



# Is Your Acceptable Use Policy Social Media-proof?

## ABSTRACT

This paper is intended for IT decision makers, HR managers and executives responsible for adopting and enforcing email and Web Acceptable Use Policies (AUPs) within an organization. It provides guidance on how to update an AUP to accommodate the increasing popularity and use of social media in the business environment. It identifies some of the complexities involved in creating and managing an AUP, especially with evolving Web 2.0 technologies, and demonstrates that a successful AUP is more than a simple list of dos and don'ts.

## CONTENTS

Introduction: What Is an Acceptable Use Policy?	2
Why You Need an Acceptable Use Policy	2
Creating and Developing an AUP	3
Why Organizations Need To Be Concerned About Social Media	3
How To Make Your AUP Social Media-proof	6
Conclusion	7
M86 Solutions for Enabling/Enforcing AUPs	7
Web Security	7
Email Security	7
About M86 Security	7

## INTRODUCTION: WHAT IS AN ACCEPTABLE USE POLICY?

Nearly all organizations rely on information technology to do business. Most office-based employees use a computer, and many have a dedicated business laptop or PC that is also accessed for personal use. Both email and the Web are essential tools that enable employees to do their jobs efficiently and expediently. However, technology is open to abuse.

For years employers have issued guidelines to their staff regarding the acceptable use of telephones at work. Most companies adopt a pragmatic approach and permit reasonable personal use of their telephones, excluding, for example, lengthy or international calls. Others have issued a clear edict that no personal use is permitted whatsoever. With the increased use of email and Web at the workplace, these guidelines are frequently extended to all areas of information technology, eventually becoming an Acceptable Use Policy (AUP).

These AUP policies were among the first drivers for content-orientated features in email security solutions, enabling organizations to uniformly and technically enforce these policies. These email security solutions can be used to train user behavior by alerting the user that a recent action was outside of the organization's AUP. Frequent abusers come to the attention of IT security and human resources staff, where disciplinary actions can be taken. These content features are now being used to enforce other policies such as regulatory compliance and corporate governance policies across email the Web. Some organizations also have a "Business Conduct Guidelines" policy, for which principles the Internet-use AUP should follow.

Some basic filters that can be employed as part of an AUP include:

- Inappropriate language filters
- Inappropriate image analysis
- Dangerous file types
- Inappropriate websites
- Overuse of non-work-related Web browsing activity
- Overuse of non-work-related email

## WHY YOU NEED AN ACCEPTABLE USE POLICY

There are three main reasons for an organization to develop AUPs for email and Web use in their organizations:

1. Safe working environment
2. Employee productivity
3. Internet security

All three areas impact organizations and employees and should effectively work together to ensure employees can do their jobs safely, productively and securely.



Organizations are responsible for providing a safe work environment for employees, and different countries and jurisdictions impose varying levels of enforcement. As part of this environment, employees should be protected from inappropriate material, whether an emailed joke or imagery seen on another employee's computer. Offended employees often hold their employers responsible although the act was perpetrated by other employees. An example of how serious this can get is the US\$982,000 settlement to a former employee of the town of Morristown, NJ, where the employee was subjected to on-going sexual harassment by another employee who displayed imagery on a work computer. ([http://www.nj.com/news/index.ssf/2009/03/former\\_morristown\\_employee\\_rec.html](http://www.nj.com/news/index.ssf/2009/03/former_morristown_employee_rec.html))

Employee productivity can be hampered if un-controlled access to internet resources such as sports sites, video streaming sites, personal webmail, or shopping sites is allowed. Dividing these sites into two main categories, "work related" and "non-work related" helps organizations track usage, but the ability to control usage by time of day or set time limits on non-work-related activities enables AUP enforcement. For example, allowing non-work related internet use before and after work as well as at lunch time. Limiting the access to non-work-related websites keeps employees on task with minimal disruptions.

While of primary concern to the organization, Internet security impacts employees as well. They can be vulnerable to identity theft or another compromise resulting from internet Web-based attack. Providing an effective security barrier is much easier if the organization can tightly control who has access to what types of content. For example, does any employee, except IT staff, need access to executable files? Does anyone apart from marketing need access to streaming video or image files? By tightly limiting employee access to different file types over email or the Web, you reduce your organization's attack surface.

Another helpful control is to limit access to well-known, legitimate, but often maliciously-infected sites that are not business related. Blocking as much unwanted email from employees as possible reduces the chance of employee workstation infection.

While these three areas drive the development and enforcement of AUP policies, they sometimes interfere with each other. This necessitates that organizations prioritize these policies. Importantly, there is no single ideal policy to fit all organizations. Begin from a base framework and customise an AUP to suit your organization.

## CREATING AND DEVELOPING AN AUP

Each organization needs its own customized AUP to suit its business ideals and standards. At a minimum, consider these points:

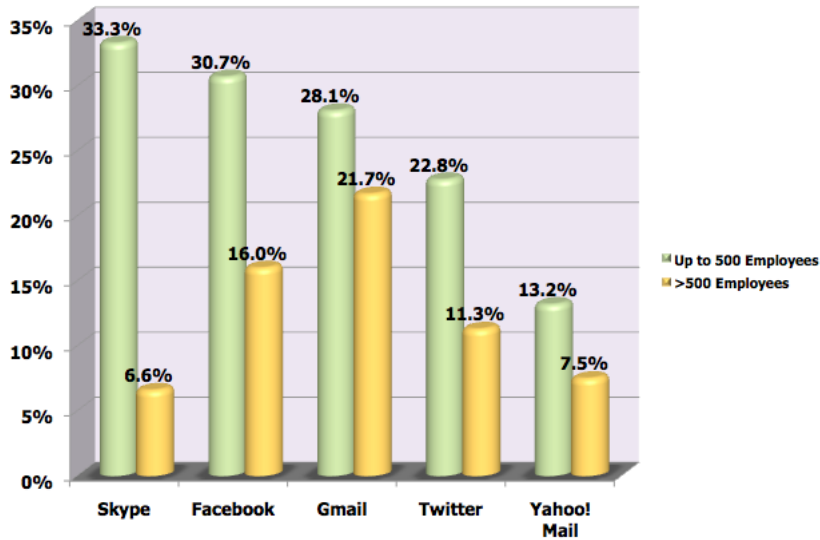
1. Allow limited personal use of Web and email
2. Outline what is acceptable and what is not, while preserving company culture
3. Be consistent with enforcement and setting precedents
4. Identify all email with a name or email address; avoid spoofing
5. Inform staff on copyright issues relating to email or Internet documents
6. Inform staff about what is acceptable inside business hours and what is acceptable outside of business hours, if there is any difference (clearly state this in the policy)
7. Reserve the right to monitor all messages/files on the company network

Many websites offer AUP templates and ideas., Look for sites in a similar jurisdiction to your own, and consider multiple AUPs if you have globally distributed staff, you need to cover any differences in local laws and customs. M86 Security has a white paper and several resources on creating AUPs at [www.m86security.com](http://www.m86security.com).

## WHY ORGANIZATIONS NEED TO BE CONCERNED ABOUT SOCIAL MEDIA

Social media adoption is growing faster than anticipated. It is becoming the new de-facto way of staying in touch with personal contacts, and increasingly, to network with professional contacts. Users spend more time every day, even at the workplace, communicating through these new sites — typically with very little control or security enforcement. This is why organizations need to address social media activities in their AUPs. Simply blocking all access will alienate users and increasingly limit their work-related activities.

This chart shows how often these new forms of communication are used in different organizations. Many organizations use social media platforms as part of their company communication channels, issuing company news on Twitter or maintaining a company profile on Facebook, for example.



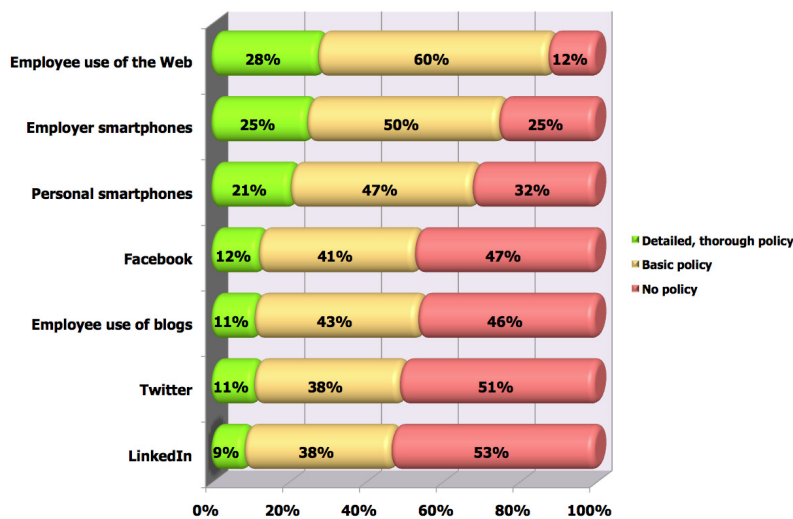
Use of various Web 2.0 tools  
From "The Benefits and Risks of Web 2.0", a whitepaper by Osterman Research

Industry data and research show that users increasingly use the Web and Web 2.0 tools. For example:

- In April 2010, 110 billion minutes were spent on blog and social networking sites. The typical visitor spent two-thirds more time on these sites compared to a year earlier<sup>1</sup>.
- In April 2010, blog and social networking sites attracted 24% more online users compared to a year earlier<sup>2</sup>.
- There are currently 190 million users on Twitter<sup>3</sup>, 519 million users on Facebook<sup>4</sup>, 65 million users on LinkedIn<sup>5</sup> and 115 million on Friendster<sup>6</sup>.

Although social networking tools have a reputation for trivial applications, there are a growing number of useful business applications for social networking and related tools. For example, some rely on these tools for receiving breaking news from trusted colleagues, demonstrating subject-matter expertise to clients and prospects, sending marketing messages, or announcing upcoming webinars and trade show attendance.

These tools can make employees more productive by giving them faster access to information, speeding decision-making, and they can offer companies a distinct competitive advantage. The chart below demonstrates where most organizations are in terms of defining policy controls for the use of these emerging technologies.



Current Organizational Policies for Various Communication Tools  
From "The Benefits and Risks of Web 2.0", a white paper by Osterman Research

Why go to the trouble of developing policy to control new communication technologies like social media? This goes back to the original reasons for developing AUPs—safe working environment, employee productivity and Internet security. Because social media communications are interactive, difficult to detract, and occur in real time, the un-monitored, un-managed use of these tools can increase organizations' liability and reputation risks.

Email today is well-protected and controlled by most organizations. More importantly, employees realize this, so instances of misuse are dropping. However, social media does not use email as a communication vector. It uses Web protocols such as HTTP and HTTPS which are less protected and controlled. Most organizations have a basic form of URL filtering to ensure users do not visit pornographic websites. And in the past, some organizations completely blocked social media sites, but that has changed as these sites are now used as valid business tools.

Because the Web is less controlled, employees are more likely to use it to spread inappropriate material or bully other workers (the site itself is not within the company policy). This is where an appropriately-defined AUP is important—the organization owns the infrastructure used to access and view the site, and therefore has the right to dictate how that infrastructure is used. Keeping employees on task is more difficult today, as, on one hand, they edit the organization's Facebook profile, but they also spend time on their own Facebook site. More than 95% of all malware infections originate on the Web, so secure protection and control is critical to an organization.

A final point about corporate reputation: it takes years to build a good reputation but only seconds to destroy it. The press has reported on employee Facebook or Twitter comments about their bosses, employees—and even customers—as in the following example:

In January 2009, an employee of public relations firm Ketchum used Twitter to post some very unflattering comments about the city of Memphis shortly before presenting to the worldwide communications group at FedEx—Memphis' largest employer. An employee of FedEx discovered the tweet, responded to the tweeter, and then copied FedEx's senior managers, the management of FedEx's communication department and the powers that be at Ketchum.

A senior manager at FedEx responded to this post with the following: "...everyone participating in today's event, including those in the auditorium with you this morning, just received their first pay check of 2009 containing a 5% pay cut...many of my peers and I question the expense of paying Ketchum to produce the video open for today's event; work that could have been achieved by internal, awardwinning professionals with decades of experience in television production."

<http://shankman.com/be-careful-what-you-post/>

The next example highlights the importance of carefully restricting access to a corporation's social media assets:

A homophobic Vodafone UK employee wrote the following message on the company's official Twitter account: "Vodafone UK is fed up of dirty homos and is going after beaver".

According to The Guardian newspaper, this nasty tweet prompted hundreds of users to contact the company to complain. The firm later issued the following press release indicating the message originated from a rogue staff member:

"This afternoon an employee posted an obscene message from the official Vodafone UK Twitter profile. The employee has been suspended immediately and we have started an internal investigation. This was not a hack and we apologise for any offence the tweet may have caused."

The employee faces almost certain dismissal for gross misconduct.

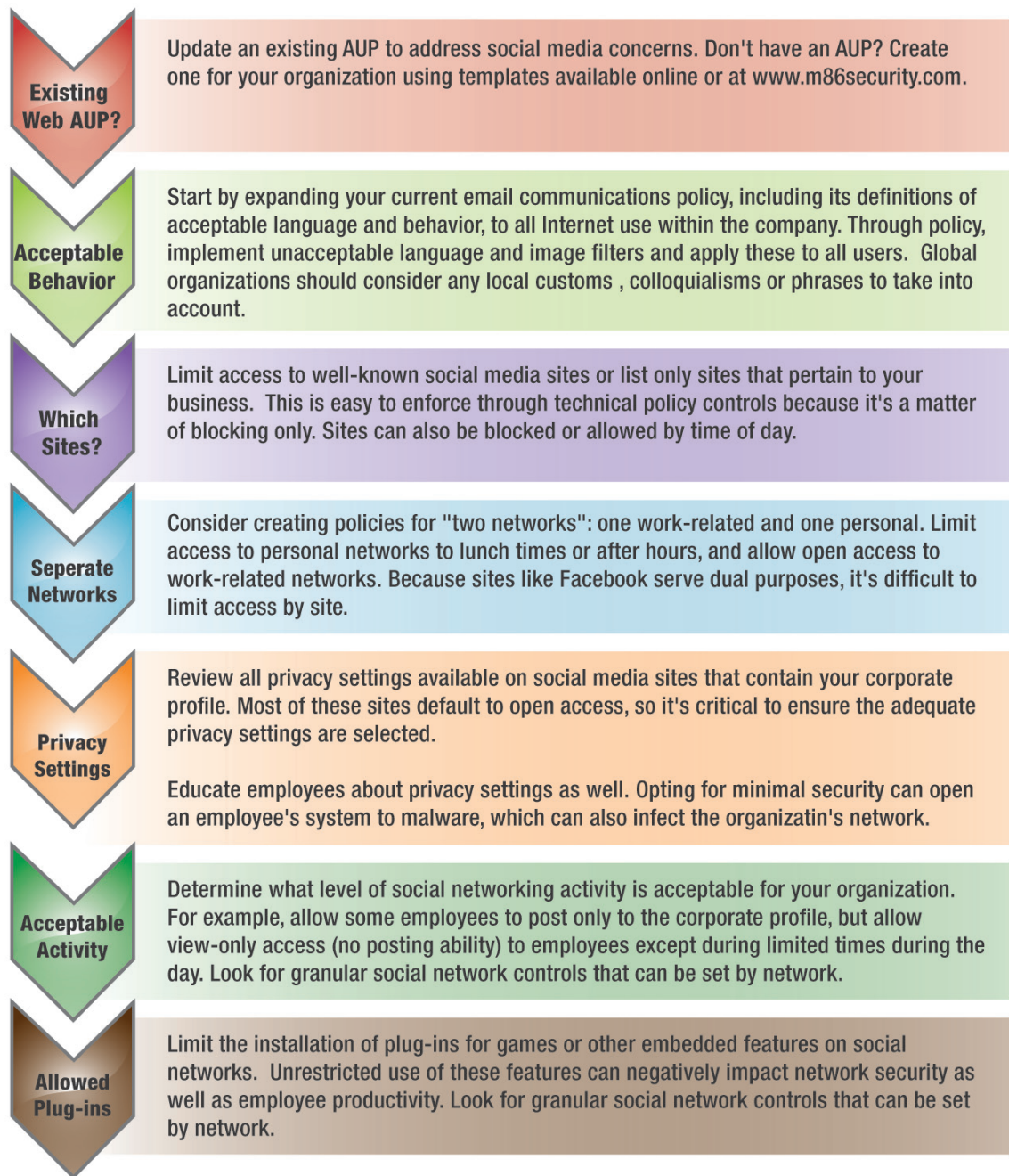
<http://blogs.findlaw.com/solicitor/2010/02/homophobic-employee-causes-vodafone-severe-twitter-embarrassment.html>

Organizations should understand how social media technologies can be used and syndicated before they incorporate them in business activities. This lesson was learned by the UK Conservative party when they launched a website meant to expose the relationship between then UK Prime Minister, Gordon Brown, and a major UK union. The conservatives hoped visitors to the site would use social media to spread the information further, but due to a missing security control on the site, hackers easily re-directed visitors to other websites, including pornographic sites. <http://www.telegraph.co.uk/technology/twitter/7499228/Conservatives-embarrassed-as-hackers-exploit-loophole-on-anti-union-website.html>

One of the major problems with social networking communications is that they are open for other parties to view and indexed by search engines. This means that conversations or tweets can turn up in anyone's search results, allowing other parties to see them, and causing considerable embarrassment and litigation.

## HOW TO MAKE YOUR AUP SOCIAL MEDIA PROOF

The following chart shows how to expand an existing AUP to cover social media use.



These steps ensure that organizations create the most effective AUPs possible, and they help policy makers determine the levels of access and types of content they want to allow their employees to access.

## CONCLUSION

This paper reviewed the importance and use of AUPs for email and Web use. For many organizations, AUPs are especially useful if they enforce them using technical Internet security solutions. Properly extending your AUP to include social media use is critical. Otherwise, organizations risk damage to their reputations, litigation and/or malware attacks. When extending your AUP policies to support social media use, refer to the guidance recommendations and technical enforcement examples outlined in this paper.

## REFERENCES

1. Source: The Nielsen Company, April 2010 (<http://is.gd/cR9GP>)
2. Source: The Nielsen Company, April 2010 (<http://is.gd/cR9GP>)
3. <http://is.gd/cRaJQ4> <http://is.gd/cRaUd>
4. <http://is.gd/cRaYw>
5. <http://is.gd/cRaYw>

## M86 SOLUTIONS FOR ENABLING/ENFORCING AUPs

Developing an AUP is the first step in managing and regulating social media use. AUPs take on more importance when organizations technically enforce them for all users consistently. M86 Security offers innovative solutions that address all Internet security issues, ensure user productivity and provide the reporting and monitoring organizations need.

### Web Security

**M86 Secure Web Gateway** – Appliance and SaaS-based solution that delivers maximum security coverage for organizations across the most vulnerable Web channels, HTTP and HTTPS. Combines proactive malware detection with URL filtering, antivirus scanning, caching and DLP controls to deliver the most effective Web security and productivity solution available on the market today. The SWG includes granular social media controls that provide organizations with control over social media sites.

**M86 WebMarshal** – Software-based secure Web gateway solution delivering advanced capability for employee productivity and policy enforcement. It goes beyond URL filtering to provide comprehensive Web access control and management, complete threat protection (URL, antivirus and malware filtering) and data leakage prevention in a single, policy-based, easy-to-manage and highly scalable solution.

**M86 Web Filter** – Appliance-based solution that enforces and reports on employee Web use with a special emphasis on productivity. The appliance can control which websites users visit, the phrases they search for and provide deeply granular forensic reporting. The Web filter is used to ensure users stay on task and safe when using the Web.

### Email Security

**M86 MailMarshal SMTP** – an email security solution that combines email threat protection, content security, policy enforcement, compliance and data leakage prevention into a highly scalable, flexible, easy-to-manage solution. M86 MailMarshal acts as an email gateway, powered by an unrivalled Defense-in-Depth Anti-Spam Engine, filtering all incoming and outgoing email at the network perimeter.

**M86 MailMarshal Exchange** – one of the few solutions available in the market to provide email management that filters and manages external and internal inbox-to-inbox email for organizations. It monitors and controls internal office email content that travels within an organization to ensure a safe, productive working environment and compliance with acceptable use policies.

**M86 MailMarshal Email Encryption Solutions** – deliver all the email encryption capability organizations are looking for in business to business (B2B) or business to consumer (B2C) modes. The solutions can be deployed automatically through policy set in the base MailMarshal products and ensure that organizations can communicate securely and safely with their customers and business partners.

## ABOUT M86 SECURITY

M86 Security is the global expert in real-time threat protection and the industry's leading Secure Web Gateway provider. The company's hardware, virtual appliance, software, and Software as a Service (SaaS) solutions for Web and email security protect more than 25,000 customers and 26 million users worldwide. M86 products use patented real-time code analysis and behavior-based malware detection technologies as well as threat intelligence from M86 Security Labs to protect networks against new and advanced threats, secure confidential information, and ensure regulatory compliance. The company is based in Irvine, California with international headquarters in London and development centers in California, Israel, and New Zealand. For more information about M86 Security, please visit: [www.m86security.com](http://www.m86security.com).

---

### TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit [www.m86security.com/downloads](http://www.m86security.com/downloads)



**Corporate Headquarters**  
8845 Irvine Center Drive  
Irvine, CA 92618  
United States

Phone: +1 (949) 932-1000  
Fax: +1 (949) 932-1086

**International Headquarters**  
Renaissance 2200  
Basing View, Basingstoke  
Hampshire RG21 4EQ  
United Kingdom

Phone: +44 (0) 1256 848 080  
Fax: +44 (0) 1256 848 060

**Asia-Pacific**  
Suite 3, Level 7, 100 Walker St.  
North Sydney NSW 2060  
Australia

Phone: +61 (0)2 9466 5800  
Fax: +61 (0)2 9466 5899

Version 08/23/11