and the University uses several general and agency-specific authorities to determine retention, destruction and transfer actions for its records.
7. Processes for data capture, validation and processing should be automated wherever possible.

8. Business processes must ensure the maintenance of reliable data. All institutional data management practices in the University are to be in accordance with these procedures and related policy.

### **Data Stewardship**

For accountability and stewardship, all data must have a defined Data Steward responsible for accuracy, integrity, and security of data. Data management, authority and accountability for data assets within their allocated data domain. Data is shared to the maximum extent possible in accordance with security requirements. Data quality is actively maintained to a high standard. Business process for the data is established. Concerns of others relating to data assets under their care are addressed.

A collaborative approach for addressing institutional data quality issues is critical to maintaining data integrity. Data quality issues relating to: accuracy, completeness, duplication and/or currency of data, or changes to business processes impacting on data collection and recording, should be provided to the appropriate data steward for action. The Data Steward will conduct preliminary/root cause investigations, evaluation of possible solutions, and ultimately, propose a final solution. The Data Steward may call on Data Administrators and other members of the University community to assist in this step. The Data Steward is responsible for the implementation of a solution to resolve the data quality issue.

At times, an identified data quality issue will be outside the responsibilities of a single Data Steward. In these instances, it may take collaboration or further resources to identify the root cause and propose a solution.

### **List of Data Stewards**

- Employee data – The Director of Human Resources and the VP Administration/Finance
- Financial data and facilities data – The University Controller and the VP Administration/Finance
- Student data, academic data and curriculum data - The University Registrar and the VP Academic

### **Forms and Tools:**

N/A

**Data Management Policy:** <https://nscad.ca/site-nscad/media/nscad/6.10DataManagementPolicy.pdf>