

MAKING A CASE FOR COMPUTER, INTERNET OR E-MAIL ABUSE

It is a fair statement to say that today's businesses are dependant on the computer, Internet and email. Companies reap the benefits of on-line access and instantaneous communication, but at the same time risk corporate liability (harassment and discrimination claims; creating a poisoned work environment), criminal liability (possession or distribution of obscene material), or breach of confidentiality, copyright or other intellectual property claims resulting from an employee's email or internet indiscretions and misconduct. Liability, virus damage, lower productivity and lost profits, makes uncontrolled or unregulated use of the computer, internet or email in the workplace a concern for the modern employer. Having a plan in place that identifies and deals effectively with computer abuse gives the employer an advantage in protecting the workplace, the workforce and ultimately, its business interests.

Discovering computer, Internet or email abuse

Many organizations have introduced *pro-active*, on-going monitoring of employee computer use. Technology is at a point where employee use is easily identified, tracked and recorded. Access to particular web sites or site categories is easily restricted through basic web and email filtering software. Scanning incoming and outgoing information can identify viruses, offensive or confidential information. Effective monitoring will notify the employer of an employee's misuse or abuse of its computer, Internet or email system while at the same time, balancing the employer's concerns against employees' privacy rights.

There are also numerous examples where management is required to *react* to computer, internet or email abuse -- as a result of incidents brought directly to their attention, as the recipient of inappropriate or offensive material, workplace complaints, or information discovered while investigating a related effect of the misconduct, for example, low productivity stats or a slowdown in network operation or efficiency. In these instances, the employee misconduct has an adverse impact on business operations and/or employee morale and forces the employer to remedy the situation or expose itself to greater liability.

Investigate

A proper investigation will determine the existence and extent of the alleged misconduct, including the type of behaviour involved and the degree of time or number of incidents. Whether the investigation can be done in-house, or in conjunction with an expert in computer forensics, the employer must move swiftly to both uncover and preserve the evidence. Electronic logs, audited records and software tools can and should be utilized to trace the employee's electronic footprints.

In addition to high-tech tracking, basic management tools for investigation and complaint handling should not be overlooked. The failure to inquire whether others had access to the computer or whether there were witnesses to the alleged crimes will act to the employer's detriment. Something more than circumstantial or hearsay evidence is often necessary before action can be taken against an employee.

Identify the level of seriousness

Upon discovery, identify the type of misconduct involved. Specifying the behaviour in issue helps determine the level of seriousness, which in turn affects the degree of discipline, including termination, that can be imposed and likely upheld at trial or arbitration.

Decided cases in this area appear to group computer, email and Internet abuse in three main categories:

- (1) personal use – which would include three subcategories:
 - a. downloading inappropriate email from the internet;
 - b. receiving and sending inappropriate email; and
 - c. general correspondence, banking/trading, shopping;
- (2) accessing and/or distributing confidential internal information; and
- (3) using the email or computer system as the vehicle for insubordinate or insolent behaviour.

Subject to individual mitigating circumstances, significant indiscretions of personal use, including downloading of pornography (and child pornography in particular), and the dissemination of sexual, racial or other offensive material is viewed as serious misconduct and will justify greater disciplinary responses, including termination. Similarly, unauthorized access and distribution of confidential information will expose a curious employee to stiffer penalties, regardless of whether or not the employee gained any personal benefit.

On the other hand, limited personal use of the company's computer, internet and e-mail system which is not distributed to management, co-workers or business clientele, and does not meet the threshold for harassing or discriminating conduct is not viewed with the same level of seriousness, and in most circumstances will not justify the greater penalties, if any.

Acts of insolence and insubordination using email also varies with the degree of disrespectful behaviour displayed. For example, discharge was upheld in a case involving emails to a parent company's Board of Directors containing false, inflammatory and disrespectful comments about local management, whereas the use of email to inform 400 co-workers of the reasons for an employee's work refusal attracted only a 2-day suspension.

Apply the policy

The average workforce would likely resist a complete prohibition on computer use for personal reasons. Experience tells us that an acceptable use policy should identify the scope of permissible and prohibited use and confirm that employees do not have a reasonable expectation of privacy when using employer-provided internet or email access. Furthermore, failure to satisfy all the requirements of a valid policy¹ could vitiate any penalty ultimately imposed.

A number of employers have lost cases despite ample evidence of employee misconduct where the policy did not apply to the specific behaviour complained of; where the employer failed to fully communicate the policy to the staff; where the policy was applied inconsistently as between employees, or a lax application of the policy altogether. A thorough review of the policy and its importance with the staff will defeat any claim that an employee was unaware of the policy or that its significance was not understood.

Consider Mitigating Circumstances

Lastly, consider any mitigating circumstances. These would include a long period of employment with a clear disciplinary record; personal, emotional or financial problems; general misunderstandings and whether the employee accepted responsibility and acknowledged any wrongdoing. Mitigating circumstances have the effect of reducing or negating the imposition of otherwise stringent penalties.

Although yet to be formally recognized, a few cases are raising the issue of "internet addiction", similar in fashion to gambling or alcohol addictions where the evidence demonstrates an employee's loss of control and inability to self-regulate. If accepted, an "internet addiction" would act to an employee's defence and further impose upon an employer a duty to accommodate.

¹ A policy or workplace rule unilaterally implemented by an employer must not, where applicable, be inconsistent with the collective agreement; must not be unreasonable; must be clear and unequivocal; must be brought to the attention of the employees before it can be acted upon; if used as the foundation for discharge, the employee must be notified that breach could result in his termination; and must be consistently enforced from the time of introduction.

Conclusion

It is an employer's responsibility to protect its business interests, the workplace and its employees from the effects of computer, Internet and email abuse. Effective management, in conjunction with technological tracking and filtering devices, will assist in investigating and identifying computer misconduct. Awareness of limitations on acceptable and inappropriate computer use and employee behaviour defines the boundaries by which employee behaviour will be measured. Together, these skills provide a strategy to deal effectively with computer, Internet and email abuse as it arises, and to avoid the potential for greater liability in instances where such behaviour goes unchecked.