THE TRUSTEES OF TRINITY COLLEGE
POLICY ON THE ACCEPTABLE USE OF TECHNOLOGY RESOURCES

Trinity College Policy No. 11.3

Policy Statement

Trinity College technology resources and the data contained in those resources are made available to college employees, students, and affiliates, for college-related purposes. Access to and use of such resources come with specific expectations and user responsibilities. This policy sets forth the rules and standards for acceptable use of technology resources at Trinity College. This policy and its corresponding rules and standards apply to all college technology resources that are owned or managed by the college, that connect to the college network, that connect to another college technology or service, or that store college data or information. This policy applies to all college faculty, staff, students, contractors, and any other individual permitted to use college technology resources or data.

Definitions

Information Security Program

The Trinity College information security program is a set of coordinated services and activities designed to protect college technology resources and data, and manage the risks associated with the use of technology resources. The program includes the policies, standards, assessments, protocols, controls, and training needed to protect the college's technology resources and data. This policy is one component of the information security program.

Data

"Data" means any data or information, regardless of format – electronic or printed – or location, that is created, acquired, processed, transmitted, or stored on behalf of Trinity College. Data includes the data processed or stored by the college in hosted environments even if the college does not own or operate the technology infrastructure.

Technology Resources

"Technology resources" means:

- any computer or electronic resources that are used in the search, access, acquisition, transmission, storage, retrieval, or dissemination of college data;
- any technologies or services that are owned or managed by the college that connect to the college network, connect to another college technology or service, or store college data or information; and
- any services or applications used by the college in hosted environments even if the college does not own or operate the technology infrastructure.

Acceptable Use of Technology Resources

College technology resources are owned by the college and designated for college-related purposes. Technology resources must be used in a manner consistent with the college's academic mission. The use of technology resources at the college is a privilege and not a right. Members of

the college community are expected to be good stewards of the college's technology resources and data, and to use them in a manner that is safe, responsible, ethical, and legal. The privilege to continue using college technology resources is contingent upon their being used appropriately and responsibly.

Acceptable Use Practices

All users of college technology resources must abide by the following standards of behavior regarding technology resources and data use:

1. Users must comply with all federal, State of Connecticut, and other applicable laws, regulations, and contracts, including college or third-party copyright, patents, trademarks, and software license agreements.
2. Users must comply with all Trinity College policies, standards, procedures, guidelines, and codes of conduct regarding electronic communications, protection and privacy of college technology resources and data, and the operation and use of technology resources and data.
3. Users may only use those technology resources and data that they have been authorized to use, and use them only to the extent authorized and in a manner that is consistent with the mission and values of the college.
4. Users may only store college data on technology resources, devices, and cloud services provided by the college unless otherwise approved by the Associate Vice President and Chief Technology Officer.
5. Users are prohibited from automatically forwarding college mail (i.e., from trincoll.edu) to an outside third-party mail system (e.g., Gmail, Hotmail, Yahoo, etc.).
6. Users may not use technology resources, including but not limited to, official college email lists or listservs, to send messages that violate applicable laws or other college policies, standards, procedures, guidelines, and codes of conduct; or to engage in political activity, campaign for or against a ballot initiative or candidate running for office, or conduct a political campaign, or any other activity that constitutes a violation of the Trinity College Policy on Political Campaign Contributions.
7. Users must refrain from using technology resources in a manner that creates the appearance that the college is endorsing, affiliated with, or otherwise supporting any organization, product, service, candidate, or position.
8. Users may send mass communications using technology resources, only with the permission of college personnel with authority to grant such permission, and provided the communications relate to an official college business, activity, or event.
9. Users may not use technology resources for personal commercial purposes or personal financial or other gain, except as permitted by the Trinity College Conflict of Interest Policy.

10. Users must refrain from disproportionate uses of technology resources that have the likelihood of consuming an unreasonable amount of resources, disrupting the intended use of these resources, or impinging on the access of others.
11. Users may not interfere with the intended use or proper functioning of technology resources, or gain or seek to gain unauthorized access to any technology resources or data contained on college technology resources.
12. Users may not circumvent, bypass, or impede security measures, requirements, or any standard protocols in place to ensure the confidentiality, integrity, and availability of college technology resources, data, information technology systems, and networks.
13. Users must promptly report actual or potential information security incidents to security@trincoll.edu.

Incidental Personal Use

Incidental and non-recurring personal use of technology resources is permissible, provided such use does not:

- unreasonably interfere with the use of technology resources by other users, or with the college's operation of technology resources;
- interfere with the user's employment or other obligations to the college;
- circumvent any measures put into place by the college Information Security Program;
- violate any applicable law or regulation; or
- violate this or other applicable college policies, standards, procedures, guidelines, or codes of conduct.

Personally Owned Devices Used for College Business

Any personally-owned devices used for college business are subject to this policy and must comply with all college policies, standards, procedures and guidelines governing the type of device and the type of data involved. Personally-owned devices must also comply with any additional security requirements specific to the particular college functions for which they are used. Users have no expectation of privacy regarding any college data residing on personally-owned devices, regardless of the reasons the data was placed on the personal device.

No Expectation of Privacy

The normal operation and maintenance of the college's technology resources require backup and caching of data and communications, the logging of activity, automatic monitoring of general usage patterns, and other such activities. College personnel may, with or without further notice to users, take any action deemed necessary to preserve, protect and promote the interests of the college, its technology resources, or college data. The college may access and monitor its technology resources for any purpose consistent with the college's duties or mission without notice.

Representations and Warranties

Trinity College makes no warranties of any kind, whether expressed or implied, concerning the technology resources that it provides. The college is not responsible for damages resulting from the use of technology resources, including but not limited to loss of data resulting from delays, non-deliveries, missed deliveries, service interruptions caused by the negligence of a college employee, or by any user's error or omission. The college specifically denies any responsibility for the accuracy or quality of information obtained through technology resources, except material that is presented as an official record of the college.

Responsibilities

The roles and responsibilities for the administration of this policy include:

President

The President of the college has general responsibility and control of all of the business and affairs of the college. The President and President's Cabinet are accountable for providing executive oversight and support of the college information security program and for compliance with campus information technology policies and standards.

Vice President for Library and Information Technology Services

The Vice President for Library and Information Technology Services is responsible for overseeing the implementation and enforcement of the college's information security program and for providing guidance to Trinity College leadership concerning the appropriate use of information resources.

Associate Vice President and Chief Technology Officer

The Associate Vice President and Chief Technology Officer is responsible for administering this policy and monitoring the effectiveness of the college information security program. This includes education and awareness for all Vice Presidents, Deans, Department Heads, and Supervisors.

Vice Presidents, Deans, Department Heads, and Supervisors

Vice Presidents, Deans, Department Heads, and Supervisors are responsible for ensuring that units, staff, and end-users receive appropriate information security training and adhere to the standards of behavior outlined in this policy.

End-Users

All end-users of college technology resources, including students, faculty, and staff, are responsible for the appropriate use of technology resources and data as described in this policy.

Compliance

Violations of this policy or any law related to the use of college technology resources or college data, including, but not limited to the Family Educational Rights and Privacy Act of 1974 (FERPA), and the Gramm-Leach-Bliley Act (GLBA), may result in disciplinary action in accordance with the Student Handbook, Faculty Manual, Employee Handbook, as appropriate, and/or any other applicable rules or policies governing employment at Trinity College.

Cross References to Related Policies
Trinity College Policy of Information Security

Trinity College Policy on Political Campaigning Contributions

Trinity College Conflict of Interest Policy

Trinity College Policy on Flexible Work Arrangements

Responsible Officer
Vice President for Library and Information Technology Services or a designee appointed by the President

Key Offices to Contact Regarding the Policy and Its Implementation
Questions or clarifications regarding this policy and actual or suspected information security incidents should be reported to: security@trincoll.edu.

Links to Procedures or Forms
Information technology policies, standards, procedures, and guidelines can be found at https://www.trincoll.edu/lits/help-support/.

The effective date of this policy is: March17. 2022