1. Introduction

Louisville Presbyterian Theological Seminary provides access to computers and other information technology resources for members of its faculty, administration, staff, and students. Information technology resources are valuable assets to be used and managed responsibly to ensure their integrity, confidentiality, and availability for appropriate research, education, outreach and administrative objectives of the institution. Community members are granted use of these resources in support of accomplishing the Seminary's Mission, Vision, and Core Values.

All users of information technology resources, whether or not affiliated with the Seminary, are responsible for their appropriate use, and by their use, agree to comply with all applicable Seminary policies; federal, state, and local laws; and contractual obligations. These include but are not limited to information security, data privacy, commercial use, and those that prohibit harassment, theft, copyright and licensing infringement, and unlawful intrusion and unethical conduct.

Louisville Presbyterian Theological Seminary accepts no responsibility or liability for any personal or unauthorized use of its resources by users.

2. Definitions and Scope of the Policy

Users refer to those authorized to use the institution's information technology resources, including members of the Seminary's faculty, administration, staff, and students, and others who may or may not be affiliated with the school.

Louisville Presbyterian Theological Seminary's ***Information Technology Resources,*** referred to hereafter as "IT resources", include but are not limited to desktop and portable computer systems, fax machines and scanners, internet, intranet and extranet access (including WWW browsing and FTP), email and instant messenger, video conferencing equipment, such as the OWL or similar devices, Zoom, telephone, and voice mail, smart phones, tablets, cellular phones, and other similar mobile devices, TheraNest and/or successor vendors, LMS system, SIS system, operating systems such as Microsoft and software, and storage media.

This policy applies to all IT resources that are owned or leased by the Seminary and used to access Seminary networks or cloud-based technology services. Additionally, this policy applies to all activities using any organization-based accounts, subscriptions, or other IT services, such as Internet access, voice mail, and email, whether or not the activities are conducted on the Seminary's premises.

3. Acceptable Use

The Acceptable Use of Information Technology Resources Policy establishes the minimum standards and includes, but is not limited to, respecting the rights of other users, avoiding actions that jeopardize the integrity and security of information technology resources, and complying with all pertinent licensing and legal requirements. Users with access to Louisville Seminary's information technology resources must agree to and accept the following:

- Only use information technology resources they are authorized to use and only in the manner and to the extent authorized. Ability to access information technology resources does not, by itself, imply authorization to do so.
- Only use accounts, passwords, encryptions, and/or authentication credentials that they have been authorized to use for their role at the Seminary.
- Protect their assigned accounts and authentications (e.g., passwords and/or authentication credentials) from unauthorized use.
- Only share data with others as allowed by applicable policies and procedures, and dependent on their assigned role.
- Comply with the security controls on all information technology resources used for seminary business, including but not limited to mobile and computing devices, whether Seminary or personally owned.
- Comply with licensing and contractual agreements related to information technology resources.
- Comply with intellectual property rights (e.g., as reflected in licenses and copyrights).
- Accept responsibility for the content of their personal communications and may be subject to any personal liability resulting from that use.
- Accept responsibility for saving documents or files to appropriate Seminary storage. Louisville Seminary is not responsible for recovering documents lost or damaged on a user's local drive.
- Report the loss or theft of any Information Technology Resource to the Dean's Office (dmumford@lpts.edu), RFX (Support@RFXTechnologies.com), and the Business Office (atraylor@lpts.edu).

4. Unacceptable Use

The Acceptable Use of Information Technology Resources Policy also includes what the Seminary considers as unacceptable use of these same resources.

Unacceptable use includes and is not limited to the following list.

Users are not permitted to

- Share authentication details or provide access to their seminary accounts with anyone else (e.g., sharing user names and passwords), except with the systems administrator (RFX) in order to solve a problem in seminary or seminary-paid software.
- Circumvent, attempt to circumvent, or assist another in circumventing the security controls in place to protect information technology resources and data.
- Knowingly download or install software onto seminary's information technology resources, or use software applications which do not meet the seminary's security requirements, or may interfere or disrupt service, or do not have a clear business or academic use.
- Engage in activities that interfere with or disrupt users, equipment, or service; intentionally distribute viruses or other malicious code; or install software, applications, or hardware that permits unauthorized access to technology resources.
- Access information technology resources for which authorization may be erroneous or inadvertent.
- Conduct unauthorized scanning of information technology resources.
- Engage in inappropriate use, including but not limited to: activities that violate state or federal law, regulations, or Seminary policies; or widespread dissemination of unsolicited and unauthorized electronic communication.
- Engage in use that is harassing, offensive, defamatory, insulting, discriminatory, pornographic or obscene.
- Violate any Seminary policies or rules.
- Engage in excessive use of system information technology, including but not limited to network capacity. Excessive use means use that is disproportionate to other users, or is unrelated to academic or employment-related needs, or that interferes with other authorized uses. Seminary administration may require users to limit or refrain from certain activities in accordance with this provision.

Users of Information Technology Resources are responsible for the content of their individual communications and may be subject to personal liability resulting from that use. The Seminary accepts no responsibility or liability for any individual or unauthorized use of Information Technology Resources by users.

Access to Information Technology Resources is a privilege and continued access is contingent upon compliance with this and other Seminary policies.

5. Privacy and Security Measures

Users must not violate the privacy of other users. Technical ability to access others' accounts does not, by itself, imply authorization to do so.

Users play an important role in the protection of their personal information. All faculty, staff, administrators, and students are required to use all available user security controls provided by the Seminary and meet the user specific controls identified in departmental/administrative policy in order to assist in the protection of assets and the protection of their personal information and assets. Failure on the part of community members to employ in good faith the available security controls and to secure their personal information appropriately will mean that the Seminary will not reimburse the community member (user) for the loss of misdirected salary, expense reimbursements, financial aid, or any other assets.

Employees must understand that any records and communications they create related to Seminary business, electronic or otherwise, on an assigned or personally owned device, may be subject to disclosure under certain state laws.

The Seminary takes reasonable measures to protect the privacy of its information technology resources and accounts assigned to individuals. However, the Seminary does not guarantee absolute security and privacy. Users should be aware that any activity on information technology resources may be monitored, logged and reviewed by Seminary-approved personnel or may be discovered in legal proceedings. The Seminary assigns responsibility for protecting its resources and data to technical staff (RFX), data owners, and data custodians, who treat the contents of individual assigned accounts and personal communications as private and do not examine or disclose the content except:

- as required for system maintenance, including security measures;
- when there exists reason to believe that an individual is violating the law or Seminary policy; and/or
- as permitted by applicable policy or law.

The Seminary reserves the right to employ security measures. When it becomes aware of violations, either through routine maintenance or from a complaint, it is the Seminary's responsibility to investigate as needed, or directed, and to take necessary actions to protect its resources and/or to provide information relevant to an investigation.

6. Enforcement

Individuals who use information technology resources that violate a Seminary policy, law(s), regulations, contractual/licensing agreements, or violate an individual's rights, may be subject to limitation or termination of user privileges and appropriate

disciplinary action, legal action, or both. Alleged violations will be referred to the appropriate office or law enforcement agency.

The Seminary may temporarily deny access to information technology resources if it appears necessary to protect the integrity, security, or continued operation of these resources or to protect itself from liability.

Individuals or departments should report non-compliance with this policy to the appropriate senior administrator in the institution.

7. Exceptions

Departments and programs within the Seminary may define additional conditions of use for information technology resources or facilities under their control. Such additional conditions must be consistent with or at least as restrictive as any governing Board or Administrative policy, including this Acceptable Use Policy, and may contain additional details and guidelines.

8. Additional Guidelines:

Louisville Presbyterian Theological Seminary
Campus Email Information and Policies

Email is an official form of communication at LPTS. All students and employees are given a Seminary email address through Microsoft Outlook. Students and employees are expected to check emails regularly for official seminary announcements and notices.

CAMPUS EMAILS: Addresses generally follow the format below, though there are exceptions.

- **Student email addresses:** firstname.lastname@lpts.edu
  (example: jane.doe@lpts.edu)
- **Employee email addresses:** firstinitiallastname@lpts.edu
  (example: jdoe@lpts.edu)

GROUP LISTS: For convenience in disseminating information to certain groups on campus, there are the following group email lists that can be utilized:

- **EMPLOYEES - ALL** (employeesX@lpts.edu): This includes all paid employees (administrators, employees, faculty, and staff)
- **FACULTY - ALL** (facultyX@lpts.edu): This includes all faculty.
- **STUDENTS - ALL** (studentsX@lpts.edu): This includes all currently enrolled students.

Please use these lists to communicate matters pertaining to Seminary business, course information, special lectures, general campus announcements, events, opportunities, and requests.

OTHER IMPORTANT LPTS EMAIL GROUPS/EMAILS:

- **RESERVES** (library@lpts.edu): To email all library employees. Can also be used to reserve library books.
- **Tech Support** (support@rfxtechnologies.com): To send LPTS-related computer or technology issues or requests.
- **Seminary Times** (seminarytimes@lpts.edu): To advise the communication department of articles, events, and general info to be included in the Seminary Times weekly publication.
- **Facilities Workorder** (facilitiesworkorder@lpts.edu): To submit on-campus work orders.

General E-mail Etiquette
- Respond to emails in a timely fashion.
- Be respectful of professional boundaries. Employees are not expected to check emails during non-business hours.
- Set up an out of office notice during periods of vacation or other absence.
- "Reply all" only when requested or necessary.

For questions, please contact Kassandra Turpin, Communications Director, at 239-728-8836 or kturpin@lpts.edu.

9. References:

Association of Theological Schools Standards of Accreditation (2020), Standards 3.14 and 7.

Commission on Accreditation for Marriage and Family Therapy Education Accreditation Standards, Version 12.0 (2017), Standard III: Infrastructure and Environmental Supports, Key Element III-B: Technological Resources.

SACSCOC Principles of Accreditation (2017), Standards 10.6(b) and 12.5.

Final review and approval by the President and the Senior Administrators
August 17, 2022