

Electronic mail, Internet access, and other electronic media and equipment are business tools that are provided by John A. Logan College (JALC) to employees and students to facilitate timely and efficient conduct of business. To help ensure that these tools are used appropriately, JALC has developed the following acceptable use policy. This policy addresses access, use and disclosure of electronic mail and Internet messages and material created, sent or received by JALC employees and students using the College's systems.

As a condition of access to and use of the College's computer and network system, users are deemed to acknowledge and agree to comply with the Board's policies and the Administration's rules and regulations.

1. **Purpose.** JALC maintains electronic mail, Internet access, local network storage and other information systems. These systems are provided by the College to assist in the conduct of business within the College.

2. **Relation to Other Policies.** Employees and students are to use JALC's electronic mail, Internet systems and other network resources in a manner that is consistent with other College policies.

3. **Acceptable Use.** The use of the electronic mail, Internet/LAN (Local Area Network) systems is reserved primarily for the conduct of business at the College. Limited personal use of the electronic mail and Internet/LAN systems is permitted, but should not be excessive or interfere with normal operations of the College.

4. **College Property.** The electronic mail and Internet/LAN systems and hardware are College property. Additionally, all documents, messages and attachments composed, sent, received or stored on the electronic mail or Internet/LAN storage systems are and remain the property of JALC.

5. **Password Accountability.** Employees or students shall not use a password, access a file, or retrieve any stored communication, other than where authorized. All passwords used in the conduct of College business are the property of JALC. Employees or students may not use passwords on critical systems that have not been disclosed to the Chief Information Technology Officer or other account manager. Any compromised password should be reported to the account administrator. Student passwords are confidential and students are accountable for all usage under their password of the JALC computer systems. Students should change their default password as soon as possible.

6. **Non-Removal.** Employees or students may not remove from the premises any hardware, software, sensitive files or data without prior authorization by the Chief Information Technology Officer. Licensing agreements can only be used for College purposes unless otherwise specifically authorized by the Chief Information Technology Officer and shall comply with the terms of the relevant third party licensing agreement.

7. **Downloading.** In downloading documents from the Internet, JALC requires that such documents shall be related to College business and constitute a reasonable use of the College resources. Executable files may not be downloaded without prior management authorization. Applications such as Peer to Peer file swapping tools and unauthorized browser enhancements/plugin-ins are STRICTLY PROHIBITED.

8. **Offensive or Harassing Use Prohibited.** The electronic mail and Internet/LAN systems are not to be used to create or distribute any offensive or disruptive messages. Among those that are considered offensive are messages or material that contains sexual implications, racial or ethnic slurs, or other comments that offensively address someone's age, sex, sexual orientation, religion, national origin,

ancestry or disability. In addition, the electronic mail and Internet/LAN systems shall not be used to communicate other improper messages, for example, messages or material that is defamatory, derogatory, obscene or otherwise inappropriate.

9. Compliance with the Law. The electronic mail and Internet/LAN systems shall not be used to commit any crime, including but not limited to sending obscene emails over the Internet with the intent to annoy, abuse, threaten, or harass another person, and users shall comply with all state, federal and local laws and regulations.

10. No Sexually Explicit Sites. College-owned equipment, hardware, and infrastructure shall not be used to visit sexually explicit or otherwise offensive or inappropriate Web sites, or to send, display, download or print offensive material, pornographic or sexually explicit pictures or any other materials which would be found offensive by most reasonable people. Content filters which are designed to disrupt access to these materials shall not be bypassed or altered without prior approval of the Chief Information Technology Officer.

11. Solicitation Prohibited and/or Restricted. The electronic mail and Internet/LAN systems may not be used by College employees to solicit or proselytize for outside or personal commercial ventures, religious or political causes, outside organizations, or other solicitations that are not job-related. JALC may provide access to a public electronic bulletin board system which will facilitate voluntary participation in non-business related messages and other transactions. Employees shall not engage in activity which violates the Illinois Governmental Ethics Act (5 ILCS 420/1-101 et seq.).

12. Viruses. Employees or students may not use JALC e-mail or Internet systems to develop or send any virus or otherwise destructive programs. Employees or students should not open e-mails or attachments unless they are confident of the identity of the sender and the content of any attachments.

13. Copyrighted Material and Trade Secrets. The electronic mail and Internet/LAN systems shall not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization. Any attempt to bypass current bandwidth management systems is strictly prohibited.

14. Right to Monitor. JALC reserves the right to review, audit, intercept, access and/or disclose any and all traffic in the system, including messages or material, including attachments created, received or sent, web sites visited and/or files downloaded over the College's electronic mail or Internet/LAN systems. Authorized representatives of the College may monitor the use of its systems at any time, with or without notice to any user and may by-pass any password. Such monitoring is capable of tracking and recording e-mail messages sent and received as well as web sites visited by employees and students.

15. Confidentiality. The confidentiality of any message or material should not be assumed. Even when a message or material is erased, it may still be possible to retrieve and read that message or material. Further, the use of passwords for security does not guarantee confidentiality. Messages read in HTML may identify the reader to the sender. Notwithstanding JALC's right to retrieve and read any electronic mail or Internet messages or material, such messages or material should be treated as confidential by other employees or students and accessed only by the intended recipient. Employees and students are responsible for maintaining the confidentiality of material on the systems. Without prior authorization from the President or a designated representative, employees or students are not permitted to retrieve or read e-mail messages that are not sent to them. The contents of electronic mail or Internet messages or material maybe disclosed to others for enforcement of this policy.

16. Representation of College. Employees and students should be aware that Internet sites accessed from JALC's computer network may identify the College as the originator of each visit. Employees should make clear when they are or are not representing the College in their e-mail or Internet communications. Usage of an appropriate disclaimer on the footer of all messages is encouraged.

17. Disciplinary Action. A violation of this policy may result in disciplinary action ranging from a verbal warning up to and including discharge from employment, expulsion from school and/or pursuit of legal action in accordance with policy and collective bargaining agreements.

ADOPTED: MARCH 14, 1988
AMENDED: JUNE 23, 1998; **NOVEMBER 26, 2013**
LEGAL REF.: 5 ILCS 420/1-101 ET SEQ.
CROSS REF.: