njea NEW JERSEY EDUCATION ASSOCIATION

LEGAL SERVICES ADVISORY

Employer-Required Dual Authentication Apps on Personal Devices

In recent months, questions have been raised regarding an increasingly widespread practice of school districts asking their employees to install two-factor authentication mobile phone-based apps, such as Duo Mobile, for the purposes of authenticating authorized users when accessing District computer systems. The measure is designed to combat recent cybersecurity threats that have emerged against districts, particularly ransomware attacks, which have become increasingly prevalent and severe. School districts, much like other industries, are more frequently required to employ multi-factor authentication devices by their insurance companies as a condition of coverage. Often, a cybersecurity threat can be stopped by preventing unauthorized users from accessing a computer system.

What are some members' concerns with these applications?

The requirement for school staff to download dual authentication apps to their personal devices has led to its own understandable security and privacy concerns. Many members feel they should not be required to download applications to their personal device for work use, particularly due to concerns that the software could cause a security breach or be used to monitor employees without authorization, sell their personal data, or subject them to other privacy intrusions.

Can dual authentication be required?

Currently, there is no specific federal or state law that prohibits the employer from asking employees to download such apps. There are reports that insurance industry is requiring districts to implement two-factor authentication as a condition of eligibility for insurance coverage due to the increase in ransomware attacks in all industries, including public education. However, there are negotiable issues to consider.

Is it negotiable?

Yes. There is no authority that preempts negotiations over the devices and methods used for dual authentication, particularly since employers are asking employees to use their personal devices for work purposes.

What should locals be bargaining?

A local association can use its bargaining power to demand more information concerning the specific terms of service and practices of these applications, to assert the interests of members and achieve more favorable terms sensitive to members' privacy so that any objectionable terms of service in the app's license can be negotiated. Additionally, local associations should demand impact bargaining on the implementation of dual authentication software, such as by exploring whether alternatives to downloading dual authentication applications to personal devices, such as the use of separate fob devices for work, could be used for dual authentication purposes.