POLICY

Policy No.	**B.5.1**
Title	**Sharing & Stewardship of Information**
Approval Body	Board of Governors
Policy Sponsor	Vice President Administration & Chief Financial Officer
Last Revised/Replaces	January 30, 1997
Effective Date	September 26, 2018

CONTEXT AND PURPOSE

Vancouver Community College (VCC, the College) is accountable for the collection, integrity, consistency, confidentiality, accuracy and security of information.

This policy establishes how information is managed and maintained as a shared resource.

For information on records retention or protection of privacy, refer to VCC policies A.3.9 Records Retention and A.3.3 Freedom of Information and Protection of Privacy.

SCOPE AND LIMITS

This policy applies to all data collected at VCC or generated through the course of ongoing operations, including personally identifiable data and proprietary information.

This policy applies to all VCC employees and contractors and is complaint with collective agreements.

College data may be stored either electronically or on paper and may take many forms (including but not limited to: text, graphics, images, sound or video). Research data, scholarly work of faculty or students and intellectual property are not covered by this policy.

STATEMENT OF POLICY PRINCIPLES

1. This policy works to establish best institutional practice regarding access, security of data and standards. Policy A.3.3 Freedom of Information and Protection of Privacy (FOIPPA) addresses regulations around what information can be collected and public disclosure of information.
2. VCC is committed to ensuring the integrity of College information and will develop and maintain clear and consistent procedures for access to all College data.
3. VCC is the owner of all data collected, stored and/or managed by College employees or using institutional resources.
4. VCC will apply the “least privilege” data management approach. Employees will only have access to the information they need in order to perform the job duties assigned to them.

5. VCC will ensure that industry standard management and oversight of College data is in place. This information will be maintained and updated through the VCC Data Standards, Data Integrity and Security Guidelines.
6. Data security is a shared concern and responsibility throughout the College. Users share responsibility and are accountable for their use and access of data and shall be aware of the restrictions, regulations and other usage provisions that apply to the data they handle and shall participate in education as necessary to appropriate use and care of data.
7. IT will document the security of all digital data assets.
8. Security access audit and assessment will be carried out on a scheduled basis to ensure compliance.
9. VCC will perform audit on a regular basis to ensure compliance and risk assessment.
10. The College will comply with BC Privacy Legislation.

DEFINITIONS

College Data: Information that is collected, maintained and utilized by the College for the purpose of carrying out institutional business.

College data will fall into one of three classifications:

a. Public data – All data intended for public use and poses no risk to the College. An example would be a listing of courses offered by the College and the rooms in which they are taught.
b. Protected data – All data which, if released, altered or destructed in an uncontrolled fashion, could cause moderate risk to the College or its affiliates. By default, the data that is not classified as public or restricted is considered as protected data.
c. Confidential data – All data which, if released, altered or destructed could cause significant risk to the College or its affiliates. Examples include personal data containing elements such as Social Insurance Numbers, health/disability related records, student grades and personnel records.

College Data Resource: The mechanism by which all data owned and/or managed on behalf of the College is accessed.

Data Custodian: The College designate responsible for providing secure access to protected and confidential data including, but not limited to: providing physical security; backup and recovery processes; providing access to users as authorized by the Data Stewards; and implementing and administering appropriate levels of control over the information. This can also include individuals in physical possession of data for the College. This role owns the technical accountability of data assets.

Data Standards, Data Integrity and Security Guidelines: An institutional set of data standards and security guidelines by which data integrity and security is maintained. This document is reviewed on a regular basis, is accessible by the College community and the oversight group will provide an annual report to Operations Council, or delegate.

Data Steward: College official or designate having direct operational-level responsibility for information management. Data Stewards are responsible for data access model and policy implementation. This role owns the business accountability of data assets.

Data User: Individuals who need and use College data as part of their assigned duties or in fulfillment of assigned roles or functions within the College community. Individuals who are given access to sensitive data have a position of special trust and as such are responsible for protecting the security and integrity of that data. Any College employee with access to College data can be considered a Data User.

Least Privilege Protocol: The extent of access privileges for Data Users is defined and implemented according to the role and job function of the Data User's position/job description rather than on an individual basis. If a Data User changes positions or job function, e.g. through promotion, transfer, separation, etc., that individual's privileges will be eliminated or changed according to the new position.

Shared Resource: A shared resource is generally something like address information. The information itself is not owned by a specific department of the College as a staff member could also be a student or a donor. As such, those specific data elements are shared between the different functional areas.

RELATED LEGISLATION & POLICIES

Legislation:

Freedom of Information and Protection of Privacy Act
General Data Protection Regulation

Policies:

A.3.3 Freedom of Information and Protection of Privacy (FOIPPA)
A.3.6 Standards of Employee Conduct & Conflict of Interest
A.3.9 Records Management
A.3.11 Emergency Management
B.5.2 Appropriate and Responsible Use of Education and Information Technology
B.5.4 Electronic Mail (Employees)

RELATED PROCEDURES

Refer to Policy B.5.1 Sharing & Stewardship of Information Procedures.