

Electronic Communications Policies: Transparency Is The Best Policy

04/04/19

The widespread use of electronic communications devices today has employers struggling to regulate acceptable use of such devices in the workplace. Unregulated use may generate problems for employers if employees use devices (intentionally or unintentionally) in a way that violates employment policies (e.g., anti-harassment), or if employees spend excessive amounts of time on these devices so as to impact productivity or otherwise compromise performance. Considering the nuances involved in navigating acceptable use of use smartphones and other devices in the workplace, what solutions are available to employers to regulate use and prevent problems in the work place? The answer is as simple as usage is complex: the Employee Handbook.

Many employer handbooks contain general language such as, the organization “reserves the right to review and access all matters on the organization’s network and services at any time.” However, this (or similar) language is too broad to allow employers to access the numerous types of employer-provided electronic devices. In order to be able to monitor device use by employees, employers must describe each type of media system covered by policy, (e.g., laptops, smart phones, tablets, etc.) that the employer reserves the right to access and review. It is important that employers provide notice to employees that specifies which devices and systems are covered by an organization’s IT policies. If a policy fails to achieve this level of specificity, in a dispute, an employee may claim a reasonable expectation of privacy in an electronic communication relative to a specific device.

Situations arise that require employers to access an employee’s password-protected accounts. For instance, when an employee is alleged to have used those accounts to harass a co-worker, or in an another example, if an employee is out on extended leave and information is contained in that employee’s email account that must be retrieved to meet a deadline. A Policy that does not specifically state that it may monitor an employee’s personal, password protected email account on a company owned device is not specific so as to allow the employer to do so.

The key to adopting an effective electronic communications policy is for employers to provide notice to all employees that details all of the modes of electronic communications the organization monitors. Therefore, employers should identify each type of communication being monitored in the company handbook. For example, the handbook should state that employees’ personal, password protected email account accessed on company owned laptops, personal computers or smart phones is not private and may be monitored and accessed by the company at any time. Otherwise, an employer risks an argument that the employee has a privacy interest in a particular type of communication.

Caveat: An employee’s emails to an attorney in a password protected personal account is excluded from such policies because such communications are protected by the attorney-client privilege.

TAKEAWAY: Employers should be specific in drafting electronic communications policies and should provide notice to all employees.

Have an employment law question? Maybe we can help. Contact Stephanie Gironda at (732) 855-6027.

Attorney

- Stephanie D. Gironda

Practice

- Employment Law