Table of Contents

1. POLICY STATEMENT ........................................................................................................2
2. DEFINITIONS ..................................................................................................................2
3. RESPONSIBILITIES .........................................................................................................3
4. RESPONSIBLE ADMINISTRATORS ..............................................................................5
5. DISCIPLINARY SANCTIONS ..........................................................................................5
6. RELATED POLICIES AND PROCEDURES ................................................................5
7. HISTORY ..........................................................................................................................6
8. SIGNATURE, TITLE, AND DATE OF APPROVAL .........................................................6
1. POLICY STATEMENT

Westminster College maintains data essential and valuable to the performance of College business. These data resources are regulated by federal and state law, as well as College policies, that identify types of data and restrictions placed on data. This policy incorporates federal and state standards, regulations, and legislation, and establishes responsibilities for all forms of College data for confidentiality, integrity, regulatory compliance, and availability.

While data are critical to College operations and must be shared, it must also be used with care. The benefit of sharing data is greatly diminished through misuse, misinterpretation or unnecessary restrictions on access. Although some portion of the College data is public information, some data are restricted by federal or state legislation or by College policy. To comply with legislation and protect its community, the College has the right and obligation to protect, manage, secure, and control data under its purview.

2. DEFINITIONS

A. Confidential/Sensitive Information: Data that must be protected as prescribed by contract and/or legal specifications or by federal and state laws (e.g., individual financial records, social security numbers, student educational records, and credit card information).

B. Data Administrators: Individuals responsible for documenting and enabling user access to a subset of data.

C. Data Custodian: Faculty, adjunct faculty, staff, and student employees of the College with responsibility over information and data resources in their respective areas of responsibility.

D. Data Owner: College faculty and staff with the responsibility to manage a subset of data (e.g., employee, student, financial, departmental, and research data, etc.).

E. Data Processors: Individuals that are authorized by data custodians to enter, modify or delete data.

F. Data Users: Any College employee, contractor, affiliate, or duly authorized member of the community who can access internal use only and/or confidential data but does not have access to modify or delete that data.

G. Internal Use Only Data: Data not generally made available to parties outside of Westminster College (e.g., meeting minutes, memoranda, etc.).
H. **Legitimate Interest**: A need for access to internal use only or confidential data that arises within the scope of College employment and/or in the performance of authorized duties.

I. **Public Use Data**: Data intended for general public use (e.g., directory information).

### 3. RESPONSIBILITIES

A. **General**

Access to College data is provided to data users to conduct College business. Internal use only and confidential/sensitive data, as defined by this policy, will be made available to data users who have legitimate interest. This may include data collected from students, faculty, adjunct faculty, staff, students, contractors, members of the community, or those who have no affiliation with the College. Data users accessing such data must observe the requirements for privacy and confidentiality, comply with the protection and control procedures, and accurately present the data used in any type of reporting. Individuals that have custodianship responsibilities for data access must establish internal controls to ensure that college policies are enforced. All data users are responsible for the security and privacy of the data they access as prescribed by this policy.

B. **Compliance**

1. The College forbids the disclosure of internal use only data or confidential/sensitive data in any medium, including electronic information, hard copy information, and information shared verbally or visually (e.g. telephone or video), except as approved by the data custodians. The use of any internal use only or confidential/sensitive College data for one’s own personal gain or profit, for the personal gain or profit of others or to satisfy personal curiosity is strictly prohibited. Data users are responsible for the consequences resulting from their misuse of College data.

2. Should a security breach occur or the misuse of College data be reported, the Incident Response Team will invoke an incident response process to investigate the facts related to the situation and determine the appropriate response. Disciplinary action will be taken in accordance with applicable regulations or College policy, up to and including termination or expulsion.

3. All individuals accessing College data are required to comply with applicable federal and state laws (e.g. FERPA, HIPAA) and College policies and procedures regarding security of confidential/sensitive data and to exercise discretion with regard to such data. Any data user who engages in unauthorized use, disclosure, alteration, or destruction of such data in violation of this policy will be subject to
appropriate disciplinary action, including possible dismissal/expulsion and/or legal action.

C. Responsibilities: Authorization for access to and the maintenance and protection of all College data, particularly confidential/sensitive data, are delegated to specific individuals within their respective areas of responsibility. In some cases, one individual may serve in more than one role.

1. Data Owners
   a. Establish policies and direction for the security and privacy of all College data and particularly confidential/sensitive data within their respective areas of responsibilities.
   b. Identify and appoint Data Custodians for units within their areas of responsibility.

2. Data Custodians
   a. Grant access to data for legitimate interest as defined in this policy.
   b. Ensure accuracy of all data within their area of responsibility.
   c. Annually review access to all data within their area of responsibility with the appropriate data administrator, and update access of users if necessary.
   d. Ensure that authorized data users understand their responsibilities with regard to their approved access.
   e. Report any possible breach in computer security or misuse of confidential/sensitive data to the Incident Response Team.
   f. Review appeals resulting from decisions to deny access.

3. Data Administrators:
   a. Assign or configure access to College data as prescribed and approved by the data custodian.
   b. Maintain documentation of data users who have been authorized access to confidential/sensitive data. Where an abuse of privileges is discovered, make access removal recommendations to the appropriate data custodian.
   c. Work with the Chief Information Officer (CIO) to identify potential security gaps that may leave systems vulnerable to attacks or hacking and take remedial actions to make systems more secure.
   d. Ensure the usability, reliability, availability and integrity of information systems and the associated data.

4. Data Processor:
   a. Accurately input and present data. Data processors will be held responsible for their intentional misrepresentation of data.
b. Maintain data integrity. Upon recognizing that any data elements are in error, the data processor will notify the appropriate data custodian.

5. Data User:
   a. Use internal use only and confidential/sensitive data only as required to perform the employee’s job responsibilities and as authorized by the appropriate data custodian.
   b. Respect and protect the confidentiality and privacy of individuals whose records to which they have access.
   c. Abide by federal and state laws and College policies and procedures with respect to access, use, and disclosure of confidential/sensitive data.
   d. Report any suspected breach in computer security or misuse of confidential/sensitive or internal use only data to the data owner, data custodian, or Incident Response Team.

4. RESPONSIBLE ADMINISTRATORS

   The CIO is responsible for oversight and administration of this policy with the assistance of the ISPC. At least annually, the CIO will review the effectiveness of the policy and make any needed changes.

5. DISCIPLINARY SANCTIONS

   Violations of this policy may result in sanctions and corrective actions up to and including termination and/or expulsion as set forth in the Staff Corrective Action Policy and Procedures, the Faculty Manual, and the Student Code of Conduct.

6. RELATED POLICIES AND PROCEDURES

   • Computing Resources, Network and Email Use Policy
   • Confidentiality Policy
   • Information Security Program Policy
   • Data Custodianship and Access Policy Appendix A: Procedures
   • Data Custodianship and Access Policy Appendix B: Data Owners and Custodians [maintained by the CIO in consultation with data owners, custodians, and administrators]
7. HISTORY

<table>
<thead>
<tr>
<th>Date of Last Action</th>
<th>Action Taken</th>
<th>Authorizing Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

8. SIGNATURE, TITLE, AND DATE OF APPROVAL

Approved: /s/ __________________________

Bethami Dobkin, President