Lenoir Community College
Computer Acceptable Use Procedures

Section 1. Application

Lenoir Community College's (hereinafter called "College") computing and network resources are intended to support the College's mission and are to be used in a manner consistent with the College's goal to provide quality education to its students. Access to computer systems and networks owned or operated by Lenoir Community College imposes certain responsibilities and obligations and is granted subject to college policies, and local, state, and federal laws. Acceptable use always is ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and to freedom from intimidation and harassment. Users are expected to act responsibly to maintain the integrity of these resources.

Section 2. Requirements

1. Users may not connect personal devices to the College Network without express written permission from the CIO and the users VP/Dean. This requirement does not apply to users who connect to the College Network through the college-supplied "Lancer-Wireless" Wi-Fi network.
2. All devices connected to the College Network must have updated malware/anti-virus protection.
3. Users must not attempt to access any data, documents, email correspondence, and programs contained on systems for which they do not have authorization.
4. Systems administrators and authorized users must not divulge remote connection information or other access points to information technology resources to anyone without proper authorization.
5. Users must not share their account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or other similar information or devices used for identification and authorization purposes.
6. Users must not make unauthorized copies of copyrighted or college-owned software.
7. Users must ensure all files downloaded from an external source to the College Network or any device connected to the College Network, including computers, tablets, cellphones, USB flash drive, external hard drive, DVD, CD or any other electronic medium, is scanned for malicious software such as viruses, Trojan horses, worms or other malicious code.
8. Users must ensure that the transmission or handling of personally identifiable information (PII) or other sensitive data is encrypted or has adequate protection.
9. Users may not download, install or distribute software to college-owned devices unless it has been approved by the CIO and the users VP/Dean.
10. Users must not download College data to personally owned devices, including computers, tablets, cellphones, USB flash drive, external hard drive, DVD, CD or any other electronic medium, unless approved by the CIO and the users VP/Dean.
11. Users must not purposely engage in activity that violates any College policy; that is illegal according to local, state or federal law; or activity that may harass, threaten or abuse others, or intentionally access, create, store or transmit material which may be deemed to be offensive, indecent or obscene.

12. Users accessing the College Network must avoid unnecessary network traffic and interference with other users. Specific prohibitions include, but are not limited to, the following:

    (a) Unsolicited commercial advertising by public employees and College Network users. For the purpose of this policy, "unsolicited commercial advertising" includes any transmission initiated by a vendor, provider, retailer, or manufacturer of goods, products, or services, or by a third party retained by, affiliated with, or related to the vendor, provider, retailer, or manufacturer that describes goods, products, or services. This prohibition does not include the following:

        (i) discussions of a product or service's relative advantages and disadvantages by users of those products or services (unless the user is also the vendor, retailer, or manufacturer, or related to or affiliated with the vendor, provider, retailer, or manufacturer);

        (ii) responses to questions, but only if such responses are direct replies to those who inquired via electronic mail, or

        (iii) mailings to individuals or entities on a mailing list so long as the individual or entity voluntarily placed his/her name on the mailing list.

    (b) Any other type of mass mailing by employees and others accessing the College Network that does not pertain to college business or a college-sponsored activity.

13. Users accessing the College Network must only access Internet-streaming sites as consistent with the mission of the college for the minimum amount of time necessary.
14. Users must not engage in activities that may degrade the performance of information resources, deprive an authorized user access to resources, obtain extra resources beyond those allocated, or circumvent information security measures.
15. Users must not download, install or run security programs or utilities such as password cracking programs, packet sniffers, or port scanners that reveal or exploit weaknesses in the security of information technology resources unless approved in writing by the CIO and the users VP/Dean.
16. Information technology resources must not be used for personal benefit, political activity, unsolicited advertising, unauthorized fund raising, personal business ventures, or for the solicitation of performance of any activity that is prohibited by any local, state or federal law.
17. Users must not engage in any activities that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, damaging files, or making unauthorized modifications to college data.
18. Users must not modify any hardware or software settings in any way that will require technical maintenance unless approved in writing by the CIO and the users VP/Dean.
19. Access to the Internet from college-owned, home based, devices must adhere to all acceptable use policies. Employees must not allow family members or other non-employees to access nonpublic accessible information systems.
20. Users must report any weaknesses in computer security to the CIO for follow-up investigation. Weaknesses in computer security include unexpected software or system behavior, which may indicate an unauthorized disclosure of information or exposure to security threats.

21. Users must report any incidents of possible misuse or violation of the Computer Acceptable Use Procedures.
22. Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of information.
23. Computers at the College are to be used only by current Lenoir Community College students, registered guest, and employees.
24. Users must not allow anyone from outside sources to reconfigure or load software unless approved in writing by the CIO and the users VP/Dean.
25. User must log off or proactively invoke the passwords-protected screen saver when the device is unattended.

Section 3. Security and Confidentiality Statement

College employees handle a variety of personally identifiable information (PII) concerning employees, students, alumni and others associated with the College, as well as confidential information regarding College business.

It is the responsibility of all College employees to respect the highest level of privacy for the members of the College community. Disclosure and discussion of confidential information obtained from College records, either during or after employment with the College, is prohibited unless such disclosure is a normal requirement of an employee's position or has been so authorized.

All student records are protected by the Family Educational Rights and Privacy Act (FERPA). FERPA is a federal law designed to protect the privacy of a student's education records. College employees may not disclose student information without written consent from the student, regardless of the age of the student. Any request for student information should be sent to the Registrar's Office.

All employee and student financial information is protected by the Gramm-Leach-Bliley Act (GLBA). This act is designed to protect all financial information from disclosure and unapproved access.

Section 4. Violations

The College considers any violation of the Computer Acceptable Use Procedures to be a serious offense and reserves the right to copy and examine any file or information that resides on college systems allegedly related to unacceptable use, and to protect its network from systems and events that threaten or degrade operations. Violation of the Computer Acceptable Use Procedures could result in disciplinary action, termination, loss of information resources and criminal prosecution. Violators also may be prosecuted under laws including, but not limited to, the Communications Act of 1934 (as amended by the Telecommunications Act of 1996), the Family Educational Rights and Privacy Act of 1974 (FERPA), the Computer Fraud and Abuse Act of 1986, the CAN-SPAM Act of 2003, Interstate Transportation of Stolen Property, and the Electronic Communications Privacy Act.

Lenoir Community College licenses the use of its computer software from a variety of outside companies. Lenoir Community College does not own this software or its related documentation, unless authorized by the software developer, and Lenoir Community College does not have the right to

reproduce it. According to U.S. Copyright Law, illegal reproduction of software can be subject to civil damages of $50,000 or more, and criminal penalties including fines and imprisonment.

Any employee of Lenoir Community College making, acquiring, or using unauthorized copies of computer software on any of the College's computers or other computer equipment will be disciplined appropriately.

Section 5. Acknowledgement of the Computer Acceptable Use Procedures

College employees and contractors must acknowledge in writing that they have received a copy of the Computer Acceptable Use Procedures. Written acknowledgement is also required annually on a date determined by Human Resources.

I have read, understand, and will abide by the above Computer Acceptable Use Procedures when using computers and other electronic resources owned, leased, or operated by the College. I further understand that I will abide by the above Computer Acceptable Use Procedures when using personal computer devices not owned, leased, or operated by the College. I further understand that I have no expectation of privacy when connecting any device to the College Network and that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation of this policy, my access privileges may be revoked, disciplinary action may be taken, and/or appropriate legal action may be initiated.

Employee's Signature Date