Table of Contents

1. STATEMENT OF POLICY .................................................................................................................. 2
2. TO WHOM THIS POLICY APPLIES ............................................................................................. 2
3. TRAINING ........................................................................................................................................ 2
4. POLICY ........................................................................................................................................... 2
5. DISCIPLINARY SANCTIONS ........................................................................................................... 3
6. RELATED POLICIES ....................................................................................................................... 3
7. HISTORY .......................................................................................................................................... 4
8. SIGNATURE, TITLE, AND DATE OF APPROVAL ........................................................................... 4
1. STATEMENT OF POLICY

Westminster College provides computing and network resources to its students primarily for educational purposes and to its faculty and staff primarily for work purposes. The College may provide access to other users at its discretion. All users are expected to exercise personal and professional responsibility and integrity when using these resources.

2. TO WHOM THIS POLICY APPLIES

This policy applies to all users (“Users”) of College owned or managed computer-related equipment, computer systems, and interconnecting networks, as well as all information contained therein.

3. TRAINING

All Users will be subject to applicable data security training mandated by the College.

4. POLICY

The College enforces necessary restrictions, which may be revised from time to time, to protect its computing and network resources, including the revocation of use privileges for unauthorized or inappropriate use. The Chief Information Officer or designee are authorized to temporarily suspend use privileges in any case deemed appropriate until final resolution of the matter. The College desires to maintain user privacy and to avoid the unnecessary interruption of user activities while also reserving the right to investigate concerns of unauthorized or improper use of College resources, as appropriate.

The campus network, including its servers and associated software, is the property of Westminster College. Except as required for research or instructional activities, neither the network pathways nor College-owned computer systems are to be used:

- for purposes incompatible with established College policies, procedures, protocols or applicable state or local laws;
- in a manner that violates federal laws including intellectual property laws;
- for accessing information that a reasonable person would find offensive and that is incompatible with an educational environment and the mission and values of the College;
- for unauthorized commercial enterprise; or
- for harassing, fraudulent, or threatening purposes.
The following list of activities are nonexclusive examples of those that the College does not permit and that may lead to suspension or revocation of use privileges and other penalties or discipline:

- intentional damage to hardware, software, security devices, or codes, or the creation or distribution of viruses, worms, or other forms of electronic mayhem;
- unauthorized access, attempts to gain unauthorized access, unauthorized disclosure of confidential information, or violation of the College's Confidentiality Policy involving the College's computing and network resources;
- misrepresenting or attempting to misrepresent one's identity;
- altering or tampering with the configuration of computers in student labs and other common areas, or installing unauthorized games or other programs on their hard disks or on the shared-files area of the file servers;
- any network activity that impedes the flow of network traffic or significantly diminishes the availability of resources to other users; or
- unauthorized physical or virtual extension or re-configuration of any portion of the campus network by such means as routers (wired or wireless), wireless access points, network wiring, or other methods.

All Users with access to confidential data are reminded of the College's Confidentiality Policy which provides, among other things, that electronic documents and files containing confidential information are to be accessed, used, and disclosed only with explicit authorization and only on a need-to-know basis for either an employee's job functions or as authorized by contract.

### 5. DISCIPLINARY SANCTIONS

Violations of this policy may result in sanctions, 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

- Information Security Program
- Confidentiality Policy
- Password Policy
7. HISTORY

<table>
<thead>
<tr>
<th>Date of Last Action</th>
<th>Action Taken</th>
<th>Authorizing Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 21, 2019</td>
<td>Final Policy Adopted</td>
<td>Policy Governance Committee</td>
</tr>
<tr>
<td>February 11, 2019</td>
<td>Interim Policy Approved</td>
<td>President’s Cabinet</td>
</tr>
</tbody>
</table>

8. SIGNATURE, TITLE, AND DATE OF APPROVAL

Approved: /s/_________________________________________
Bethami Dobkin, President