Concordia Seminary
ST. LOUIS

Acceptable Use Policy

1 Introduction

Concordia Seminary, St. Louis (the Seminary) supports the lawful use of information technologies and data (technology assets). Technology assets must be used for their intended purpose in serving the interests of the Seminary's educational, instructional, research, and administrative business while respecting the rights of other technology users and the integrity of the workplace.

The Seminary community includes faculty, adjunct faculty, staff, students, senior leadership, members of the Board of Regents, vendors, consultants, contractors, outside agencies and other external groups with which the Seminary has relationships.

If an individual is in violation of this Acceptable Use Policy, the Seminary may take one or more of the following actions:

- Restriction of and possible loss of access or privileges Disciplinary action
- Termination of employment
- Termination of contract or other business agreement Expulsion from the Seminary
- Requirement to repay costs incurred by the Seminary
- Referral to law enforcement for legal action

2 Policy

The Seminary requires users to adhere to this Acceptable Use Policy.

Users of technology assets have access to valuable Seminary resources and legally controlled and Confidential Information.

Technology assets issued by the Seminary remain the property of the Seminary. Members of the Seminary community are individually responsible for appropriate use of all resources assigned to them. Members of the Seminary community must have a valid business or educational need and authorization to access Seminary technology assets.

Data created and/or stored on Seminary assets remains the property of the Seminary unless a policy exception applies. Users should have no expectation of privacy when using Seminary systems unless otherwise required by Seminary policy or applicable law. The Seminary reserves the right to monitor all activity for security purposes.

2.1 Scope

This policy applies to all users and technology assets owned, provisioned, entrusted to, or managed by the Seminary. It includes but is not limited to computer equipment, hardware, storage media, software, business applications, data files, business licenses, operating systems, networks, as well as use of services such as internet, voice communication, computer accounts, electronic mail, collaboration tools, and data in use or entrusted to the Seminary or any portion or subsidiary. It also extends to:

- The use of personally owned devices for Seminary business
- The use of Seminary owned devices for personal business

2.2 Purpose

The use of the Seminary technology assets by members of the Seminary community is expected to be ethical, comply with all laws and Seminary policies, and be used for the purpose of achieving the Seminary mission. Members of the Seminary community must refrain from activity known to put the well-being of the Seminary and its members at risk.

2.3 Roles and Responsibilities

All users are responsible for knowing and complying with Seminary policies that apply to appropriate use of its technologies and resources to include this Acceptable Use Policy (see the Employee Handbook, Student Handbook, Faculty Handbook or other agreements in place).
Members of the Seminary community are required to use assets lawfully and are individually responsible for knowing the law.

3 Procedure

3.1 Acceptable Use

This section of the policy identifies the acceptable use of technology assets at the Seminary to protect the user and the Seminary community.

In making acceptable use of resources, individuals covered by this policy must:

- **Use resources for authorized purposes** and adhere to local, state, federal, and international laws governing the use of technology assets issued by the Seminary.
- **Protect user credentials and systems from unauthorized use**. Each individual is responsible for all access to Seminary technology assets by their credentials and/or any activity originating from their system.
- **Access only the information to which you have been authorized** or that is publicly available using the appropriate account.
- **Protect Confidential Information**. Examples of Confidential Information include but are not limited

to personally identifiable information (PII), FERPA protected student data, financial aid data, bank account information, payment card data and other data such as intellectual property, confidential, and competition-sensitive information.

- **Protect data** that resides on or is transmitted to and from Seminary systems in all forms to include but not limited to electronic data and hardcopy data.
- **Use only legal versions of copyrighted software** in compliance with vendor license requirements and comply with third-party agreements.
- **Report immediately any suspicious or unusual activity**, unexplained service interruption or degradation, suspected theft, loss, or compromise of technology assets to your supervisor or Seminary point of contact.
- **Limit personal use of Seminary technology** assets to incidental, intermittent and minor use that is consistent with applicable law and Seminary policy. Personal use must never put the Seminary at risk and must not interfere with Seminary business or productivity. The Seminary is not responsible for the confidentiality, integrity, or availability of personal content on Seminary-issued assets. Examples include but are not limited to personal files, pictures, videos, sound files, personal software or software licenses, personal emails, eBooks, user credentials that access personal accounts, and other personal electronic files residing on a Seminary-issued asset.
- **Return Seminary assets when separating from the Seminary.**

3.2 Prohibited Use

In making acceptable use of resources, individuals covered by this policy **must not:**

- **Use technology assets unlawfully** or in violation of Seminary policy.
- **Install unauthorized software or hardware** on a Seminary-issued asset.
- **Allow an unauthorized individual access** to use Seminary technology assets (individuals who do not have a user account, or business relationship with the Seminary).
- **Leave your device unsecured** (fail to lock screen, logging out of the system or positioning screen away from public view when accessing Confidential Information).
- **Access, process or store Confidential Information if not authorized.**
- **Fail to provide reasonable physical protection** to Seminary-issued assets to avoid theft (ways of preventing theft include storing assets out of view, locking them up, and keeping them on your person).
- **Attempt to circumvent security controls.** Change or remove any computer settings, software or controls that provide confidentiality, integrity or availability to data or systems such as antivirus software, group/active directory policies, system folder permissions, user permissions, screen lock settings, audit settings, system services.
- **Deliberately introduce unauthorized software** to a Seminary-issued asset such as malware, hacking/cracking tools, anti-forensic or network tunnelling software especially through the use of a personal (non-Seminary issued) email account (be cautious when accessing these email accounts from a Seminary-issued device).
- **Share Seminary-issued passwords.**
- Physically connect a wired network connection of a personally owned devices to any Seminary network receptacle. **Personal devices (when on campus) are only permitted on the Seminary's publicly advertised WiFi**.
- Disclose confidential Seminary information to an unauthorized entity or person.
- Attempt to gain unauthorized access to any Seminary information system.

- Use of a Seminary technology asset that conflicts with the Employee, Faculty or Student Handbook or Seminary policy (including but not restricted to abusive, harassing, defamatory, profane, racist, or illegal behavior).

3.3 Use of Personally-Owned Computing Devices for Seminary purposes

Users are required to adhere to local, state, federal and international laws governing the use of personally owned devices while on Seminary property or while conducting Seminary business regardless of location.

Seminary staff who have been authorized to access Confidential Information using their personally owned device must use reasonable security controls, including requiring authentication to access the device (PIN, password, biometric, encryption).

Users who are not authorized to use personal devices to access Confidential Information **must not:**

- Access, store, or record any Seminary information on personal devices. Privacy data, payment card and bank account information, health data, and student data are examples of data regulated by law.
- Use personally owned devices of any kind to take pictures or record video in private areas of the Seminary (including private offices, gym, locker room, bathrooms, and any other area of the Seminary where a reasonable expectation of privacy exists).