OLYMPIC COLLEGE POLICY

TITLE: Data Governance Policy

POLICY NUMBER: 200-11

REFERENCE: State Board of Community and Technical Colleges – Data Governance Committee and College Resources**; Preservation and Destruction of Public Records**, RCW 40.14**, Public Records Act**, RCW 42.56; **OC FERPA (The Family Educational Rights and Privacy Act)** Policy #300-07

I. Introduction

Data Governance is the practice of making strategic and effective decisions regarding the College's information to optimize data integrity, data quality, and ensure that derived data is meaningful and useful. This is accomplished by applying formal guidelines and processes for the management of the College's information and the assignment of responsibility for their compliance and evaluation.

II. Purpose

This policy establishes data governance standards and guidelines for the management of institutional data to ensure the availability, usability, integrity, and security of data used by Olympic College.

III. Applicability

This policy applies to anyone at Olympic College who creates, accesses, manages, or relies on data for decision making and planning.

IV. Definitions

A. ***College Data*** – Data that is created, acquired, or maintained by College employees in performance of official administrative job duties.

B. ***Critical Data Assets*** **-** Data assets selected based on their criticality to include data required to be always available and protected or contain confidential information and require special handling.

C. ***Data*** - Non-physical bits of information that when organized or processed can be made coherent or useful.

D. Data Assets - Entities comprised of data determined to have specific value that include information assets, system and software assets, and information technology assets.

E. Data Classification – The classification of College data using the categories identified by the Washington Community and Technical College System.

F. Data Governance Council (DGC) – The body that establishes policy and guidelines for the management of and access to the College's Data in accordance with existing College policies.

G. Data Integrity – Processes used to ensure that data is current, accurate, and secure.

H. Data Management – Processes used to define and manage the data of the College to provide a consistent point of reference.

I. Data Retention – Processes used to define the retention and disposition requirements for College Data.

J. Data Types – Any information derived from non-physical data in its raw form that when organized or processed can be made coherent or useful.

V. Data Governance Scope

A. Data Governance Network

Responsibility for data governance is shared among essential data areas throughout the college. These roles include:

i. *Data Governance Council (DGC)* - The DGC provides oversight and guidance for the College's data governance activities to ensure data availability and integrity, best practices in data management, reporting standards, information consistency, and data access. This includes establishing data definitions and standards, recommending data policies, performing data quality reviews, providing data analytics support, and overseeing the execution of data management.

ii. *Data Administrators* - Data Administrators are senior College officials appointed by the President with executive level responsibility for essential data functions, which may include the

Chief Information Officer (CIO) and Executive Director of Institutional Effectiveness. These roles ensure data management and analysis align and support the institutional data strategy. They also supervise key personnel who execute key data functions.

iii. *Executive Data System Owners* - Data system owners have executive level ownership of data systems. The function of this role is to apply the business processes and services in coordination with policy and system development. Technical expertise is provided by data experts and data stewards for assistance in complying with established data policy. Data system owners are typically at the Executive Team level. Systems development is overseen by the head of Information Technology and the Office of Institutional Effectiveness. Data stewards are also overseen by this role.

iv. *Data Stewards* – Data stewards are assigned for key functional areas and are responsible for ensuring effective control and use of data and exercising a series of assigned functions as defined by the Data Governance Council. These duties include implementing adopted data procedures, providing expertise and guidance in data system development, safeguarding data from unauthorized access and abuse, and authorizing the use of data within their functional areas. Implementation procedures outline the roles and responsibilities of data stewards in greater detail.

v. *Data Custodians* – Data custodians are typically subject matter experts with responsibilities to maintain data quality in their subject matter processes. Under the direction of a data steward, this role ensures that established data procedures are followed and regular audits are performed. Implementation procedures outline the roles and responsibilities of data custodians in greater detail.

vi. *Data Analysts* – Data analysts provide data analysis and data compilation by interpreting business problems and applying the appropriate derived data definitions.

vii. *Business Systems Analysts* – Business systems analysts provide expertise in data systems design to support business processes and analytics.

viii. *Data Management Team* – The Data Management Team, with oversight from the DGC, is comprised of data analysts and data

stewards who help define and manage the data of the College to provide a consistent point of reference, and ensure data integrity.

B. Data Standards

Data standards will be developed, implemented, and audited regarding data input and derived data definitions.

C. Critical Data Assets

Data assets defined as critical that need to be always available and protected and/or contain confidential information and require special handling. The DGC will maintain an inventory of identified critical data assets.

D. Data Access

College data is managed to ensure that users have access to institutional data and information as appropriate to their role and responsibilities. The College will protect its data assets through security measures that assure the proper use of the data when accessed. Data items will be classified by data stewards to have an appropriate access level. The DGC will establish data access.

E. Data Usage

Data usage is focused on ensuring that College data is not misused or abused, and are used ethically according to applicable law with due consideration for individual privacy. Data usage falls into the categories of *update, read-only*, and *external dissemination*. Authorized personnel must access and use data only as necessary to perform their assigned job functions according to the security levels assigned to the data. Data usage practices will be disseminated through adopted procedures established by the DGC.

F. Data Integrity and Integration

An important function of data governance is to ensure that institutional data have a high degree of *integrity* to ensure data accuracy, consistency, and security. *Data integration* ensures that key data elements can be integrated across functional units and electronic systems so that they can rely on data for information and decision support. Data integrity and integration practices will be conducted in accordance with procedures established by the DGC.

G. Data Types

College data will be managed as a strategic asset in accordance with procedures established by the DGC. This includes: 1) information derived from non-physical data in its raw form that when organized or processed can be made coherent or useful; 2) electronic objects organized using a database; 3) back-up and archived data on all media; and 4) any data that resides on internal systems or systems hosted outside the control of the College.

H. Data Classification

Certain types of information must be strictly protected. All College data requires classification according to the sensitivity of the data. A data classification must also take into account the most sensitive data in the collection. Once information is classified, appropriate security measures must be taken to maintain the confidentiality of that information. College data is classified using the categories identified by the Washington Community and Technical College System. Data classification practices will be conducted in accordance with procedures established by the DGC.

I. Data Analytics

Data analytics and compilation will generally be produced by designated data analysts using derived data definitions whenever appropriate. Strategy and standards to support data analytics will be provided by the head of the Institutional Office of Effectiveness. Data analytics practices will be conducted in accordance with procedures established by the DGC.

J. Data Quality Management

Data quality management ensures that policies, responsibilities, and processes with regard to the creation, acquisition, maintenance, production, disposition and distribution of data are in place. The DGC will communicate these standards to data stewards, custodians, and users through analyzing, implementing, and auditing procedures.

K. Data Controls

The College will implement processes for safeguarding important information from unacceptable use, corruption, compromise, or loss. This includes establishing procedures to control data access, restrict data availability, and ensure data privacy.

i. Protection of Data - Data systems will provide reasonable administrative, technical, and physical safeguards to control access and ensure confidentiality, integrity, and availability of data. This includes the ability to detect and prevent unauthorized or inappropriate access to data. Adherence to data privacy and confidentiality standards shall be verified through appropriate monitoring, auditing, and use of controls, which should be properly documented.

ii. Disaster Recovery Plan - The IT department will maintain a disaster recovery plan to help minimize the impacts from data loss. This plan will outline strategies for backing up critical data assets including critical servers, IT equipment, and essential data.

L. Data Storage

Only College related data and files should be stored on the institution's infrastructure. The College assumes no responsibility for the loss, protection, or restoration of personal data.

i. Authorized Data Storage Locations - College employees shall only use authorized data storage locations, which generally include College servers, individual shared drives, local computer, SharePoint folders, and cloud-based storage.

ii. Removable Storage Devices - Removable storage devices including thumb/USB drives and other removable media shall generally not be used to store any type of sensitive or confidential College data or information.

M. Data Retention and Disposition

It is the practice of the College to: 1) create only the data it needs; 2) retain data according to established records retention schedules; 3) maintain active and inactive records in appropriate storage equipment and locations; 4) preserve data of historical significance; 5) identify and protect vital records; and 6) discard data appropriately when no longer required. The College's Data Retention Policy outlines the institution's data retention standards and requirements for the orderly disposition and maintenance of data.

N. Training

College employees who access, generate, or maintain FERPA-protected information will be required to complete FERPA training prior to accessing Category 3 or 4 information.

Recommended by Allison Phayre, Executive Director	*December 7, 2018*
Office of Institutional Effectiveness	
Submitted to President's Cabinet for Review	*December 18, 2018*
Approved by President	*December 18, 2018*
Submitted to Board of Trustees	*February 27, 2019*
Approved by Board of Trustees	*March 19, 2019*