

Policy 4027: Workplace Privacy

The District will abide by the Nebraska Workplace Privacy Act and will not:

1. Require or request that an employee or applicant provide or disclose any user name or password or any other related account information in order to gain access to the employee's or applicant's personal Internet account by way of an electronic communication device;
2. Require or request that an employee or applicant log into a personal Internet account by way of an electronic communication device in the presence of the District in a manner that enables the District to observe the contents of the employee's or applicant's personal Internet account or provides the District access to the employee's or applicant's personal Internet account;
3. Require an employee or applicant to add anyone, including the District, to the list of contacts associated with the employee's or applicant's personal Internet account or require or otherwise coerce an employee or applicant to change the settings on the employee's or applicant's personal Internet account which affects the ability of others to view the content of such account;
4. Take adverse action against, fail to hire, or otherwise penalize an employee or applicant for failure to provide or disclose any of the information or to take any of the actions prohibited by the Workplace Privacy Act.
5. Require an employee or applicant to waive or limit any protection granted under the Workplace Privacy Act as a condition of continued employment or of applying for or receiving an offer of employment.

Notwithstanding anything to the contrary, all employees must abide by the District's technology policies, procedures and guidelines, including the District's Internet Use policy and/or practice. Pursuant to the Workplace Privacy Act, the District may also:

1. Monitor, review, access, or block electronic data stored on an electronic communication device supplied by or paid for in whole or in part by the District or stored on the District's network, to the extent permissible under applicable laws;
2. Access information about an employee or applicant that is in the public domain or is otherwise obtained in compliance with the Workplace Privacy Act;
3. Conduct an investigation or require an employee to cooperate in an investigation if the District has specific information about potentially wrongful activity taking place on the employee's personal Internet account, for the purpose of ensuring compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct;
4. Any other reason permitted by the Workplace Privacy Act.

Legal Reference: Laws 2016, LB 821

Adopted 7/18/16