I. Purpose

This policy describes guidelines for the use of the College's technology resources and use of College wide data. Use of College-owned technology resources is a privilege extended by Lansing Community College to students, employees, and other authorized users as a tool to promote the mission of the College and to enhance technological/computer literacy.

II. Scope

This policy applies to all users (employees, students, trustees, alumni, contractors, and guests) of Lansing Community College technology resources and data, including those using the College's network via a personally owned device.

III. General

A. Applicable Statues

Lansing Community College and all users will comply with all federal state and local governing laws. These laws include, but are not limited to:

FERPA – Family Educational Rights and Privacy Act of 1974
FTC Red Flag Rule – Federal Trade Commission Identity Theft Prevention
GLBA – Gramm-Leach-Bliley Act of 1999
HIPAA – Health Insurance Portability and Accountability Act of 1996
ADA – Americans with Disabilities Act of 1990
PCI DSS – Payment Card Industry Data Security Standard
Digital Millennium Copyright ACT (DMCA) of 1998

B. General Usage

The use of Lansing Community College's technology resources, including, but not limited to, computers, fax machines, email, cell phones, printers/copies, audio/visual equipment, software applications and all forms of Internet/intranet access, is for College business and for authorized purposes only.

Employees are permitted brief and occasional personal use of College technology resources if it does not result in expense or harm to the College, interfere with their job responsibilities, or otherwise violate this policy. Appropriate care must be given for technology resources issued to or used by students and employees and returned in the same condition with minimal wear.

No protected data, (SSN, credit card, FERPA, HIPPA), or other confidential information should be stored on non-College systems or any mobile device, and secure communication channels must be used whenever such data is accessed.

Use of the College's resources is a privilege granted by the College and may be revoked at any time for inappropriate conduct carried out on such systems, including, but not limited to:

- Sending chain letters or participating in the creation or transmission of unsolicited commercial email ("spam") that is unrelated to legitimate College purposes;
- Engaging in private or personal business activities, including excessive use of instant messaging or chat rooms, except as allowed by this policy;
- Accessing email messages, networks, servers, drives, folders, or files to which the individual has not been granted access or authorization from someone with the right to make such a grant. It violates College policy for any user, including system administrators and supervisors, to access email and computer systems files to satisfy personal curiosity about the affairs of others, unless such access is directly related to that employee's job duties;
- Email messages received must not be altered without the sender's permission. Users are also prohibited from knowingly falsifying email messages (e.g., by altering and forwarding email to another user without acknowledging the alteration, placing unauthorized or misleading attachments on another's email message, etc.);
- Making unauthorized copies of, or changes to, College files or other College records or data;
- Making unauthorized copies of software or third party files, or otherwise violating software licensing agreements or copyright laws;
- Destroying, deleting, erasing, corrupting or concealing College files or other College data, or otherwise making such files or data unavailable or inaccessible to the College or to other authorized users of College systems, except as provided by the Data Retention and Disposal Schedules;
- Misrepresenting oneself or the College;
- Engaging in unlawful or malicious activities. (e.g., deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the College's networks or systems or those of any other individual or entity, etc.)
- Except as protected by applicable law, using abusive or threatening language or comments in communications; spreading knowingly false and/or malicious information about any other person, the College or any other entity; transmitting sexist, racist or similarly discriminatory remarks or images; or unlawfully harassing, intimidating, or stalking anyone.
- Sending, accessing, viewing, uploading, or downloading pornographic materials;
- Using peer-to-peer applications that violate content copyright;
- Causing congestion, disruption, disablement, alteration, or impairment of College networks or systems;
- Circumventing, attempting to circumvent, defeating, or attempting to defeat any security system, application, and/or procedures, including unauthorized activities or attempts aimed at compromising system or network security, such as hacking, probing, or scanning; attempting to break into another user's accounts or to obtain another user's passwords; sharing Usernames or

passwords with another person or utilization of another person's Username or password;

- Failing to log off any secure, controlled-access computer or other form of data system to which you are assigned, if you leave such computer or system unattended;
- Threatening any person(s) or property**;**
- Employees must not use College technology resources to solicit or provide products or services that are unrelated to the College, or to distract, intimidate, or harass coworkers or third parties, or to disrupt the workplace;
- Except as otherwise permitted by law, employees and others acting for the College are prohibited from using College technology resources to support or oppose a political party, candidate or ballot proposal;
- Accessing and/or utilizing any pay-to-play Internet gambling site;
- Accessing reviewing or transmitting protected or confidential College information for purposes other than completing job duties;
- Installing or connecting servers or wireless access points to the College's network without prior written authorization.
- Employee bulk email auto-forwarding of all received emails to a non-LCC email address without advance approval of the Chief Information Officer or designee.

Violations of this policy may result in loss of computer privileges and/or disciplinary action under the Student Code of Conduct and/or employee disciplinary action up to and including discharge of employment. In addition, the user may face both civil and criminal liability from the College, from law enforcement officials or from individuals whose rights are harmed by the violation.

C. Authorized Monitoring and Access to Technology Resources

The College scans and monitors the content of traffic transmitted over the College's network and data stored on College systems using electronic tools. The sole purpose of monitoring and scanning activity is to reduce risk to the College, to protect the College's technology resources and data, and to enforce this and other College polices and applicable laws.

When responding to Freedom of Information Act requests, internal investigations, or court-ordered documentation requests, the College will search email messaging systems and other electronic storage devices as needed. Therefore, there should be no presumption of privacy or confidentiality when using College technology resources. The College will provide complete or redacted versions of records of business transactions and communications as required. College staff participating in investigations as part of their job duties will endeavor to safeguard the privacy of all parties and will themselves follow the guidelines provided in this policy.

D. Personal Electronic Equipment

Any user connecting a personal computing device, data storage device or image recording device to any College-owned computer or network resources assumes all

risks associated with such connection and accepts responsibility for any damages or loss (to the user, the College or any third party) resulting from such connection.

The College is not responsible for repair or replacement of non-College hardware.

E. Student Computing

College computer labs and devices/equipment for checkout from the Library and Information Technology Services are available on campus for students to complete their course work. Students are expected to follow the rules for any lab or the department which houses the computer they use. Students must possess a current College Starcard to access the computer labs.

Failure to follow this policy will be considered a violation of the Student Code of Conduct and will be reported to the Office of Student Compliance.

F. Indemnification Provision

Lansing Community College makes absolutely no warranties of any kind, either express or implied, for the Internet services it provides. The College will not be responsible for any damages suffered by users, including, but not limited to, any loss of data resulting from delays, non-deliveries, user errors, or service interruptions.

The College is not responsible for the accuracy or quality of information obtained through its Internet services, including email. Users assume responsibility for any damages suffered as a result of information obtained through these sources.

The user agrees to indemnify and hold harmless Lansing Community College, the Board of Trustees, and College employees from and against any claim, lawsuit, cause of action, damage judgment, loss, expense, or liability resulting from any claim, including reasonable attorneys' fees, arising out of or related to the use of the College's hardware, software, and network facilities. This indemnity shall include, without limitation, those claims based on trademark or service mark infringement, trade name infringement, copyright infringement, defamation, unlawful discrimination or harassment, rights of publicity, and invasion of privacy.

IV. Responsibility

Responsibility for the interpretation and administration of this policy is delegated to the Chief Information Office or his/her designee.

Adopted: 3/18/2002
Revised: 12/12/2011, 12/17/2012, 12/15/2014, 12/17/2018, 12/16/2019