INFORMATION MANAGEMENT

NORTHWESTERN POLYTECHNIC

INFORMATION MANAGEMENT POLICY			
Effective Date	June 1, 2023	**Policy Type**	Administrative
Responsibility	Title of the person(s) responsible for ownership and implementation of the policy	**Related Policies**	IT Acceptable Use IT Security IT Access Control Records Management
Approval Authority	Board	**Review Schedule**	June 1, 2028

1. **Policy Statement:** To manage NWP's data as a strategic asset, sound principles of governance are required to ensure data quality, integrity, access, security, use, and disposal. This Policy on NWP establishes roles and responsibilities for managing. NWP's data, as well as more detailed standards for the operational management of these data.

2. **Scope:** All members of the NWP Community are responsible for complying with applicable law and regulations and institutional policy with respect to NWP Data, as defined below.

3. **Reason for Policy:** Information Management Policy promotes and supports the responsible use of high-quality institutional data, to facilitate informed and insightful use of these data, and to increase their value to the NWP community and beyond.

4. **Definitions:**

"Data": Recorded, ordered symbols (e.g., letters, numbers) that carry information. Data are the basic building blocks of information and knowledge. There are many types of data that can be categorized by form (digital, analog), purpose (thematic, spatial, temporal), processor (numeric, text), and media (documents, images, video, audio).

"Information": Data that have been interpreted or translated to reveal the underlying meaning. For example, data can be processed and interpreted as words, statements, and ideas. NWP, information is generally specific to a particular domain (activity, process, function). Information may be presented in many formats (reports, images, tables, charts) and media (documents, sound recordings, photographs, video). Information is more valuable than data.

"Legitimate NWP Business Purposes": Lawful business purposes that are consistent with the context in which data are provided to the institution, as well as considered as appropriate by reasonable NWP Community expectations.

"Northwestern Polytechnic Community": A Member of the NWP Community. Member(s) under this Policy includes but is not limited to the following: 1) Employee: any person who is employed by NWP or who provides services to NWP under an employment contract. 2) Student: any person enrolled in study at NWP. 3) Volunteer: any person performing work for NWP in an unpaid capacity. 4) Contractor: an individual or company (and its employees) who provides services to NWP under a service contract (i.e., a non-employee-employer relationship). 5) Community Member: any person working in collaboration with NWP for a business or an academic purpose, former students, or alumni.

"NWP Data": Any data or records created or received by NWP employees or other constituents in the performance or transaction of NWP business that are shared by Authorized Users across departments. Administrative data collected in the course of the institution's research activities covered by NWP's Regulation on the Conduct of Research, as well as the regulations of the research sponsors. NWP Data include, but are not limited to, machine-readable data, data in electronic communication systems, data in print, and backup and archived data on all media.

5. Guiding Principles

1. This policy is guided by on the principle to promote effective governance structures and processes to provide mechanisms for strategic oversight and decision-making, as well as transparent and accountable leadership, and support the institutional goals.

2. The NWP Board of Governors is the owner of NWP Data. Individual departments, divisions, or schools bear responsibilities for certain defined domains (types) of NWP Data. The Data Governance Steering Committee (DGSC), Data Trustees, Data Stewards, Data Managers, and those in Technical roles perform distinct functions and have responsibilities for NWP Data as described below.

3. NWP Community is responsible for safe, secure and accuracy of data. Protecting NWP's Data is a responsibility shared by all members of the NWP community. Data protection begins with the person or office creating the data and is the continuing responsibility of all who subsequently access and use it.

4. Data is collected, stored, and disposed of in ways appropriate to the risk and impact of unintended disclosure.

5. Access to data is open and transparent while abiding by institutional policies, legislation, personal privacy, security requirements and collective agreements.

6. Data Governance Steering Committee (DGSC) with responsibilities for this policy development are responsible for applying laws governing data access and related issues. DGSC strategic data access, standards and disclosure.

Responsibilities:

Designated individuals within the NWP have specific data management accountabilities and responsibilities as outlined in the Data Governance Steering Committee (DGSC).

Information and Technology:

Information Technology (IT) is responsible for maintaining the availability and security of the NWP's data infrastructure and ensuring that authorized users have access to the data they require for academic, research, and administrative activities.

IT is responsible for implementing security and access measures that mitigate the risk of unintended disclosure of electronic data. This includes, but is not limited to, continually improving end-user awareness of proper data management; maintaining physical security of data infrastructure; implementing appropriate data access; and providing data cataloging technologies to users.

Divisions:

Academic, administrative and ancillary units are responsible for ensuring they access and use NWP data (both electronic and hard copy) in a manner that minimizes risk to the NWP.

The best way to minimize risk to electronic NWP data is to use the NWP-approved IT infrastructure (including data centres and end-point devices) and services for all NWP activities to the greatest extent practicable.

NWP Community Members:

Individual members are responsible for ensuring they access and use NWP data (both electronic and hard copy) in a manner that minimizes risk to the NWP. They must understand that data management is a shared responsibility across the NWP community, and they must abide by data management procedures and practices. These responsibilities include:

- Using data only for authorized and intended purposes.
- Understanding the data and guarding against misinformed or incorrect interpretations. For any questions regarding the data, they should contact the designated individual with data management accountability for that data.

- Respecting the privacy of the data and the individuals that it represents. This includes not disclosing personal information, nor accessing or manipulating such data for personal gain or interest.

- Ensuring that they do not knowingly falsify data nor inappropriately delete or reproduce data.

Non-compliance

If there is reason to suspect that laws or NWP policies have been, or are being violated, or that continued access poses a threat to the NWP's data, data infrastructure, NWP community members or the reputation of the NWP, access to the NWP's data and data infrastructure may be restricted or withdrawn.

Following due process, the NWP may take action against anyone whose activities are in violation of the law or of this policy. The actions taken may include, but are not limited to:

- Revocation of access to the NWP's data, IT services, and IT infrastructure.

- Disciplinary action for students following the Student Rights Responsibilities (Standard of Student Conduct in Non-Academic Matters).

- Disciplinary action for employees (Progressive Discipline Policy).