

Technology in the Workplace

Breakfast Briefing Presentation – November 13, 2007

Presented by:
Robert M. Howie



What is Technology?

- ◆ The word **technology** comes from two Greek words: **techne** and **logos**
- ◆ **Techne** means art, skill, or the way, manner, or means by which a thing is gained
- ◆ **Logos** means word
- ◆ So, literally, technology means the manner in which words are gained
- ◆ Merriam-Webster definition: “the practical application of knowledge especially in a particular area” and “a capability given by the practical application of knowledge”





What is Technology?

In today's workplace, **technology** means

- A. An essential and indispensable business tool
- B. Trouble
- C. A way to buy Christmas presents for relatives
- D. A dating service
- E. A bulletin board
- F. The modern workplace
- G. All of the above



Workplace Technology Risks – The Top 7

1. Internet usage
2. Electronic mail
3. Blogging
4. Telework/working remotely
5. Laptop computers
6. Cell phones, text messaging and Blackberries
7. Security of data



Internet Usage – Some Statistics

- ◆ Employee internet usage is sky high
- ◆ According to a Vault.com survey, **90%** of workers admit using internet during working hours for personal purposes
- ◆ Personal internet use makes up **1/3** to **1/2** of all usage
- ◆ Electronic monitoring software sales swelled nearly **5 times** from **\$139** million in sales in 2001 to **\$662** million in 2006
- ◆ According to American Management Association, upwards of **76%** of employers monitor internet usage – and over **50%** of employers have disciplined or fired someone for inappropriate usage



Internet Usage – More Statistics

- ◆ **Electronic surveillance** by employers is “the merciless electronic whip that drives the fast pace of today’s workplace”
- ◆ **59 percent** of sales online were conducted from work
- ◆ The most frequent online shopping occurred at work between **11 a.m. and noon**
- ◆ For each hour of unnecessary surfing per day, a company with 1,000 employees loses an average of **\$11 million a year** in productivity



Where do Employees Go?

- ◆ Where do **employees** say they surf at work? (Harris)
 - ◆ Work related sites - 93%
 - ◆ Maps - 83%
 - ◆ News - 80%
 - ◆ Weather - 76%
 - ◆ Government - 69%
 - ◆ Educational - 63%
 - ◆ Banking - 57%
 - ◆ Travel - 56%
 - ◆ Personal e-mail - 49%
 - ◆ Shopping - 48%
 - ◆ Sports - 30%
 - ◆ Investment/stocks - 29%
 - ◆ Dating - 3%
 - ◆ Adult - 1%



Where do Employees Go?

- ◆ Where do **IT people** say employees surf at work? (Harris)
 - ◆ Weather - 75%
 - ◆ Maps - 73%
 - ◆ News - 70%
 - ◆ Shopping - 65%
 - ◆ Banking - 64%
 - ◆ Travel - 63%
 - ◆ Sports - 61%
 - ◆ Personal e-mail - 60%
 - ◆ Work related - 58%
 - ◆ Educational - 54%
 - ◆ Investment/stocks - 52%
 - ◆ Government - 49%
 - ◆ Dating - 18%
 - ◆ Adult - 11%

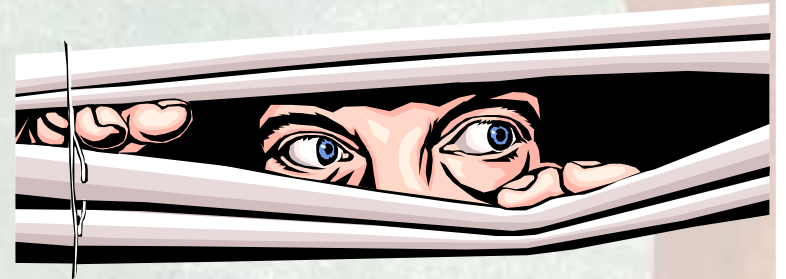


So What Do Employers Do?

“**Work Examiner Standard** is a system for controlling employees' office hours designed for small and medium businesses.

The distinguishing features of the Standard edition include quick deployment, simple and intuitive use of the program, ease of controlling the program.

This solution will allow you to effectively control your employees' efficiency.”





Internet Usage – Legal Considerations

- ◆ Should I have a policy governing internet use?
- ◆ About 80% of employers have policies governing personal internet usage (AMA)
- ◆ A well-drafted policy serves multiple purposes
 - ◆ Educates employees
 - ◆ Clarifies ownership of company equipment
 - ◆ Negates any expectations of privacy



Internet Usage – Legal Considerations

1. Absolute prohibition vs. occasional use
2. Company owns property
3. No expectation of privacy
4. Primarily for business use
5. Responsibility when using
6. Right to access, monitor, disclose, use
7. No inappropriate sites or content
8. No violation of intellectual property rights



Doe v. XYZ Corporation

- ◆ Jane Doe v. XYZ Corporation, 887 A.2d 1156 (N.J. 2005) — Perils of Monitoring
 - ◆ New Jersey accountant arrested on child pornography charges
 - ◆ A police investigation prior to the arrest showed that the employee had stored nude pictures of under-aged girls, including pornographic images of his ten year old stepdaughter
 - ◆ The investigation also revealed that the employee's website viewing history showed the employee had visited sites called "Young First Nude 13 to 17 years old" and "Incest Taboo"



Doe v. XYZ Corporation

- ◆ The stepdaughter's mother sued XYZ Corporation for negligence. Mom claimed that the employer knew or should have known that the accountant was using company computer systems to view, download and participate in child pornography
- ◆ The mother also alleged that the employer had a duty to report its employee to the proper authorities for crimes committed on its property during work hours



Doe v. XYZ Corporation

- ◆ The Appellate Division in New Jersey found that by not fully investigating the employee's prohibited activity, the company was exposed to negligence claims
- ◆ The Court explained: *“The defendant’s Network Administrator testified that he was able to use the network’s daily log system to isolate and identify pornographic websites visited by Employee. However, he did not pen any specific sites and, after reporting his findings to his supervisor, was instructed not to investigate Employee’s internet usage again.”*



Doe v. XYZ Corporation

- ◆ The supervisor was then instructed by corporate management to instruct the employee to cease whatever he was doing. The Court concluded that if the employer had properly investigated the employee's computer usage, it would have discovered the child pornography
- ◆ The Court then concluded that if the employer had discovered the illegal usage, it had an obligation to report the employee to law enforcement authorities



Reporting Child Pornography in Washington

- ◆ RCW 9.68A.080
 - ◆ Scenario: while repairing, modifying, or maintaining a workplace computer, discover data depicting a minor engaged in sexually explicit conduct
 - ◆ MAY report the incident to law enforcement
 - ◆ Immune from civil liability for good faith reports



Other Recent Cases Involving Internet Usage

- ◆ Recent 9th Circuit case affirmed summary judgment for employer where a female employee sued for retaliation after she complained about a male employee looking at pornography at work
- ◆ *Delfino v. Agilent Technologies* – Employer immune from tort lawsuit under Communications Decency Act of 1996 – despite employer providing Internet access and despite employee sending threatening communications to a third party



Who's Got Mail?

- ◆ E-mail volume has doubled over the past 5 years to over **40 billion** person-to-person e-mails daily
- ◆ The volume is expected to continue to grow **over 18%** in each of the next 5 years
- ◆ For the average e-mail user, over **30% of their day** is now spent on creating, organizing, reading and responding to e-mail





E-Mail - Risks/Concerns

- ◆ Lack of productivity
- ◆ Inappropriate content
- ◆ Intellectual property loss
- ◆ Damage to network through misuse
- ◆ Infiltration by third parties



E-Mail - Solutions

- ◆ What can be done about **lack of productivity**:
 - ◆ Have an e-mail etiquette protocol
 - ◆ Limit distribution of mass e-mails
 - ◆ Monitor e-mail use
 - ◆ Draft a policy that regulates and limits personal use of e-mail



E-Mail - Solutions

- ◆ What can be done about **inappropriate content**:
 - ◆ Written policy should explicitly prohibit e-mail harassment or other inappropriate content
 - ◆ Strongly discourage forwarded material
 - ◆ Annual training should include e-mail component
 - ◆ Monitor e-mail periodically
 - ◆ Have managers/supervisors sign acknowledgment of compliance with policy – set an example
 - ◆ Spam filters



E-Mail - Solutions

- ◆ What to do about **intellectual property loss**:
 - ◆ Written policy protecting intellectual property
 - ◆ Monitor electronic mail usage
 - ◆ Ask employees to sign acknowledgment
 - ◆ Pay special attention to departing employees
- ◆ What to do about **damage to network through misuse**:
 - ◆ Policy should prohibit use of downloading unauthorized content



E-Mail - Solutions

- ◆ What to do about **infiltration of third parties**:
 - ◆ The “business use only” dilemma
 - ◆ Policy should clearly state no privacy expectation
 - ◆ Policy should clearly state that employer can monitor, read and access electronic mail
 - ◆ Policy should state that e-mail is company property
 - ◆ E-mail and union organizing – the NLRB and the Eugene Register-Guard



E-Mail - Stories

- ◆ Scott v. Beth Israel Medical Center, NY Supreme Court, October 18, 2007
 - ◆ Plaintiff sued for wrongful termination
 - ◆ While still employed, Plaintiff used employer's e-mail system to communicate with his attorney
 - ◆ Employee moved for protective order returning e-mails
 - ◆ Employee argued privilege – they said “attorney client privilege” on them



E-Mail - Stories

- ◆ Company argued – no expectation of privacy
- ◆ Plaintiff knew or should have known of company policy
- ◆ Three important factors
 - ◆ Company e-mails were for business use only
 - ◆ Employee on notice no right to privacy
 - ◆ Employee on notice of right to access and disclose



E-mail Stories

- ◆ Real e-mail sent by regional manager to HR!

I think her mom was Black Hispanic and her dad was White Pacific Islander, but I can't be sure.

Based on my keen observation skills I would think she was a middle aged woman with dark graying black hair.

However, Elizabeth was the Queen of England and this indicates she probably has Anglo-Saxon blood lines, while Martinez coming from the Japanese American Indian words meaning "Martini" and "Nez Perce" would lead one to believe that her ancestry comes from a long line of American Indians who developed tolerance to alcohol during their journey towards Canada along side Chief Joseph and thus added their favorite beverage to their family name. This however being completely politically incorrect motivated them to cover up the true meaning by claiming Mexican national status on their 1879 Immigration and Naturalization forms.

Now if I have to pin point her ethnicity I would venture to say – Latino or Hispanic.

I hope this has broadened your understanding of the need, or lack thereof, to place people in boxes and categorize them like cattle. God Bless America.



E-mail Stories

- ◆ Real e-mail sent by same regional manager to HR:

Here is my new tally:

Jennifer – pregnant due Sept 4

Hailey – pregnant due Feb 2008

Joanne – pregnant due February 2008

So of my little staff of 7, half are pregnant and/or possibly leaving our employ. I remember the days when the only employee that got pregnant was the one I helped. I sure miss the old mom and pop situation.

I hope you find this as humorous as I do. Thanks.



E-mail – Final Thoughts

- ◆ Beware! Employment pitfalls ahead!
 - ◆ Ignoring an internal complaint sent via e-mail
 - ◆ Failure to preserve e-mails (good or bad)
 - ◆ Inadvertent forwarding to wrong person
 - ◆ E-mails substituting for performance evaluation
 - ◆ Inconsistent enforcement of e-mail rules
 - ◆ Humor/emoticons
 - ◆ The gullible employee/boy who cried wolf



Blogging – What is it?

- ◆ A web journal or log (“blog”) is a user generated Internet web site, often a chronological diary of personal thought on the internet
- ◆ Many web hosts that are inexpensive - blogs are easy to start
- ◆ Some people compare a blog to the company's water cooler where thoughts are expressed or questions asked, followed by a string of other bits of wisdom or ignorance
- ◆ 63 million blogs in existence (175,000 new each day!) – 1.6 million posts





Blogging – What is it?

- ◆ So what happens when a blog focuses on work?
 - ◆ Does the First Amendment apply?
 - ◆ Can employer regulate a blog?
- ◆ Legal Risks to Employers
 - ◆ Negligent supervision claims
 - ◆ Trade Secret disclosure
 - ◆ Securities violations



Blogging – What is it?

- ◆ Several prominent cases involving employers terminating employees for items in a blog
 - ◆ Ellen Simonetti and Delta (<http://queenofsky.journalspace.com/>)
 - ◆ Michael Hanscom and Microsoft
 - ◆ Mark Jen and Google
 - ◆ Jessica Cutler (Senate staffer)



Queen of the Sky





Learn a New Vocabulary Word!

- ◆ Heather Armstrong learned the hard way that employers are not blind to blogs
- ◆ A friend sent an email to the vice president of her company directing him to her blog, in which she complained about her supervisors using offensive pseudonyms
- ◆ She was terminated
- ◆ Her blog, www.dooce.com, gave rise to the term “dooiced,” which is the term for getting fired because of the content of one’s website



Are There Any Legal Restrictions On Termination?

- ◆ Consider on-duty vs. off-duty distinction
- ◆ In some states there are lifestyle discrimination statutes
 - ◆ See Howie & Shapero: “Lifestyle Discrimination Statutes: A Dangerous Erosion of At-Will Employment, a Passing Fad, or Both?” *Employee Relations Law Journal*, Vol. 31, No. 1 (Summer 2005)
 - ◆ California, Colorado, North Dakota, New York, among others that may apply to blogging
- ◆ NLRB prohibits surveillance of employees ([Konop v. Hawaiian Airlines, Inc.](#))
- ◆ Whistleblower laws and SOX
- ◆ “Big brother” mentality



Blogging – Do's and Don'ts

- ◆ **DO** consider promulgating a blogging policy
- ◆ **DON'T** encourage blogging unless you are prepared to accept the consequences
- ◆ **DO** protect confidentiality of company's information and trade secrets
- ◆ **DON'T** overreact to criticism on blogs or make hasty employment decisions
- ◆ **DO** investigate if an employee complains about inappropriate commentary/defamation in a blog



Blogging Policy

- ◆ Elements of a Blogging Policy
 - ◆ No expectation of privacy
 - ◆ No protection of personal information
 - ◆ Require protection of company information
 - ◆ No blogging about company financial information, business plans
 - ◆ Need prominent disclaimer
 - ◆ Reserve right to discipline/discharge
 - ◆ No defamation/no violation of company policy



Telework/Remote Work

- ◆ Benefits
 - ◆ Allows flexibility
 - ◆ Can be disability accommodation
 - ◆ Can encourage return from workers' compensation injury
 - ◆ Great for new parents
 - ◆ Avoids longer commutes
 - ◆ Reduces pollution



Telework/Remote Work

- ◆ Employment Risks
 - ◆ Oversight – how to enforce rules?
 - ◆ Safety/health compliance
 - ◆ Workplace injuries
 - ◆ Protection of confidential information
 - ◆ Monitoring of home computer
 - ◆ Hours worked and breaks



Laptops

- ◆ Who is allowed to use a laptop?
- ◆ What rules govern taking laptops off company property?
- ◆ Who pays the costs if laptops are lost or stolen?
- ◆ What happens if employees start working on the laptop (Brinks case; Singh case)?



Risk of Laptop Theft

- ◆ Many states have laws requiring notification of people if you lose their personal information
- ◆ Washington provides a private right of action
- ◆ HIPAA rules
- ◆ Be careful how much information is on a laptop – the more information = higher risk



Cell Phones & PDAs

- ◆ Employers often provide cell phones and other hand held devices
- ◆ Policies should govern their use
- ◆ Address safety concerns
- ◆ Washington State law (effective 1/1/08) bans text messaging while driving and bans holding a wireless device to the driver's ear (hands free are OK)
- ◆ Consider possible liability if employee violates law and is in an accident while driving during the work day



Security of Data

- ◆ Ensure that employees sign confidentiality agreement
- ◆ Agreement should require protection of company information
- ◆ Require employee acknowledgement not to download unauthorized materials onto company computers
- ◆ Some employers restrict access to personal e-mail accounts at work



Security of Data

- ◆ A federal appellate court recently reinstated a lawsuit brought by an employer against a former employee who deleted all the data on his company issued computer following his resignation. The court ruled that the employee could be held liable under federal law for loading software on the computer which made recovering business files impossible.

International Airport Centers, L.L.C. v. Citrin,
No. 05-1522, Seventh Circuit Court of Appeals (March 8, 2006).



Security of Data

- ◆ New weapon against employees who leave to join the competition and access information from their former employer's computer system without authorization.
- ◆ Computer Fraud and Abuse Act ("CFAA"). Amendments have greatly expanded this 1994 law and CFAA is an attractive weapon against disloyal employees. Damages and injunctive relief are available and, more important, a federal cause of action that does not require that confidentiality, trade secret, and/or noncompete agreements be in place



Security of Data



For instance, the company that hired the computer guy in “Jurassic Park” who created a program to prevent his employer from accessing the system, which allowed T-Rex to escape the electric fence and eat the lawyer, might have a cause of action against the employee



Listening to the Classics

- ◆ Old laws still apply to new technologies
 - ◆ FLSA / Washington Minimum Wage Act
 - ◆ Portal to Portal Act
 - ◆ NLRA
 - ◆ OSHA / WISHA
 - ◆ Title VII





Technology Resources Usage Policy



TECHNOLOGY RESOURCES USAGE POLICY February 2006

we use and rely on electronic forms of communication and information exchange such as electronic mail, the InternetWorld Wide Web, our computer network, voice mail and fax machines, along with other Technology Resources. These Technology Resources are the property of Riddell Williams and are made available for business use because they make communications more efficient and effective and are valuable sources of gathering and storing information. Because these Technology Resources are Riddell Williams' assets, the Firm may, in its discretion, determine how and when they will be used and for what purposes.

For purposes of this policy, "Technology Resources" means all components of Riddell Williams' computer network including, but not limited to: host computers, file servers, application servers, communications servers, mail servers, fax servers, Web servers, workstations, stand alone computers, printers, software, data files, and all internal and external computer and communications systems (for example, Internet, Intranet, extranet) online sources, electronic mail systems, telephone systems, answering machines and voice mail, video equipment, tapes, tape recorders, electronic organizers, recordings and papers) that may be accessed directly or indirectly from the Riddell Williams computer network.

Technology Resources are primarily for Riddell Williams business use. Limited, occasional or incidental use of such resources for personal, non-business use is acceptable during non-working time or in event of an emergency. However, employees (which in this policy includes shareholders, salaried principals, associates and staff) need to demonstrate a sense of responsibility and may not abuse this privilege. Employees are prohibited from using any Firm property, including Technology Resources, to promote any personal, commercial or business ventures or interests.

Although employees have individual access codes to voice mail, electronic mail and computer network systems, these Technology Resources are accessible at all times by authorized Riddell Williams personnel. All Technology Resources, including all electronic mail and voice mail on our systems, are the property of Riddell Williams. The Firm reserves the right to access, monitor, read, disclose, law and otherwise deal with any messages on its system in any manner that it chooses. Employees have no expectation of privacy in information (including electronic mail) stored in or transmitted through Riddell Williams computers. Consequently, employees should not use these Technology Resources for any information that is personal or private.

In addition, employees should always exercise good judgment in using Technology Resources. Our Technology Resources should never be used for any document or communications that would cause embarrassment or concern to an employee if anyone else inside or outside the Firm knew of its existence. Even though passwords and other security provisions are used they are meant to protect the Technology Resources and their contents from third party intrusion and not to give the user a sense of confidentiality vis-a-vis authorized Riddell Williams personnel. Employees may not use Technology Resources to transmit, create, store, print or download vulgar, sexually explicit messages or jokes or comments that are inconsistent with Riddell Williams' policies prohibiting discrimination and unlawful harassment. Our policies prohibiting unlawful harassment and discrimination apply to all of our Technology Resources.

498-026-0001-014
11/03/11/04/0001-0001

1

These Technology Resources are
Riddell Williams' assets



Technology Resources Usage Policy

Riddell Williams P.S.
Technology Resources Usage Policy
February 2008

For example, in using our Technology Resources, avoid any jokes or comments aimed at individuals because of their sex, race, religion, national origin, disability, marital status, sexual orientation or age. If you receive such messages from individuals outside the Firm, please delete them and do not forward the messages to others. Employees are prohibited from using the Internet or World Wide Web to access offensive or inappropriate sites such as sites with sexually explicit or obscene content or pornographic sites. Employees may not use Technology Resources to transmit, store or download defamatory or threatening messages or "chain letters."

Employees should not send any non-business related electronic mail messages to an "RW Everyone" electronic mailing list without prior permission from the Managing Principal, Executive Director or Human Resources Director.

Passwords are subject to override by authorized Riddell Williams personnel. Although some of our Technology Resources may contain a delete function, the information which has been "deleted" may previously have been backed up or exist in another location. In particular, all Internet/World Wide Web users should be aware that the Riddell Williams computer system maintains a record of all Internet/World Wide Web access. Although a user may "erase" the access "history" from a computer, the main system retains a record of all access. Riddell Williams completes monthly reports of Internet/World Wide Web usage by employees. In addition, Internet/World Wide Web access is not anonymous and users should realize that their access to web sites may be logged by the owner of the web site.

Employees are prohibited from the unauthorized use of the access codes of other employees to gain access to their computers, electronic mail and voice mail messages with the intention of making system modifications or to alter, view, create or display information for an improper purpose.

Riddell Williams' copyright policy applies to all Technology Resources and these resources should not be used for the unauthorized dissemination of copyrighted materials, trade secrets, proprietary financial information, or similar materials. Riddell Williams prohibits the download and use of unauthorized electronic programs from the Internet/World Wide Web to protect the network computer systems from viruses and other malicious programs. The Firm requires that employees observe all applicable intellectual property rights when installing authorized programs.

Riddell Williams' attorney-client privileges with its clients extend to all employees using Technology Resources and all employees must take care to maintain confidentiality regarding issues related to client representation.

Violation of this policy or misuse of our Technology Resources may lead to disciplinary action up to and including termination.

4946-0001-0013.04
1/20/07 11:43:29 AM C:\0000

2

Avoid any jokes or comments aimed at individuals because of their sex, race, religion . . .



Technology Resources Usage Policy

Riddell Williams P.S.
Technology Resources Usage Policy
February 2008

- I have read and understand the Firm's Technology Resources Usage Policy.
- I agree to use all Riddell Williams Technology Resources in compliance with this Policy.
- I will not use any form of e-mail (e.g. Outlook) on my networked PC. (Internet electronic mail can be accessed on any standard PC in the office).
- I will not download software without the prior permission of Information Systems.
- I will not download Internet utilities (such as Active X controls) unless they are approved in advance by Information Systems.
- I will not use "push" technologies or any other continually updating method.
- I will not "stream" audio or video from the Internet unless it is a direct requirement or approved in advance by Information Systems.
- I understand that the Firm's computer system maintains a log of every website that is accessed from a computer on the Firm's network.

Signature _____

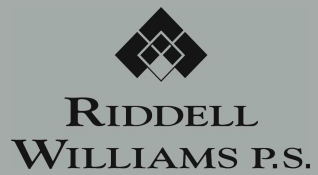
Print Name _____

Date _____

4845-0008-0513.14
1/10/08 11:07:00 AM

13

I understand that the Firm's computer system maintains a log of every website that is accessed from a computer . . .



Questions?

Please contact us any time with additional questions.

Robert M. Howie
206.389.1561
rhowie@riddellwilliams.com