Technology Policy of the Nebraska Legislature

Adopted 11-03-16

Purpose and Intent:

The purpose of the Technology Policy of the Nebraska Legislature is to provide guidance for use of the Legislature’s technology equipment and state secure network and to protect the integrity and security of the state secure network and legislative information.

All use of Legislative equipment or the state secure network shall be subject to this Policy and applicable State and Federal Laws.

Authority:

50-401.01

(1) The Legislative Council shall have an executive board, to be known as the Executive Board of the Legislative Council.

(2) The executive board shall:

(a) Supervise all services and service personnel of the Legislature and may employ and fix compensation and other terms of employment for such personnel as may be needed to carry out the intent and activities of the Legislature or of the board, unless otherwise directed by the Legislature.

49-14,137

Discipline of public officials or employees; effect of act.

The penalties prescribed in the Nebraska Political Accountability and Disclosure Act do not limit the power of the Legislature to discipline its own members or impeach a public official and do not limit the power of agencies or commissions to discipline officials or employees.

Application:

This policy applies to all authorized users of the Legislature’s technology equipment or the state secure network.

Only senators and legislative employees, paid or unpaid, are authorized users of the legislature’s technology equipment and state secure network.
All senators and legislative employees will be required to take a technology training course and sign a statement acknowledging: He or she has taken the training course, received a copy of the Legislature’s Technology Policy, and understands it. This action must be taken prior to being issued login credentials and/or issued state equipment.

**Passwords:**

Effective January 1, 2017, all login passwords will expire annually, or as directed by Legislative Technology, at which time senators and staff will be required to create a new one. A password should not be shared with any other person. If a password is shared, the owner of the password will be responsible for all activity.

**Use of Public Resources:**

Section 49-14,101.01

Financial gain; gift of travel or lodging; prohibited acts; violation; penalty; permissible activities and uses.

(1) A public official or public employee shall not use or authorize the use of his or her public office or any confidential information received through the holding of a public office to obtain financial gain, other than compensation provided by law, for himself or herself, a member of his or her immediate family, or a business with which the individual is associated.

(2) A public official or public employee shall not use or authorize the use of personnel, resources, property, or funds under his or her official care and control other than in accordance with prescribed constitutional, statutory, and regulatory procedures or use such items, other than compensation provided by law, for personal financial gain.

(7) …, any person violating this section shall be guilty of a Class III misdemeanor, except that no vote by any member of the Legislature shall subject such member to any criminal sanction under this section.

**Acceptable Use:**

The policy incorporates the *Acceptable Use Policy* adopted by the Nebraska Information Technology Commission (NITC), which is attached or may be found at: [http://www.nitc.nebraska.gov/standards/7-101.html](http://www.nitc.nebraska.gov/standards/7-101.html)

Examples of uses that are not acceptable include, but are not limited to, the following:

- Use of the Internet for illegal activities, such as gambling;
- Access of sites with adult content, such as pornography, or dating services;
• Posting information on personal, commercial or campaign-related social media sites or websites;
• Use of state resources for personal gain, including buying or selling products or services;
• Copyright infringements, such as downloading unauthorized music, movies, or software; or
• Use of state resources for personal entertainment.

In addition to the above, authorized legislative users shall:

• Respect the privacy of other users and intellectual property or data;
• Not intentionally seek information, obtain copies, modify files or data, or use passwords belonging to other users without authorization from the appropriate party;
• Respect the legal protection provided by copyright and licensing laws to software and data;
• Protect the integrity of the Legislature’s technology equipment and state secure network and not intentionally develop or propagate programs that harass other users or infiltrate a computer or technology system;
• Not knowingly allow unauthorized access to the Legislature’s technology equipment or the state secure network;
• Not damage or alter software or other components of legislative technology equipment or the state secure network; or
• Not install unauthorized software or hardware peripherals, even though they may be related to legislative business.

It is the responsibility of each senator, division director, and ultimately the Executive Board, to make sure that the Legislature’s technology equipment and state secure network are being used consistent with state or federal law and the Legislature’s Technology Policy. Therefore, a senator, division director, or Executive Board chairperson may request, in writing, that the Clerk of the Legislature provide access to electronic work files, messages, and resource usage by an employee under his or her supervision. An employee has no right to privacy from his or her supervisor or the Executive Board as it relates to his or her use of the Legislature’s technology equipment or the state secure network.

**The Capitol Public Network:**

The capitol public network is available for use by senators and staff for non-legislative use. It should be understood that neither access, privacy, nor security is guaranteed on the capitol public network.
**Data release authorization:**

When a senator resigns or otherwise leaves the Legislature, he or she will receive written notification of his or her options relating to technology files. The senator may designate that files, including shared files, be deleted, turned over to the new senator, or archived. In the event the form is not returned, the files will be deleted by the Legislative Technology Center’s staff.

When the Legislature elects new committee chairpersons, committee work files will not be deleted, except for any files that are identified by the previous committee chairperson or legal counsel as protected by attorney client privilege, or as confidential legislative correspondence or memoranda.

When an employee leaves the Legislature, all of his or her files will be deleted after 30 days unless otherwise directed by a division director or chairperson of the Executive Board.

**Violations of the Policy:**

Suspected violations of this Policy should be reported to the senator or division director who should report the suspected violations and the corrective action taken to the Executive Board. Suspected violations may also be reported directly to the Executive Board.

If there is reason to believe that a violation has occurred that could adversely affect the Legislature’s technology equipment or state secure network safety, the senator or division director shall immediately notify the Clerk of the Legislature who shall take appropriate action to protect the state’s secure network and/or equipment. Any situation that is not satisfactorily resolved may be reported to the Executive Board. The Executive Board reserves the right to examine technology equipment and usage archives if a senator or division director does not take action. If a violation involves a member of the Legislature, the Executive Board may only examine relevant information relating to the alleged violation.

If a violation of this policy or of state law is discovered, the Executive Board will take appropriate action, including temporarily suspending, blocking, or restricting access to the Legislature’s technology equipment and the state secure network.

In addition, a violation by an employee may result in appropriate disciplinary action, including termination.

If a violation involves illegal activity, the Executive Board shall notify the appropriate authorities.
Conclusion:

No policy can specify every scenario that might come about, especially in the ever changing area of technology. Therefore, the Executive Board of the Legislative Council reserves the right to determine, at its discretion, whether conduct is reasonable and appropriate under the circumstances.