



Running a Home Business on the Office Server (and other good reasons to have a Technical Use Policy)

By Dave Bilinsky¹

Introduction

It has become a daily happening in the tabloids — employees discovered having downloaded pornographic material from the web onto their office computers, sending offensive messages or attachments using the office email system, visiting adult chat rooms, downloading questionable software, introducing viruses embedded in cartoons and graphic files, running pirated copies of software and otherwise placing their companies' assets and reputations at risk. Furthermore, there is the less visible misuse of those assets through employees' unauthorized personal use such as running personal businesses on the office servers. Lastly, there is the loss of productive time by employees surfing or otherwise not engaging in authorized activities.

Why does an law firm need an acceptable use or technical use policy?

- for HR purposes if action must be taken against a staff member for inappropriate use
- to set a framework for outlining behaviour — both appropriate and inappropriate
- to assist if a matter must go to court
- to create awareness in order that all staff recognize compliance and non-compliance
- to provide a standard or reference point

Law firms have a particular status relative to their legal responsibilities to their clients, not to mention their reputation and status in the community and the threat of disciplinary action. Lawyers should be acutely aware of potential liability issues that can arise in the above-noted scenarios.

All law firms need to draw the appropriate use of the firm's technology resources to the attention of new and current employees alike and remind all employees of changes and updates as they occur. Wendy Leibowitz in the article cited in the web sites of interest below states that some firms have the Acceptable Use Policy ("AUP") appear as the employees' default page on the

¹ This paper was presented initially at the 2002 ABA Techshow, held in Chicago in March 2002.

Running a Home Business on the Office Server

office intranet. However the firm promulgates the policy, there must be a method in place to draw all staff's attention to changes as they occur.

What are the issues involved in considering an AUP?

Scope

The issues with regard to scope can be summarized in WHO, WHEN, WHAT and WHERE.

To whom is the policy to apply? All staff are a given — give further consideration to temporary employees or third parties such as IT consultants, guests and visitors and others who could get access, such as children via office equipment connected to the internet at home.

When is it to apply? 24 hours a day, 365 days a week would be the normal default unless special considerations apply.

What resources are covered? Start with all equipment in the office. Consider that many firms allow telecommuting, off-site access and dial-in access. Furthermore, laptops and personal digital assistants (PDAs) allow wireless access to the internet, either through the office connection or via a separate ISP connection.

Where are the resources located? Firms now store data on either their own servers, on third-party servers via ASP's (application service providers) or internet group work spaces.

Purpose

The stated purpose of the AUP is to set a minimum standard governing the use of the firm's technological resources and, in particular, the internet and email resources, to minimize the risks and costs to the law firm. It also serves to communicate to all that management views this issue seriously and that personal responsibility is expected of all.

Principles

The firm needs to consider if the firm's technological assets are to be used solely for business use or if a reasonable amount of personal use will be tolerated. If personal use is tolerated (similar to personal use of the telephone system), what are the constraints on that use?

Use of all of a firm's resources brings on responsibilities and obligations.

The principles section should also set forth the expectations of employees relative to the Firm's other policies and procedures and all federal, state or provincial law. Since internet use can cross political boundaries, employees should be expected to respect the laws of all relevant jurisdictions.

Running a Home Business on the Office Server

Conduct should not just be legal — law firms would expect that their staff act in an ethical and courteous manner, respecting privacy and confidentiality and avoiding all harassment, intimidation and annoyance. In particular, staff would be expected to strictly safeguard all client confidential materials in all forms — paper, digital, video, audio or a combination of any of these.

The firm is also financially interested in ensuring that the resources are used effectively, productively and efficiently.

Acceptable and Unacceptable Activities

The AUP sets out that the firm expects staff to use the resources for the mission of the firm (acceptable use) and not for unacceptable purposes.

Unacceptable uses include:

- Prohibiting activity such as accessing, storing or distribution of adult content or visiting adult sites or chat rooms or using the email system for such content distribution.
- Distribution of harassing jokes, threats or other items of whatever nature (cartoons, graphics, drawings, photographs, WAV files, streaming media) that do not belong in a work environment.
- The unauthorized practice of law.
- Any illegal purpose.
- The use of the resources for private purposes, such as the running of a business off the firm's resources, distribution of chain mail, solicitations, promotions, religious or political causes, the distribution of controversial or potentially offensive or defamatory comments.
- The downloading of intellectual property in contravention of licenses, copyright or trademark laws.
- The downloading or installation of any software not approved by the firm.
- Using the equipment to hack or attack other systems.
- Accessing web-based email from computers behind the firm's firewall protection. This email can circumvent the anti-virus and malicious code protections built into the office's network and email system.

Users may also be subject to limitations as determined by the Firm from time to time.

Other Use

The firm must decide if it will allow limited commercial or non-commercial, charitable or not-for-profit uses and, if so, what the policy will be for approval of such use.

The firm should consider the limitation on use of equipment such as laptops that can access not only the office network, but also other networks via the network and modem capabilities built into these computers.

Privacy Considerations

All staff should be made aware that their use may be monitored and there is no expectation of privacy subject of course, to all relevant labour and privacy laws. Courts can demand electronic evidence, including backup copies of emails sent and files stored on the system, regardless of whether those are personal or work-related. Aside from being potentially embarrassing, the production of such evidence can be very time-consuming and expensive.

Whether the firm routinely monitors the use of resources is a matter to be considered and the resultant policy should be set forth in the AUP.

The firm should take no responsibility for the disclosure of private communications that may take place using the firm's resources.

Users are expected to keep all passwords and security means and methods confidential. There should be a prohibition on the sharing of passwords.

Staff are expected to gauge the sensitivity of information and the means contemplated to transmit that information among staff members, to clients and to third parties (such as consultants, experts and others). If encryption technology is utilized, staff should provide the firm with all passwords and/or keys or other means to access those encrypted communications.

Sanctions

No AUP would be complete without a discussion of the possible sanctions that may result for lack of compliance. Possible sanctions include loss of access to firm resources including email and internet access, loss of passwords and disciplinary action including termination.

Since the actions of staff may open up the firm to legal action, the AUP should state that illegal acts could open up the violator to prosecution under relevant statutes. Furthermore, the firm itself could seek redress against any violators including damages, indemnification and costs.

Acknowledgement

The staff member would be expected to read this document and sign a copy indicating his or her acceptance to the terms set out therein.

Consider a statement that any potential signatory may seek independent legal advice prior to signing the document.

Web sites of interest

<http://rr.sans.org/policy/considerations.php> — Considerations for an Acceptable Use Policy for a Commercial Enterprise, David P. Ehinger, November 22, 2000

<http://www.llrx.com/features/wulffson1.htm> — Internet Usage Policies in the Workplace, Part I, by Todd Wulffson

<http://www.llrx.com/features/internetpolicy.htm> — My Kingdom for an Effective Internet Policy!, by Wendy Leibowitz

<http://www.gigalaw.com/articles/gall-2000-01-p1.html> — Company E-mail and Internet Policies, by Barbara Weil Gall

<http://www.cli.org/emailpolicy/assemble.html> — Computer Law Institute's "Assembly a Policy" site

www.sans.org — SANS Institute has a sample Acceptable Use Policy as well as other sample use policies for different technology resources

Appendix

Sample

[INTERNET AND EMAIL USE POLICY](#)

(click on link above for sample policy)