POLICIES *and* PROCEDURES

Board of Trustees Policy Number: **Date of Adoption/Revision: April 17, 2014**
IT 13.01

SUBJECT	Acceptable Use of Information Technology
AUTHORITY	Information Technology
APPLICABILITY	The policy applies to the Board of Trustees, faculty, staff and students of Bennett College.
PURPOSE	The College operates and maintains many information technology assets, including but not limited to: voice, video, and data systems. These assets are connected by networks and communications systems of many types. The College must act to protect the confidentiality, integrity and availability of information technology assets in accordance with applicable policies, standards and procedures. The College provides information technology resources for use by faculty and staff for College-related duties and responsibilities. The use of information technology resources for personal or other non-College purposes is strictly prohibited.

POLICY	All users of College information technology resources must adhere to applicable state and federal laws, statutes, and regulations; must comply with applicable policies, standards and procedures as defined by the College; must understand and acknowledge that information technology assets and data are for authorized use only; and must not compromise the confidentiality, integrity and availability of these assets and data.
PROCEDURES	**Definitions:** • The College's voice, video, and data systems, as described above, and those systems as defined below, will be referred to generally as "College information technology assets" in this document. • The term "user(s)" refers to any person(s) accessing College information technology assets, including but not limited to: students, faculty, staff, contractors, clients, consultants, invited guests, and others working at or for the College. • The phrase "College information technology assets" includes College owned, operated or maintained: workstations, servers, printers, telephones, switches, routers, wiring and hubs; wireless and cellular components; mobile devices such as smart phones, tablets, laptops and

other portable computing devices; or any College owned, operated or maintained technology, software, components or devices that store, process or transmit information or data.

- Personally owned technology such as mobile devices (e.g., smart phones, tablets, portable computing devices, etc.) or home computers that interface with College information technology assets will be subject to this policy.
- The "College Information Technology Office" is defined as the group assigned to implement College-wide information security strategy and is led by the senior information security person as appointed by the College.
- The term "access credentials" refers to the user identification, logon/login identification, or other system-specific means granted to a user permitting access to College information technology assets or data.
- The term "authentication" is defined as a means to determine whether a user attempting to gain access to College information technology assets by means of particular access credentials is in fact the user those credentials were officially assigned to.
- The term "authorization" is defined as a means to determine whether a user is permitted access to specific College information technology assets.
- The term “consumable software” refers to College-purchased software that provides insignificant business value, as determined by the acquiring department, in terms of overall function relative to the original purchase price of the software; or to software that would cost the College more to track, reclaim, or redistribute than the original purchase price

Procedures:

The College Office of Information Technology will establish and maintain a set of requirements.

- All users are responsible for complying with this policy and established IT standards and procedures. Users are responsible and accountable for all activity initiated or conducted through the use of assigned access credentials. Dissemination of unofficial, unsolicited mass communications via College information technology assets is prohibited. Violation of any portion of this policy may result in immediate loss of access to College information technology assets, initiation of legal action by the College, and/or disciplinary action. Users are responsible for reporting any actual or suspected violation of this policy to the Information Technology Office and designated security contact immediately.
- System administrators or staff assigned the responsibility of maintaining or supporting College information technology systems or assets will be responsible for implementing requirements outlined in this policy and

	established standards and procedures. This includes monitoring vendor and public disclosure forums that report vulnerabilities, incidents, and other information of interest that could affect the confidentiality, integrity, or availability of the system or assets for which they are responsible and disseminating relevant information and/or recommended actions to their users. • All levels of management are responsible for ensuring that all users within their area of accountability are aware of responsibilities as defined in this policy and for ensuring a secure office environment. The head of each unit will authenticate the need for individual access to information technology assets and must request and obtain authorization for access to College data from the appropriate data steward. • Administrative and academic unit heads are responsible for taking the necessary steps to ensure that access to College information technology assets and data is appropriately limited or restricted for employees who transfer to another department within the College or are no longer employed by the College. • Consumable software shall not be tracked, reclaimed or redistributed, unless otherwise directed by an appropriate authority.

Replaces policy:

Date