I. Purpose

This document describes the policies and guidelines for the use of the College's computer resources and use of College wide data. Use of College-owned computer and network 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 technology users utilizing Lansing Community College resources, including those using the LCC network via a personally owned device.

III. General

A. Glossary

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
ITS – Information Technology Services Division
LCC – Lansing Community College
P2P – Peer to peer file sharing
PCI DSS – Payment Card Industry Data Security Standard
Username – LCC Technology User ID
End User Resources

B. General Usage

The use of Lansing Community College's technology, including computers, fax machines, email, and all forms of Internet/intranet access, is for College business and for authorized purposes only.

Any activity not listed here, which violates local, state or federal laws, is also considered a violation of the Lansing Community College Acceptable Use Policy.

Use of the College's computers, networks, and Internet access is a privilege granted by the College and may be revoked (and disciplinary action taken) 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 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 electronic mail 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.;
- 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 violation 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 Policy;
- 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 electronic data system to which you are assigned, if you leave such computer or system unattended;

- Threatening any person(s) or property.

LCC employees (including student-employees) are subject to several additional standards while using College technology resources and networks:

- Employees are allowed brief and occasional personal use of the electronic mail system or the Internet if it does not result in expense or harm to the College or otherwise violate this policy;
- Employees must not use College computer or network 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 computers or network resources to support or oppose a political party, candidate or ballot proposal;
- Employees are prohibited from accessing and/or utilizing any pay-to-play Internet gambling site;
- Employees are prohibited from accessing reviewing or transmitting protected or confidential College information for purposes other than completing job duties;

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. Ownership and Access of Electronic Mail, Internet Access, and Computer Files; No Expectation of Privacy

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

The College monitors the content of communications (including emails or text messages) transmitted over the LCC Network. The purpose of the monitoring of electronic mail messages (including personal/private/instant messaging systems) and their content, and all use of the Internet and of computer equipment used to create, view, or access email and Internet content, is to reduce risk to the College and to enforce this and other polices of LCC 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. The College will provide complete or redacted

versions of records of business transactions and communications as required. In investigating, LCC staff will endeavor to safeguard the privacy of all parties and will themselves follow the guidelines provided in this policy.

No user may access another user's computer, computer files, or electronic mail messages without prior written authorization from either the user or an appropriate College officer or designee.

D. Electronic Mail

Email is provided to students, employees and Trustees of LCC to support the mission and work of the College. Alumni, retirees and former Trustees are generally allowed to retain their LCC email accounts. Users are responsible for all email sent from their accounts.

Employee and Trustee emails will be archived to comply with applicable policies and laws. The College is not liable for lost or deleted email on College-managed resources.

Electronic mail 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 electronic mail to another user without acknowledging the alteration, placing unauthorized or misleading attachments on another's electronic mail message, etc.).

E. Policy Statement for End User Resources

1. All users of LCC technology resources are required to follow these general computing guidelines.

    a. Account Use

        1. The Division of Information Technology Services (ITS) has final authority to determine unique account names.

        2. Users are responsible for maintaining the security of their assigned LCC accounts and files.

        3. Passwords must not be revealed to others.

        4. Users must secure their accounts by logging off or locking their screen when leaving their device unattended.

        5. Individuals who need to temporarily use the LCC network must be sponsored by a College employee. The sponsor of the

individual is responsible for the sponsored person's actions while using LCC-owned resources and network.

b. Network use

1. Access to the Internet and College network is managed by ITS.

2. Any transmission of data over the LCC Network (email, Internet files, web pages, printer files, etc.) is governed by these guidelines.

c. Assignment of Computer Hardware

1. LCC determines the computer system needs of employees and how those needs will be met. The College retains authority to establish and enforce procedures and rules for employee use of College-owned computer systems, software, and data.

2. College-owned desktop computer equipment cannot be taken home, relocated, or reassigned without prior approval of ITS.

3. Mobile computers are assigned to employees to enable access to College information resources at meetings and remote locations. Mobile computers or devices taken out of the workplace must be protected while offsite.

d. Assignment of Computer Software

1. The College will assign appropriate computer software corresponding to the position held.

2. Some software publishers permit employees to have one copy of their software on the College-owned computer and one copy of their software on an employee-owned computer. If a software publisher permits such an arrangement, the employee is still required to obtain permission from before installing a copy of the software on any computer.

3. Only College-owned software is to be installed on College-owned computers. Any exceptions must be approved by the Chief Information Officer or Director of Technology Support Services in writing prior to installation.

4. The College has licensed the use of certain commercial software application programs for business purposes. Third parties retain the ownership and distribution rights to such software. No

employee may create, use, or distribute copies of such software not in compliance with the license agreements for the software.

e. LCC makes no warranties of any kind whether expressed or implied for the computer services it provides.

F. Policy Statement for Internet/Intranet/Infrastructure

1. The Internet is to be used to further the College's mission and to support other College-related purposes. LCC assumes no responsibility for any direct or indirect damages arising from the user's connection to the Internet. LCC is not responsible for accuracy of information found on the Internet. LCC merely facilitates the accessing and dissemination of information through its systems. Unless LCC expressly authors content, it has no editorial control over the content distributed or disseminated on the Network, and users are solely responsible for any material they access and disseminate. The various modes of Internet/Intranet access are College resources and are provided as tools to users who may use them as appropriate to their position at the College.

2. All servers must be approved by ITS. Administrative or Root access must be given to ITS for all servers on the LCC network.

G. Policy Statement for LCC-owned web sites

LCC will determine what appropriate content for the College's web pages is. Guidelines regarding the Structure and Maintenance of the LCC Website can be found (here). The College is not liable for lost or deleted web pages or the content of web pages residing on non-LCC owned computers.

H. 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.

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

I. Printing/Copying

Printers and copy machines are provided to further the College's mission and to support other College-related purposes. Excessive use or use for personal business is prohibited to all users. Departments may impose printing/copy

limits.

J. Student Computing

1. LCC computer labs are available on campus for LCC 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 LCC Starcard to access the computer labs.

2. Technology accounts are available to currently enrolled students and other individuals approved by ITS.

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.

K. Guests/Alumni/Retirees

Guests/ Alumni/Retirees are required to follow this policy. Failure to follow this policy may result in loss of network access or other actions as appropriate.

L. Applicable Statutes

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, GLBA, HIPAA, PCI DSS, and FTC Red Flag Rule.

1. Family Educational Rights and Privacy Act of 1974

    a. Directory information may be released at the discretion of College officials for any student who has not submitted a completed Request to Prevent Disclosure of Directory Information form to the Office of the Registrar by the end of the first week of the semester. The disclosure prevention form remains in effect until the student provides a written release to the Office of the Registrar.

    b. Lansing Community College prohibits the release of educational records, other than directory information, without the student's written consent or as otherwise provided by the Family Educational Rights and Privacy Act.

    c. Copies of the Request to Prevent Disclosure of Directory Information form and the Family Educational Rights and Privacy Act are available upon request in the Admissions, Registration and Records Department.

2. Higher Education Opportunity Act of 2008 (Public Law 110–315)

    a. Lansing Community College prohibits the use of its systems and equipment for unauthorized downloading and sharing of copyrighted materials such as, but not limited to, software, music, and movies. The College attempts to block the transmission of all known Peer to Peer (P2P) network traffic.

    b. The College will cooperate with authorities to stop illegal activity such as copying and sharing copyrighted material including software, music and movies. A list of legal sites to download copyrighted software, music and movies can be found here.

    c. Lansing Community College students are subject to academic discipline, and civil and criminal penalties and liabilities under this act, for using LCC systems or equipment for illegal downloading or unauthorized distribution of copyrighting material. Penalties and liabilities may include expulsion, large monetary fines, and imprisonment.

M. Indemnification Provision

As a condition and result of using any LCC computing system or computer resources, each user agrees to indemnify and hold Lansing Community College and its officers, Trustees, employees and agents harmless for any claim, action, loss, damage, expense or liability (including attorney's fees) arising out of or related to the user's use of such system or resources. Such claims shall include, without limitation, those based on trademark or service mark infringement, trade name infringement, copyright infringement, dilution, tortuous interference with contract or prospective business advantage, unfair competition, defamation, unlawful discrimination or harassment, rights of publicity, invasion of privacy and all other wrongful conduct.

IV. Responsibility

The College's Chief Information Officer is responsible for preparing procedures to implement this policy. In addition, this policy shall be reviewed every year under the direction of the Chief Information Officer or designee.

Reviewed March 2002, Revised: 12/12/2011, 12/17/2012, 12/15/2014