

Email Use Policy

January 2009

Considerations In Formulating An Email Use Policy

Email use is growing. In 2007, Statistics Canada reported that 81% of private sector enterprises made use of electronic mail, compared with only 53% in 1999. From internal meeting requests, to distribution of documents and general conversations, email has to a large degree replaced not only traditional written correspondence, but also in-person and telephone communication. It permits geographically dispersed offices to communicate and allows employees to work from offsite locations.

Although email may be one of the most important business technology advances since the invention of the telephone, the growing use and abuse of this medium of communication raises a number of critical issues for businesses. From an employment law perspective, employers must consider what steps they can take to be protected from an employee's improper use of its email system. From a risk management perspective, employers must consider how policies regarding the storage and retrieval of corporate email will facilitate records management goals and assist the corporation in defending or pursuing future litigation.

Employment Considerations

Email has become the primary means of communication between employees in many workplaces and access is as necessary as having a telephone at one's desk. However, most employees don't worry that their telephone calls are being recorded, or that every word of a telephone conversation is preserved, word for word, as a public record, forever. With email, perhaps employees ought to think that way.

Although most employers don't monitor every single email that employees send any more than they would record every telephone call made, most employers do monitor email usage at least to a limited extent. Many employers warn their employees that emails can never be considered private because they can be forwarded publicly so readily, or transmitted in error to unwanted recipients. Employers have the right to monitor emails, and in some settings they

are monitored extensively. In addition, employers have an interest in ensuring that employees use their email access primarily for work – especially during working hours.

Inappropriate email exchanges have resulted in discipline or termination of employees on the basis of just cause. It is obvious that forwarding sexist, degrading or pornographic jokes or internet sites can be grounds for summary dismissal. But also, employees who think they are sending privately-held negative views about their colleagues or supervisors might soon find their views are known to management – and viewed as insubordinate. Employers do have the right to react to these emails: they are never really private in the way that most of us expect conversation to be private.

It is difficult for employers to monitor what their employees do with information they are given over an "intranet" or email system. There are so many ways to "download" or transmit information that proprietary information like client lists, quotes or proposals or other valuable information can hardly be considered private if it is distributed broadly over an email system. Employers should therefore also be cautious about the manner in which confidential information is provided to employees. Email may not be a suitable tool for retaining or transmitting highly sensitive or valuable information.

Records Management Considerations

Systems for managing record keeping are not new. What is changing is the way we keep records. The growing use of email and other computerized documents requires

businesses to manage large quantities of records that are stored in a variety of different formats; including magnetic tapes, diskettes, hard drives, hand-held devices such as the Blackberry®, as well as the traditional paper document.

Companies must follow legal and regulatory requirements that dictate retention periods for certain documents, whether in paper or electronic form. Storage of certain types of corporate records must also comply with privacy laws.

Enforcing corporate practices over record keeping, retention and destruction policies, and instituting appropriate security measures at each stage of records management will ensure the integrity of electronic records and protect corporate networks from internal and external attack. A well-developed records management program is the key to proving the authentication of such records should the corporation subsequently become involved in litigation. Because electronic records are more susceptible to corruption, tampering, forgery and unauthorized interception than paper records, it is important for organizations to ensure that security procedures are in place.

Organizations must be able to identify what they have, what they must keep and what they can eliminate. Being able to identify, on an ongoing basis, the specific information that must be preserved pursuant to legal and regulatory obligations assists the organization in reducing its information storage and recovery costs. However, an effective records management program must recognize that even before litigation is commenced, an organization has an obligation to preserve documents that might be relevant to pending or potential future litigation. Any attempt to destroy evidence may subject a party to monetary sanctions.

Litigation Considerations

In most civil cases, email is the most sought-after form

of electronic evidence. Like any other written communication, it is subject to rules regarding disclosure to an opposing party during litigation. Emails are also subject to review by law enforcement officials and industry regulators. Yet the medium is treated so informally that people tend to write email messages without much thought. Formal contracts can be created by these casual notes, and slanderous and defamatory comments can be made in passing. Control over the content and the number of recipients is lost once the “send” button has been pushed. Even if the email is deleted, the messages can usually be retrieved from a variety of locations. Email has the potential to become the corporate equivalent of DNA evidence, on which the litigation turns.

Email messages have played a prominent role in several recent high-profile cases.

- A sole email from an in-house attorney at Arthur Anderson advising a partner to edit an internal memo about Enron Corp.’s financial disclosure helped to convict the accounting firm of obstruction of justice.
- Merrill Lynch Internet Analyst, Henry Blodget, apparently considered AtHome Corp. “crap” even while he was publicly advising clients to buy the shares.
- Credit Suisse First Boston Investment Banker, Frank Quattrone, told his staff to destroy documents that were being sought by investigators.¹
- Bill Gates emailed his executive “Do we have a clear plan on what we want Apple to do to undermine Sun?”²

In addition, an email carries “metadata” which is embedded information about the author, the creation date, the attachments and identities of all recipients, including those who received a cc or bcc. Word documents included as attachments will reveal how, when and by whom an electronic document was created, modified and transmitted. When parties exchange different versions of documents using the “track change” function, these changes become part of the metadata. This embedded data is not apparent in the printed version of the document and could be critical in situations

such as contract disputes which turn on the parties' intent and their negotiations. An electronic version of a document may also provide evidence of document tampering.

Issues to Consider in Formulating Corporate Email Policies

In formulating an email policy that properly takes into account the above concerns, an organization should be guided by several basic goals:

1) Link the records management goals of the organization to its risk management objectives. A comprehensive records management program must properly preserve corporate information thereby enabling the organization to respond to regulatory and litigation obligations.

- Define what records must be kept, where and how they are to be kept, and for what interval of time they are to be kept.
- If employees are telecommuting, determine how much control the organization requires over electronic communication in order to ensure confidentiality and security where the equipment is maintained in the employee's home.
- Identify who has access to the records, and for what purposes, in order to establish the physical security of the records.
- The architecture of the information systems used to store electronic records should take into account the need to maintain both privacy and security of the information. Certain records may require additional security protection in the form of encryption, passwords and PINs.
- The architecture of any records management strategy must also take into account technology obsolescence. Careful attention should be paid to converting stored data into current formats as part of a system upgrade.

2) Take steps to minimize the litigation risks arising from the improper or thoughtless use of corporate email. Employers have an interest in training employees and developing policies that assist employees to be careful with their words.

- Educate employees on the pitfalls of casual email conversations – ask the question “Would you want a jury or a judge to read this?” before sending an email.
- Educate employees about the myth that “delete” means permanent deletion.
- Emails which are relevant and important records of contract negotiations or terms should be retained in an electronic form that maintains the relevant metadata.
- Identify those emails that could be relevant to a civil claim brought by or against the organization. These emails should be retained in an electronic format even if printed out and stored in a secure, accessible location that ensures the organization will be in a position to meet any litigation disclosure obligations.

3) Articulate a clear acceptable use policy for employees. Explain to employees the purposes for which email systems can and cannot be used. The consequences for breaching the policy must be unambiguous. A clear policy for discipline (reprimands to dismissal) should be set out if information is conveyed via company computers that is: confidential; defamatory of the company or a co-worker; constitutes harassment of or is degrading to co-workers; insubordinate or breaches an employee's obligation of loyalty and fidelity; damaging to the company's reputation.

- Ensure that employees are aware of restrictions with respect to use of any licenses or copyright material.
- Develop clear policies allowing the employer random monitoring of email technology to prevent employees from overusing their computers for personal use, gambling, surfing and messaging.
- Try to ensure that supervisory employees don't overuse the email system. Criticism or discipline is still better implemented in person, in a private setting.
- Make sure all employees with access to confidential information understand their obligation to prevent inappropriate disclosure of that information.
- Develop policies that promote the use of language that enhances the reputation and public image of the business.

The importance of formulating a corporate email policy that correctly takes into account records management and risk management objectives cannot be overemphasized in the digital age. Implementation of a corporate email policy as part of a broader records management program can assist the corporation in defending or pursuing future litigation, help the corporation discharge legal and regulatory requirements, and reduce the burden and costs of storing irrelevant and obsolete documents. Organizations believing

such practices to be a corporate luxury or “make-work project” that can be left for another day, are only postponing the inevitable and are arguably opening themselves up for more severe cost consequences, including the inability to pursue a claim or put forward a defence.

Has your company met the business challenge of properly managing its electronic information?

¹ Steve Maich, “Who Are We Trying to Protect: Brokers Email Walls”, Financial Post, August 19, 2003, p. IN 1

² Delorah Cutland, “E-Documents Play Increasing Litigation Rose”, 10 Washington Journal (Feb. 5, 2001): Online, Applied Discovery Home Page, <http://applieddiscovery.com/lawlibrary>

Karen Groulx
is the firm's
E-Business
Law expert.



Pallett Valo LLP Commercial Litigation Law Group

Our firm has the largest Litigation Department in Peel Region, with the depth and expertise to provide legal advice and representation in complex litigation matters. Our clients are served with advice that is designed to minimize and avoid risks and business disruption through alternative dispute resolution mechanisms, and decisive and aggressive action in the Courts when necessary.

Karen's practice has a specific focus on the preservation and enforcement of construction liens, bonding and trust claims, as well as information technology and intellectual property disputes. Karen was a member of the Electronic Discovery Sub-Committee of the Task Force on the Discovery Process in Ontario, which produced the Guidelines for the Discovery of Electronic Documents in Ontario, and is an active member of The Sedona Conference® Working Group 7, "Sedona Canada."

Karen Groulx kgroulx@pallettvalo.com
Direct Dial: 905.273.3022 Ext. 281

Pamela Yudcovitch
heads up the
firm's Labour
and
Employment
Law Group.



Pallett Valo LLP Labour & Employment Law Group

We have the legal expertise and rich experience to provide creative and pragmatic solutions for a wide variety of employment-related issues. Our approach is to provide advice that minimizes the time, costs and disruption associated with labour and employment disputes.

Pamela specializes in labour relations, human rights, a broad range of employment and dismissal matters, and often represents employers with respect to workers compensation appeals.

Pamela Yudcovitch pamyudco@pallettvalo.com
Direct Dial: 905.273.3022 Ext. 218

This article provides information of a general nature only and should not be relied upon as professional advice in any particular context. For more information about email, your business and the law, contact a member of our **Commercial Litigation Law Group** or **Labour & Employment Law Group** at **905.273.3300**.

If you would like additional copies of the bulletin, or know of anyone who would be interested in joining our mailing list, please contact our Marketing Coordinator at marketing@pallettvalo.com.