Information Technology Acceptable Use and Privacy Policy

A. Purpose/Policy Statement

1. This Acceptable Use and Privacy Policy outlines the standards for acceptable use of La Salle University's computing and information technology resources ("IT Resources").

B. Definitions.

1. **IT Resources:** for purposes of this Policy, "IT Resources" include, but are not limited to, all information technology-related hardware, software, services, and data, whether owned, leased, or otherwise provided by the University, whether accessed from on-campus or remote locations, and whether accessed from University-owned or privately-owned computers, smartphones, or other devices. "Information Technology-Related Hardware" includes desktop and laptop PCs, mobile and stationary communication devices, servers, systems, networks and computer peripherals such as printers and scanners. "Information Technology-Related Services" include Internet services, email, telephone, and online databases accessed through La Salle's network.

2. **Users:** the term "Users" includes, but is not limited to: University faculty, staff, students, guests, and external individuals or organizations, whether affiliated with La Salle or not.

C. Policy Procedures/Guidelines.

1. User Understanding and Consent
   a. User Understanding Regarding No Expectation of Privacy

      The University's IT Resources are the private property of La Salle, and all Users are expressly on notice that use of the University's IT Resources *IS NOT* private or confidential.

      LA SALLE EXPRESSLY CAUTIONS THAT NO USER OF THE UNIVERSITY'S IT RESOURCES SHOULD HAVE ANY EXPECTATION OF PRIVACY WHILE USING THE UNIVERSITY'S IT RESOURCES.

      La Salle is required to obey applicable international, federal, state, and local laws; ensure that the University's mission and objectives are being upheld; protect the rights of all Users; and protect the property and operations of the University. Therefore, La Salle expressly reserves the right to review, access, copy or view any programs, files, communication, software, or other information located on or stored within the University's IT Resources, including individual login sessions and communications, without notice, unless expressly prohibited by law. Such an examination might be necessary to, among other things: comply with legal or regulatory requirements; maintain or improve functioning of technology resources; investigate potential violations of University policies/rules/regulations or federal or state laws; or if otherwise necessary to carry on the University's necessary priorities or operations. With the exception of access incidental to service requests initiated by users, access required for compliance with law enforcement requests, and access needed to respond to cybersecurity incidents or other emergency situations, the Chief Information Officer, General Counsel, and the individual's area vice president, must approve any individual inspection in advance. Upon discovery of evidence of criminal activity or serious violations of this or any other University policy, the University's General Counsel will be immediately notified as well as the appropriate reporting head. La Salle, in its discretion, may use or disclose the results of any such inspection, including the contents and records of individual communications, as it considers appropriate to University personnel,

third parties such as forensic specialists investigating cybersecurity incidents, or law enforcement agencies.

Accordingly, all Users are on notice that any information stored on or transmitted through the University's IT Resources may be accessed, copied, and viewed by La Salle without further notice. Furthermore, the normal operation and maintenance of the University's IT Resources requires backup and caching of data and communications, logging of activity, monitoring of general use patterns, and other such activities that are necessary to provide service.

All data and information stored and maintained on the University's IT Resources should comply with policies, rules, and regulations set by the University. The University assumes no responsibility for the loss or recovery of personal files. Any data stored on La Salle's IT Resources lab computers by unauthorized personnel is subject to deletion without prior notice.

b. Assumption of Risk

La Salle University provides IT Resources on an "as-is" basis without warranting any aspect of Information Technology-related Hardware or Information Technology-Related Services. Therefore, Users are on notice that they access and use University IT Resources at their own risk.

Users connecting personally-owned computers and devices to University IT Resources are on notice that by establishing such connections, they assume any and all risks and costs resulting from loss or damage, including but not limited to the possibility of compromise due to malware.

c. Scanning and Network Security

La Salle University reserves the right to conduct regular security scans and other assessments to check for vulnerabilities, Trojan software, system compromises, and other risk factors which could be exploited by Users or external attackers. All computers and networkable devices connected to the La Salle University computer network will also be subjected to initial and periodic security scans. Any systems found to be insecure or otherwise vulnerable to compromise may be refused access to or be disconnected from the campus network or have campus network access restricted until such time as the User takes the necessary steps to secure their system.

La Salle reserves the right to block or restrict access to websites and Internet addresses, including but not limited to: sites that consume excessive network bandwidth; feature criminal or illegal content; or that distribute malware, conduct phishing attacks, or otherwise might pose a cybersecurity or other threat to the University. La Salle also reserves the right to immediately disconnect any device that is sending disruptive signals to the University's IT Resources network, whether because of a defective cable, Ethernet card, or other hardware or software problems.

d. User Consent to This Policy

Using La Salle's IT Resources constitutes full agreement and understanding of this Policy, and Users are bound by the most recent version of this Policy. La Salle reserves the right to modify this Policy without permission or consent of its Users.

2. Purpose of This Policy and Concurrent Applicability of Other La Salle Policies

La Salle acquires, develops, and maintains its IT Resources to support the University's instruction, research, and service missions; University administrative functions; student and campus life activities; and the free exchange of ideas among members of the University community and between the University community and the wider local, national, and world communities. In making its IT Resources available to Users, La Salle has a responsibility to protect the University and its students from illegal or damaging actions, intentional or unintentional, committed through the use of the University's IT Resources. All members of the La Salle community are expected to use the

University's IT Resources, in a manner that: is efficient, ethical, professional, legal, academically honest; is in keeping with La Salle University's mission, values and objectives; and shows community awareness in the consumption of shared resources.

This Policy supplements and augments, but does not supersede, other relevant University policies, rules, and regulations. For this reason, all Users of the University's IT Resources must consider La Salle's existing policies, rules, and regulations, as well as this Policy, in judging appropriate uses of University IT Resources.

3. User Responsibilities

The University is subject to numerous international, federal, state, and local laws and regulations – some of which are cited below – that protect the privacy and security of certain types of information stored on La Salle's IT Resources. Users of La Salle's IT Resources are required to act in accordance with all applicable federal, state, and local laws and regulations, as well as with University policies and guidelines. Furthermore, Users have a responsibility not to abuse those IT Resources and to respect the rights of members of the La Salle community as well as the University itself. All Users must respect the privacy of other Users and their accounts, regardless of whether those accounts are securely protected. Users are expected to use only those IT Resources for which they have authorization, and the IT Resources must be used only for their intended purposes. Violations of this Policy include, but are not limited to:

   a. Using IT Resources for any purpose that is illegal, immoral, unethical, dishonest, or likely to subject La Salle to harm. Examples include but are not limited to: (a) terroristic threats; (b) promotion of a pyramid scheme; (c) committing copyright infringement; (d) violation of federal and/or state laws regarding defamation, privacy, copyright, trademark, obscenity, and pornography; (e) violation of the Electronic Communications Privacy Act (18 U.S.C. § 2510, et seq.), which sets out the provisions for access, use, disclosure, interception and privacy protections of electronic communications; and/or (f) violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), which prohibits unauthorized "hacking," "cracking," and similar activities.

   b. Using IT Resources for the unlawful or unauthorized viewing, copying, distribution, disclosure, or other access to sensitive personal information belonging to other persons. "Sensitive personal information" includes, but is not limited to (a) government-issued identification numbers such as Social Security, driver's license, passport, visa, alien registration, or employer identification numbers; (b) financial information such as credit card number, bank or checking account numbers, direct deposit or ABA routing numbers, W-2s, payroll or financial aid history, or public assistance benefits; (c) personal information such as mother's maiden name, prior names, address, telephone, or email addresses; and/or (d) any information controlled or restricted by law or statute such as The Financial Services Modernization Act of 1999, 15 U.S.C. §§ 6801-6809, §§ 6821-6827 (GLBA) or the Pennsylvania Breach of Personal Information Notification Act, 73 P.S. §§ 2301 PA-BPINA).

   c. Using the University's IT Resources to violate one or more provisions of the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232(g) and 34 C.F.R. Part 99 ("FERPA"). FERPA is a federal law protecting the privacy and security of "student education records," which are records, files, documents, and other materials that contain information directly related to a student. Users may not use IT Resources to access, copy, distribute or make other unlawful and unauthorized use of FERPA-protected student education records, examples of which include but are not limited to: academic transcripts, graduation lists, student disciplinary records, student health records, loan disbursements, Free Applications for Federal Student Aid ("FAFSAs"), institutional aid applications, work-study payroll records, records relating to eligibility and disbursement of federal student aid funds and other records created and maintained by the University's financial aid office.

d. Using the University's IT Resources to violate one or more provisions of the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. Parts 160 and 164) ("HIPAA"), which are federal privacy regulations protecting the privacy and security of individually identifiable health information. Users may not use IT Resources to access, copy, distribute or make other unlawful and unauthorized use of HIPAA-protected records, examples of which include but are not limited to medical insurance policy numbers; insurance claims, prescriptions and physician names.

e. Using the University's IT Resources to accept or process credit or bank debit card payments or donations on the University's behalf or to store or transmit credit card PANs (Permanent Account Numbers), magnetic stripe (track data), CVVs/CVCs (the 3 digit number on the signature panel on the reverse of the Discover, MasterCard or Visa payment cards or the 4-digit number on the front of American Express cards), PINs or encrypted PIN blocks. All credit card payment processing on the University's behalf involving IT Resources must be authorized by the Vice President of Finance and Administration, comply with the University's contractual obligations its financial partner institutions, and fully conform to Payment Card Industry Data Security Standards (PCI-DSS). (Purchases or donations made by individual faculty, staff, and students, whether for personal use or related to University activities, are not covered by this requirement.)

f. Using the University's IT Resources to access, copy, distribute or make other unauthorized use of data restricted by University policy or practice, data designated as "official-use only," "non-public" and/or "proprietary," or data entrusted to the University under a reasonable expectation of privacy. Examples of which include but are not limited to student, alumni, employee and donor names, home and campus addresses, phone numbers, email addresses, places of birth and mother's maiden names, and University ID numbers.

g. Using IT University resources to obtain or make unlawful or unauthorized copies of copyrighted material such as music, videos, DVDs, software, textbooks, periodicals and other printed materials, and/or other items protected by Section 106 of the Copyright Act, 17 U.S.C. §§ 101, et seq. or Title II of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. §§ 512, et seq.

   Any copying or distribution of copyrighted materials for research, classroom, or other educational use by faculty, staff, students, or others must fully comply with the restrictions and provisions of the Fair Use Exclusions of 17 U.S.C §§ 101.

h. Unlawfully downloading, copying, or distributing copyrighted materials including peer-to-peer file sharing applications.

i. Using IT Resources to deceive, harass, or stalk an individual, or display, download, post, view, print or send any harassing, obscene, pornographic or offensive material.

j. Using University IT Resources fraudulently (e.g., scams, phishing, spoofing or other misrepresentations).

k. Sending threats, "hoax" messages, "spamming" or other unwanted mail or messages.

l. Intercepting or reviewing without authorization any network communications, or otherwise attempting to defeat network or system security.

m. Creating, distributing, or propagating computer viruses, worms, or other damaging code.

n. Misusing La Salle's IT Resources, networks, applications or software to interfere with University IT Resource services to other Users in any way, or preventing others from accessing authorized IT Resource services (including but not limited to developing or using programs that may cause problems or disrupt services for others).

o. Using or distributing password guessing programs, cracking or hacking tools, packet sniffers, port scanners and monitors, or vulnerability scanners.

p. Using another individual's electronic identity, password or account for IT Resources without appropriate authorization, or misrepresenting a User's identity.

q. Using access to University systems and resources for purposes other than those directly related to job responsibilities or educational purposes. However, University students and employees who have been authorized to use IT Resources may also use such Resources for reasonable personal use to the extent that such reasonable personal use does not interfere with the academic and administrative functions of the University and to the extent that such reasonable personal use otherwise complies with the terms of this Policy. The University expects all students and employees to use sound and responsible judgment and to maintain appropriate standards while using IT Resources.

r. Failing to take best efforts to maintain the security and confidentiality of passwords and other account credentials for IT Resources.

s. Sharing accounts, passwords, and access to the University's IT Resources. (All Users are responsible for their uses of La Salle's IT Resources on and off campus, and for ensuring that their systems are maintained and used so they do not endanger, impede access to, or threaten the privacy or security of others' information or systems.)

t. Making University systems and resources available to any person or organization that is not affiliated with La Salle, with the exception of Guest and eduroam Wi-Fi.

u. Corrupting, misusing, altering, or destroying University information without authorization.

v. Using University IT Resources in a way that violates University contracts, such as software and other licensing agreements.

w. Using La Salle IT Resources for commercial or profit-making enterprises or for personal financial or other gain, including cyber-currency mining and private consulting or professional services practices.

x. Using University IT Resources in a way that suggests University endorsement of any product, service, political candidate or ballot initiative, including use of the La Salle logo or other brand resources without specific authorization from University Marketing and Communication Department.

y. Using La Salle IT Resources to host a web page for any business, including private consulting practices. (Note: non-commercial student web pages are permitted.)

z. Using applications that occupy an unusually large portion of bandwidth for extended periods of time (e.g., misusing mailing lists, propagating chain letters or virus hoaxes, spamming, bombing). Users must respect the finite capacity of the IT Resources and limit use to the extent needed for authorized activities, so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other Users. La Salle may require Users to limit or refrain from specific uses in accordance with this principle. The University will judge the reasonableness of any particular use in the context of all of the relevant circumstances.

aa. Removing or modifying any University-owned or administered equipment or data without authorization.

bb. Installing or operating wireless access points or network server services such as DHCP, DNS, NNTP, POP, SMTP, and WINS.

cc. Installing remote access solutions such as LogMeIn, PCAnywhere, or GoToMyPC on PCs or laptops operating on La Salle's network for the purpose of accessing La Salle IT Resources from off-campus locations.

The foregoing list provides an overview of prohibited uses of University IT Resources without exhaustively detailing all such abuses and misuses. Suspected abuses and misuses of La Salle IT

Resources and alleged violations of any provision of this Policy or other IT Policies or Guidelines will be investigated by the University Chief Information Officer, or his/her designee. Decisions about whether a particular use of IT Resources violates this Policy shall be made in consultation with the Provost's Office if the use involves faculty; by the Office of Student Affairs if the use involves students; and by the Office of Human Resources if the use involves staff. Violating any portion of this Policy is grounds for suspension of access privileges and/or for disciplinary action up to and including termination of employment or expulsion from the University.

Note: The items in the foregoing list that are related intercepting network traffic, the use of tools and utilities employed by hackers, or changes to network configurations, specifically Sections C.3.l, C.3.o, and C.3.bb, do not apply to faculty and to students working under the supervision of faculty in computer labs specifically designated for teaching computer- or cybersecurity-related topics in connection with computer science coursework or to IT staff and third-party cybersecurity auditors and assessors working under the supervision of IT staff.

5. Violations of this Policy or other University Information Technology Policies will be investigated by the University Chief Information Officer, or his/her designee. Decisions about whether a particular use of IT Resources violates this Policy shall be made in consultation with the Provost's Office if the use involves faculty; by the Office of Student Affairs if the use involves students; and by the Office of Human Resources if the use involves staff. Serious or repeated violations of IT Policies are grounds for suspension of access privileges and/or for disciplinary action up to and including termination of employment or expulsion from the University.

6. Annual Policy Review. This Policy will be reviewed by the Chief Information Officer and Executive Director of IT Security and Compliance on an annual basis.

4. Questions About This Policy
   Please direct questions regarding this Policy to:

   Chief Information Officer La Salle University
   1900 West Olney Avenue Philadelphia, PA 19141
   Phone: 215-951-1046
   Email address: cio@lasalle.edu

D. Responsible Office

Information Technology

E. End Notes

Effective date: January 1, 2018