Interim Confidentiality Policy

WESTMINSTER COLLEGE

Table of Contents

1. STATEMENT OF POLICY..................................................................................................................2
2. TO WHOM THIS POLICY APPLIES..................................................................................................2
3. DEFINITIONS ......................................................................................................................................2
4. POLICY .............................................................................................................................................3
5. TRAINING ..........................................................................................................................................4
6. PROHIBITED CONDUCT ....................................................................................................................4
7. DISCIPLINARY SANCTIONS ..............................................................................................................5
8. RESPONSIBLE ADMINISTRATORS .....................................................................................................5
9. RELATED POLICIES ..........................................................................................................................5
10. HISTORY ...........................................................................................................................................6
11. SIGNATURE, TITLE, AND DATE OF APPROVAL.............................................................................6
1. STATEMENT OF POLICY

Increasingly, confidential information about employees, students and others reside in Westminster College's information and business systems to assist with overall operations. Laws and regulations dealing with information and data privacy and security obligate employers and institutions of higher education to take affirmative steps to safeguard confidential information and deal with the risks of information security and privacy breaches proactively.

The purpose of this policy is to inform all College employees (including student employees), volunteers, and third party contractors of their duty to protect and safeguard all confidential information acquired during the course of employment or service to Westminster College.

2. TO WHOM THIS POLICY APPLIES

This policy applies to all faculty, adjunct faculty, staff, student employees, volunteers, and third party contractors of Westminster College.

3. DEFINITIONS

A. Confidential Information includes, but is not limited to: any personally identifiable information, student and parent records, financial records (including social security and credit card numbers), and health records; contracts; research data; alumni and donor records; personnel records other than an individual's own personnel records; College financial data; computer passwords, College proprietary information/data; and any other information for which access, use, or disclosure is not authorized by: 1) federal, state, or local law; or 2) College policy or operations. Confidential Information includes either hardcopy or electronic information.

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

C. Employee – All faculty, adjunct faculty, staff, and student employees who are employed by the College.

D. Student Employee – Students currently enrolled in six or more credit hours, eligible to work on-campus no more than 20 hours per week while classes are in session.
E. Third Parties – Authorized groups not directly employed by Westminster College that house, transmit or interact with college data and are given access to College-owned data for purposes of assisting the College with its operations, including but not limited to outside data processors, transcript providers, and Cloud based software providers.

F. Volunteers – Individuals working at the College on behalf of others without being motivated by financial or material gain.

4. POLICY

The following principles govern confidentiality at Westminster College:

A. All employees, volunteers, and third parties have a duty to adhere to the College’s Password Policy and to use other available physical, technological, and administrative safeguards to protect the security of all confidential information.

B. Employees and volunteers may access documents and files (both electronic and hardcopy) containing confidential information only on a need-to-know basis for an employee’s job functions or a volunteer's service.

C. Employees and volunteers may transmit confidential information 1) electronically only using a secure, online document sharing application (e.g., File Share), or 2) by courier mail (e.g., Federal Express). Employees and volunteers may not deliver confidential information electronically via an unsecure email application or other unsecure mechanism.

D. Upon conclusion of employment or volunteer service, or upon request of a supervisor, employees and volunteers will return originals and copies of all documents and files (whether electronic or hardcopy) containing confidential information to the College and relinquish all further access to and use of such information.

E. Employees may disclose confidential information to authorized third parties only with explicit authorization of the data owner and only after entering into a written agreement with the third party that has been approved as to form by the College’s general counsel. The agreement must contain the following:

   1. Terms governing the non-disclosure of confidential information;
2. Terms requiring the transmission of confidential information only via secure means, either electronically using a secure, online document sharing application (e.g., File Share), or by courier mail (e.g., Federal Express).
3. Terms requiring the third party to meet industry standards for data security and adhere to the college password policy.
4. Terms requiring the third party to provide either a SAS70 or SSAE16 certification or otherwise demonstrate data security satisfactory to the Chief Information Officer (CIO) if credit cards are involved, the third party must also adhere to Payment Card Industry Data Security Standards.
5. Terms requiring the third party to destroy or return all data at the completion of the business relationship. Data owners are responsible to verify that the third party has adequately returned or destroyed the data.

F. Data owners are responsible to identify all data and the relevant local, federal and international regulations for which they are accountable and work with the CIO to establish appropriate controls and safeguards.

G. Nothing in this policy prohibits employees from discussing the terms and conditions of their employment as authorized by law.

5. TRAINING

All newly hired employees are required to complete training within 60 days of hire to understand their responsibilities under this policy. All employees and volunteers must complete the mandated training on an annual basis or such other schedule as determined necessary or appropriate by the CIO.

6. PROHIBITED CONDUCT

A. Transmitting confidential information in a unsecure manner. This applies to both hardcopy and electronic data. Examples of unsecure digital data transfers are but are not limited to: unencrypted email, unencrypted flash drives and ftp (file transfer protocol).

B. Sharing confidential information to individuals or organizations without prior authorization from the applicable data owner.
C. Sharing confidential information to individuals or organizations without entering into a written agreement approved as to form by the College’s general counsel.

D. Uploading confidential information to systems that do not meet the campus password policy or demonstrate adequate data security standards required by this policy.

E. Accessing confidential information that is not required for the completion of your employment responsibilities and without prior authorization from the applicable data owner.

F. Such other conduct as may be defined by the applicable data owner.

7. 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.

8. RESPONSIBLE ADMINISTRATORS

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

9. RELATED POLICIES

- Information Security Program
- Data Custodian Policy
- Password Policy
- Computing Resources, Network, and Email Use Policy
### 10. 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>
</tbody>
</table>

### 11. SIGNATURE, TITLE, AND DATE OF APPROVAL

Approved: /s/________________________________________
Bethami Dobkin, President