



Refresh Your AUP

Top Tips to ensure your Acceptable Use Policy is fit for purpose

By Jonathan Naylor, Employed Barrister at Shoosmiths Solicitors

Table of Contents

Introduction	3
Top Tips for an Effective AUP	3
Next Steps	4

Introduction

Your organisation may well have devised and implemented an Acceptable Use Policy ("AUP") some time ago in order to guard against the risks of inappropriate use of computer systems by your workers, but are you confident that your AUP remains "fit for purpose"? This is a landscape in which the threats are constantly changing and you must review your AUP to ensure that it provides a tailored and updated solution.

Top Tips for an Effective AUP

The following tips are the core elements of any effective AUP:

- **Get the correct coverage**

You should ensure that your AUP covers all individuals that are permitted to have access to your organisation's systems, such as temporary workers, self employed consultants, contractors, home workers and agency staff. You should also consider whether you wish to have a comprehensive policy covering all communications equipment, such as telephones, Blackberries, PDAs, fax machines and CCTV, rather than just email and the Internet.

- **Link to your Disciplinary Policy**

Make it clear that a breach of the AUP will be dealt with under the organisation's disciplinary procedure. Be clear about what constitutes inappropriate usage, giving examples such as viewing offensive material, downloading software without authority or sending chain or junk emails. Highlight that in serious cases, breach of the AUP will be deemed to be gross misconduct and may lead to summary dismissal. Give examples of what would constitute gross misconduct, e.g. accessing pornographic material, making defamatory statements about any person or organisation, on line gambling or breaching copyright or confidentiality.

- **Who is responsible for the AUP?**

Ensure that you designate a senior member of the organisation to be responsible for the AUP. This person can then lead the implementation, and any necessary review, of the AUP.

- **Train your managers and staff**

It is not enough to have devised the AUP and distributed it. Staff must understand how it applies to them and managers must appreciate how to implement the AUP. Having an AUP but failing to give line managers sufficient confidence or knowledge to enforce it is a common problem.

- **Make sure that the AUP is non-contractual**

It should be stressed that the AUP, while a corporate policy that must be followed, does not form part of any employee's contract of employment. This will allow your organisation to amend the Policy without the employee's consent if required.

- **Security provisions**

Guidance should be given to workers regarding the secure use of the organisation's computers, such as good password use, locking PC's when a worker is away from their desk and security of lap tops, PDAs or Blackberries when travelling.

Are you confident that your AUP remains "fit for purpose"?

Employers have a responsibility to prevent misuse

- **Explain why monitoring is taking place**

If workers understand the potential risks to themselves and to the business as a whole, they are more likely to accept the monitoring that is adopted. While it is a challenge for employers to persuade members of staff that monitoring usage is necessary to protect workers as much as anything else, there is no doubt that inappropriate use of email and the Internet presents significant risks. Having given workers access to these applications, employers have a responsibility to prevent misuse (and, in doing so, protect employees from the risks associated with such misuse) wherever possible.

- **Good guidance for email usage and etiquette**

For example, this might include setting parameters as to how frequently during a working day workers should access their email and respond to requests. You should also set out that abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory messages will not be permitted.

- **Set boundaries on personal use**

Organisations can take different views regarding the possible limits on personal use of email and the Internet. Will you allow usage only during breaks, after working hours, or at any time provided the amount is reasonable and limited? Will you allow access to Internet chat rooms or message boards? What is your policy on blogging? Will you allow workers to access blogs but provide guidance to them on acceptable content or simply seek to stop them from accessing any such site while at work?

- **Provide for the organisation to have access where needed**

Make it clear that the computer systems are those of the organisation and that staff should have only a limited expectation of privacy. You should make it clear that the organisation will, for example, view an individual's email if they are absent from work and the needs of the business require access to ensure continuous service to a client.

Next Steps

You should review your organisation's AUP against the suggested content set out above and amend if necessary. Specific legal advice should be sought in individual situations.

To find out how MessageLabs Security Services can help enforce your Acceptable Use Policy, visit www.messagelabs.com.au/products/

www.messagelabs.com.au
info_apac@messagelabs.com

Telephone: +61 2 8208 7100

Europe
HEADQUARTERS
1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom

T +44 (0) 1452 627 627
F +44 (0) 1452 627 628

LONDON
3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom

T +44 (0) 207 291 1960
F +44 (0) 207 291 1937

NETHERLANDS
Teleport Towers
Kingsfordweg 151
1043 GR
Amsterdam
Netherlands

T +31 (0) 20 491 9600
F +31 (0) 20 491 7354

BELGIUM / LUXEMBOURG
Culliganlaan 1B
B-1831 Diegem
Belgium

T +32 (0) 2 403 12 61
F +32 (0) 2 403 12 12

DACH
FeringasträÙe 9
85774 Unterföhring
Munich
Germany

T +49 (0) 89 189 43 990
F +49 (0) 89 189 43 999

© MessageLabs 2008
All rights reserved

Americas
AMERICAS HEADQUARTERS
512 Seventh Avenue
6th Floor
New York, NY 10018
USA

T +1 646 519 8100
F +1 646 452 6570

CENTRAL REGION
7760 France Avenue South
Suite 1100
Bloomington, MN 55435
USA

T +1 952 886 7541
F +1 952 886 7498

Asia Pacific
HONG KONG
1601
Tower II
89 Queensway
Admiralty
Hong Kong

T +852 2111 3650
F +852 2111 9061

AUSTRALIA
Level 6
107 Mount Street,
North Sydney
NSW 2060
Australia

T +61 2 8208 7100
F +61 2 9954 9500

SINGAPORE
Level 14
Prudential Tower
30 Cecil Street
Singapore 049712

T +65 62 32 2855
F +65 6232 2300