MessageLabs®

Be certain

# ePolicy Best Practices

*A Business Guide to Clean & Compliant, Safe & Secure E-Mail and Web Usage and Content*

by
Nancy Flynn, Executive Director, The ePolicy Institute, for MessageLabs

# Table of Contents


**Preface**

The ePolicy Institute™, www.epolicyinstitute.com, and MessageLabs, www.messagelabs.com, have created this business guide to provide best-practices guidelines for developing and implementing effective E-Mail and Web Acceptable Usage Policies for the UK workplace. Through the implementation of clearly written Acceptable Usage Policies, employers in the UK can maximize employee compliance while minimizing the likelihood of litigation, regulatory investigations, security breaches, malicious intruders, and other electronic disasters.

The ePolicy Institute/MessageLabs Guidebook, ***ePolicy Best Practices: A Business Guide to Clean & Compliant, Safe & Secure E-Mail and Web Usage and Content*** is produced as a general best-practices guide with the understanding that neither the author (Nancy Flynn, Executive Director of The ePolicy Institute), nor the publisher (MessageLabs) is engaged in rendering advice on legal, regulatory, or other issues. Before acting on any issue, rule, or policy addressed in ***ePolicy Best Practices: A Business Guide to Clean & Compliant, Safe & Secure E-Mail and Web Usage and Content***, you should consult with legal counsel or other professionals competent to review the relevant issue.

**ePolicy Best Practices: A Business Guide to Clean & Compliant, Safe & Secure E-Mail and Web Usage and Content** is based on material excerpted from author Nancy Flynn's books E-Mail Rules, Blog Rules, Instant Messaging Rules, The ePolicy Handbook, Writing Effective E-Mail, and E-Mail Management.

**The ePolicy Institute** is a leading source of speaking, training, and consulting services related to workplace e-mail/Web/blog/IM risks, policies, and management. The US-based ePolicy Institute is dedicated to helping employers limit e-mail and Web risks, including litigation and regulatory investigations, while enhancing employees' electronic communications skills. Visit www.epolicyinstitute.com to learn more.

"….any time you allow employees to access the Web and e-mail, you put your organization's assets, future, and reputation at risk."

**Why Establish Acceptable Usage Policies Governing E-Mail & Web Use and Content?**

Whether your organization is a mid-sized company, a small family business, or a publicly traded corporation, any time you allow employees to access the Web and e-mail, you put your organization's assets, future, and reputation at risk. Accidental misuse—and intentional abuse—of e-mail and the Internet can create potentially costly and time-consuming legal, regulatory, security, and productivity headaches for employers of all sizes in all industries.

Best Advice: Manage your organization's e-mail and Web liabilities today with clearly written Acceptable Usage Policies supported by comprehensive, company wide employee training and policy-based monitoring and management technology tools—or risk potentially costly and protracted disaster tomorrow.

**Put Best Practices to Work With Policy, Training, and Technology**

Organizations that are committed to preventing accidental and intentional e-mail and Web disasters put best practices to work by combining the *"3-Es"* of electronic risk management: (1) Establish policy; (2) Educate the workforce; (3) Enforce policy with discipline and technology.

**1. Establish comprehensive, clearly written e-mail and Web Acceptable Usage Policies for all employees, from entry-level staff to senior executives.** Make sure Acceptable Usage Policies are easy for employees to access, understand, and adhere to. Avoid vague language that leaves policies open to individual interpretation. Update e-mail and Web Acceptable Usage Policies annually to ensure that you respond to evolving laws governing privacy and the Internet; address "emerging" technologies like instant messaging; and adhere to regulatory rules impacting your business and industry.

***ePolicy Tip**: Because some employees tend to play it "fast and loose" with language and content when e-mailing friends and family, be sure to incorporate rules governing personal e-mail use in your Acceptable Usage Policy. Spell out exactly how much personal e-mail is allowed, when, with whom, under what circumstances, and for how long. Use clear language to communicate specific personal use guidelines. Don't leave room for individual interpretation by employees who might be tempted to engage in excessive personal correspondence on company time.*

**2. Educate Employees.** Should you ever need to terminate an employee for e-mail or Web misuse, your Acceptable Usage Policy, coupled with formal employee education, could be enough to convince an Employment Tribunal that the employee's dismissal was based on legitimate grounds and a fair process.

***ePolicy Tip:*** *Introduce Acceptable Usage Policies during mandatory training covering e-mail and Web risks, rights, rules, regulations, and responsibilities. For a large or geographically disperse workforce, consider a combination of on-site, online, and video training sessions. Build quizzes into training to certify that employees have participated, understand the risks and rules, and agree to comply with e-mail and Web Acceptable Usage Policies—or accept the consequences up to and including termination. Ensure 100% participation by stripping e-mail and Web privileges from any employee who fails to complete training. Repeat the training and certification process annually as part of your annual review of Acceptable Usage Policies.*

**3. Enforce Policy.** Many employers find that the best way to manage people problems is through the application of technology solutions. If you have any doubt about your employees' willingness to adhere to e-mail and Web usage and content rules, visit MessageLabs, www.messagelabs.com/content, to review policy-based management and monitoring technology solutions designed to help maximize employee compliance while minimizing workplace risks.

"Don't allow employees to dismiss Acceptable Usage Policies as insignificant or unenforceable."

***ePolicy Tip:*** *Don't allow employees to dismiss Acceptable Usage Policies as insignificant or unenforceable. Take the lead from employers worldwide who increasingly are "putting teeth" in ePolicies. For examples, 26% of US bosses have fired Internet abusers, and another 26% have dismissed e-mail violators. Employers in the UK have the legal right to dismiss e-mail and Web violators—but must clearly demonstrate adherence to a fair process. If Acceptable Usage Policies are not clearly written and effectively communicated, then an Employment Tribunal may rule the dismissal of an e-mail or Web violator is unfair. Don't leave policy enforcement—and legitimate disciplinary action—to chance. Establish clear policy, educate all employees, and maximize compliance with policy-based monitoring and management technology tools.*

***Sources:*** *2005 Electronic Monitoring & Surveillance Survey and 2006 Workplace E-Mail, IM & Blog Survey from American Management Association and The ePolicy Institute; and Jonathan Naylor, Morgan Cole Solicitors.*

**Ban Inappropriate Web Sites to Preserve Resources and Productivity**

Use written Acceptable Usage Policies to alert employees that they are prohibited from viewing, downloading, uploading, forwarding, printing, copying, or filing sexually explicit or otherwise objectionable, non-business-related Web content. Outlaw wasteful and potentially risky activities including visiting online dating sites, playing games, participating in chat rooms, gambling, shopping, and downloading streaming audio, video and other bandwidth-wasting files. Support written Web rules—and enforce employee compliance—with employee training program backed by policy-based monitoring and management technology tools, www.messagelabs.com/content, designed to review and restrict inappropriate online behaviour.

"Because UK law respects employee privacy, employers must be up-front about computer monitoring."

***ePolicy Tip**: Because UK law respects employee privacy, employers must be up-front about computer monitoring. While the law allows employers to monitor Web surfing and e-mail transmissions, employers are obligated to notify employees they are being watched and use the least intrusive surveillance method possible. Use clearly written, comprehensive Acceptable Usage Policies to notify employees of monitoring policies and procedures. Let employees know exactly why you are monitoring, precisely what type of violations you are looking for, and specifically how monitoring technology works. Apply these best practices to satisfy employees who are concerned about privacy and Employment Tribunals that will closely examine e-mail and Web Acceptable Usage Policies and monitoring procedures in response to wrongful termination claims. Source: Jonathan Naylor, Morgan Cole Solicitors.*

**Control E-Mail Risk by Controlling Written Content**

Good e-mail is businesslike and free of obscene, pornographic, sexual, harassing, menacing, defamatory, threatening, or otherwise offensive language and content. Good e-mail is well-written and adheres to the rules of netiquette, or electronic etiquette. Reduce e-mail risks by incorporating content rules that govern text, art, photos, cartoons, and other graphics into your e-mail policy. Don't forget to ban jokes, gossip, rumours, innuendoes, and disparaging remarks that can lead to misunderstandings, hurt feelings, and legal claims. Many employers find content is best managed by policy-based technology tools that monitor and filter messages that violate written policy, while protecting the system from spam, viruses, Trojan horses, worms, spyware, hackers, and other malicious intruders. Visit www.messagelabs.com/content for more information.

**Top 10 Best Practices to Maximize Compliance and Minimize E-Mail & Web Risk**

**1. Put Acceptable Usage Policies In Writing.** Don't rely on e-mail or the Intranet alone to inform employees of e-mail and Web policies and procedures. Distribute a hard copy of each policy to every employee. Require employees to sign and date each policy, acknowledging they have read it, understand it, and agree to comply with it or accept the consequences, up to and including termination.

**2. Educate Employees About Risks, Policies, and Compliance**. Don't assume employees understand e-mail and Web risks, and don't expect untrained employees to comply with Acceptable Usage Policies. Because you may one day need to demonstrate your commitment to formal, companywide training to an Employment Tribunal, be sure to enforce mandatory training by revoking the e-mail and Web privileges from those who skip training.

**3. Establish E-Mail Business Record Retention Guidelines.** Should you ever face a workplace lawsuit, e-mail business records will be subpoenaed as evidence. As part of your strategic e-mail management and Acceptable Usage Policy program, be sure to define "e-mail business record" for your organization. Based on that definition, consistently apply formal retention rules, policies, procedures, and schedules to business-related/business record e-mail.

**4. Set Rules for Personal Use.** Use Acceptable Usage Policies to spell out exactly how much personal e-mail use and Web surfing is allowed, when, with whom, and under what circumstances. Be clear. Use specific language to prevent misunderstandings or individual interpretation of policy.

**5. Recap Harassment, Discrimination, Ethics, Confidentiality, Security, and Other Policies**. Company policy is company policy, regardless of the communications tool employed. Make sure employees understand that all company policies—including but not limited to those governing harassment, discrimination, ethics, confidentiality, and security—apply to e-mail and Web use and content.

**6. Stress Compliance with Sexual Harassment Policy.** Because of the relaxed, informal nature of e-mail, some employees will write comments they would never say aloud. Make sure employees understand that, regardless of how it is transmitted, an inappropriate comment is an inappropriate comment. All it takes is one off-colour joke, "naughty" photo, sexually charged cartoon, or otherwise offensive message to trigger an expensive, protracted legal claim.

**7. Address Monitoring and Privacy.** Under UK law, employers must respect employee privacy. Use clearly written, comprehensive Acceptable Usage Policies to notify employees—in clear and specific detail—of the organization's monitoring policies and practices, which by law must be as unobtrusive as possible.

**8. Enforce Content Rules.** Communicate the fact that e-mail and the Web are to be used primarily as business communications tools. Clearly define approved and banned language and content. Insist that employees behave professionally and adhere to the rules of civil business behaviour, also known as "netiquette" or electronic etiquette, when using the organization's e-mail and Internet systems.

**9. Support Acceptable Usage Policies with Technology.** Because accidents happen (and disgruntled employees occasionally trigger intentional disasters), it's impossible to ensure 100% compliance. Support written rules with policy-based management technology tools, www.messagelabs.com/content, designed to monitor and filter content, block access to inappropriate sites, and lock out malicious intruders.

**10. Don't Allow Employees to Dismiss Policy as Unenforceable.** Make sure employees understand that their computer activity may be monitored. Stress the fact that policy violators will face disciplinary action that may include termination. Let employees know you mean business by enforcing your e-mail and Web Acceptable Usage Policies consistently among all employees, regardless of rank or title.

***ePolicy "Bonus" Tip:*** *Before introducing e-mail and Web Acceptable Usage Policies to employees, be sure to have your legal counsel review and sign off on each policy. Make sure policies address every potential risk facing your organization and industry. Be certain policies and procedures are in compliance with UK laws governing monitoring and privacy. If you operate within a regulated industry, ensure that your policies comply with regulatory rules. Make sure policies are clearly written and training programs effectively communicate the company's policies and procedures. Your up-front investment in a legal review of e-mail and Web Acceptable Usage Policies will pay huge dividends should you one day face an Employment Tribunal in the course of a wrongful termination claim or other employment action.*

**Sample Web Acceptable Usage Policy**

The company is pleased to offer associates access to the organization's computer Network and the Internet. This Policy applies to employees granted Network and Internet access by the Company. For the Company to continue making Network and Internet access available, employees must behave appropriately and lawfully. Upon acceptance of your account information and agreement to follow this Policy, you will be granted Network and Internet access in your office. If you have any questions about the provisions of this Policy, you should contact the Chief Information Officer.

If you or anyone you allow to access your account (itself a violation of this Policy) violates this Policy, your access will be denied or withdrawn. In addition, you may be subject to disciplinary action, up to and including termination.

**1. Personal Responsibility**

By accepting your account password and related information, and accessing the Company's Network or Internet system, you agree to adhere to this Policy. You also agree to report any Network or Internet misuse to the Chief Information Officer. Misuse includes Policy violations that harm another person or another individual's property.

**2. Term of Permitted Use**

Network and Internet access extends throughout the term of your employment, provided you do not violate the organization's Computer Network and Internet Acceptable Usage Policy. Note: The Company may suspend access at any time for technical reasons, Policy violations, or other concerns.

**3. Purpose and Use**

The Company offers access to its Network and Internet system for business purposes only. If you are unsure whether an activity constitutes appropriate business use, consult the Chief Information Officer.

**4. Netiquette Rules**

Employees must adhere to the rules of Network etiquette, or Netiquette. In other words, you must be polite, adhere to the organization's electronic writing and content guidelines, and use the Network and Internet appropriately and legally. The Company will determine what materials, files, information, software, communications, and other content and activity are permitted or prohibited, as outlined below.

**5. Banned Activity**

The following activities violate the Company's Computer Network and Internet Acceptable Usage Policy:

(A) Using, transmitting, receiving, or seeking inappropriate, offensive, vulgar, suggestive, obscene, abusive, harassing, belligerent, threatening, defamatory (harming another person's reputation by lies), or misleading language or materials.

(B) Revealing personal information, such as the home address, telephone number, or financial data of another person or yourself.

(C) Making ethnic, sexual-preference, or gender-related slurs or jokes.

(D) Engaging in illegal activities, violating the Employee Handbook, or encouraging others to do so. Examples:

1. Selling or providing substances prohibited by the Company's employment policy or the Employee Handbook.
2. Accessing, transmitting, receiving, or seeking unauthorized, confidential information about clients or colleagues.
3. Conducting unauthorized business.
4. Viewing, transmitting, downloading, or searching for obscene, pornographic, or illegal materials.
5. Accessing others' folders, files, work, networks, or computers. Intercepting communications intended for others.
6. Downloading or transmitting the organization's confidential information or trade secrets.

(E) Causing harm or damaging others' property. Examples:

1. Downloading or transmitting copyrighted materials without permission from the copyright holder. Even when materials on the Network or the Internet are not marked with the copyright symbol, ©, employees should assume all materials are protected under copyright laws—unless explicit permission to use the materials is granted.
2. Using another employee's password to trick recipients into believing someone other than you is communicating or accessing the Network or Internet.
3. Uploading a virus, harmful component, or corrupted data. Vandalizing the Network.
4. Using software that is not licensed or approved by the Company.

(F) Jeopardizing the security of access, the Network, or other Internet Networks by disclosing or sharing passwords and/or impersonating others.

(G) Accessing or attempting to access controversial or offensive materials. Network and Internet access may expose employees to illegal, defamatory, inaccurate, or offensive materials. Employees must avoid these sites. If you know of employees who are visiting offensive or harmful sites, report that use to the Company's Chief Information Officer.

(H) Engaging in commercial activity. Employees may not sell or buy anything over the Internet. Employees may not solicit or advertise the sale of any goods or services. Employees may not divulge private information — including credit card numbers and other financial data — about themselves or others.

(I) Wasting the Company's computer resources. Specifically, do not waste printer toner or paper. Do not send electronic chain letters. Do not send e-mail copies to nonessential readers. Do not send e-mail to group lists unless it is appropriate for everyone on a list to receive the e-mail. Do not send organization-wide e-mails without your supervisor's permission.

(J) Encouraging associates to view, download, or search for materials, files, information, software, or other offensive, defamatory, misleading, infringing, or illegal content.

**6. Confidential Information**

Employees may have access to confidential information about the Company, our employees, and clients. With the approval of management, employees may use e-mail to communicate confidential information internally to those with a need to know. Such e-mail must be marked "Confidential." When in doubt, do not use e-mail to communicate confidential material. When a matter is personal, it may be more appropriate to send a hard copy, place a phone call, or meet in person.

**7. Privacy**

Network and Internet access is provided as a tool for our organization's business. The Company has the legal right to monitor usage of the Network and the Internet, using the least intrusive method available. When monitoring is deemed necessary, employees will be notified of management's decision to monitor, will be provided with details of what is being monitored, why and how.

**8. Non-compliance**

Your use of the Network and the Internet is a privilege, not a right. Violate this policy and, at minimum, your access to the Network and the Internet will be terminated, perhaps for the duration of your tenure with the Company. Policy breaches include violating the above provisions, and failing to report violations by other users. Permitting another person to use your account or password to access the Network or the Internet—including but not limited to someone whose access has been denied or terminated—is a violation of Policy. Should another user violate this Policy while using your account, you will be held responsible, and both of you will be subject to disciplinary action.

**A.1 Employee Acknowledgment**

Note: If you have questions or concerns about this ePolicy, contact the Company's Chief Information Officer before signing this agreement.

I have read the Company's Computer Network and Internet Acceptable Usage Policy and agree to abide by it. I understand violation of any of the above terms may result in discipline, up to and including my termination.

| _____ | _____ | _____ |
|---|---|---|
| Employee Name (Printed) | Employee Signature | Date |

**Sample E-Mail Acceptable Usage Policy**

The Company provides employees with electronic communications tools, including an E-Mail System. This written E-Mail Acceptable Usage Policy, which governs employees' use of the Company's E-Mail system, applies to e-mail use at the Company's headquarters and district offices, as well as at remote locations, including but not limited to employees' homes, airports, hotels, client and supplier offices. The Company's e-mail rules and policies apply to full-time employees, part-time employees, independent contractors, interns, consultants, suppliers, clients, and other third parties. Any employee who violates the Company's e-mail rules and policies is subject to disciplinary action, up to and including termination.

**E-Mail Exists for Business Purposes.**

The Company allows e-mail access primarily for business purposes. Employees may use the Company's e-mail system for personal use only in accordance with this policy. Employees are prohibited from using personal e-mail software (Hotmail, etc.) for business or personal communications at the office.

**Authorized Personal Use of E-Mail.**

Employees may use e-mail to communicate with spouses, children, domestic partners, and other family members. Employees' personal use of e-mail is limited to lunch breaks and work breaks only. Employees may not use e-mail during otherwise productive business hours.

Employees are prohibited from using e-mail to operate a business, conduct an external job search, solicit money for personal gain, campaign for political causes or candidates, or promote or solicit funds for a religious or other personal cause.

**Privacy.**

The Company has the legal right to monitor usage of the e-mail system, using the least intrusive method available. When monitoring is deemed necessary, employees will be notified of management's decision to monitor, will be provided with details of what is being monitored, why and how.

**Offensive Content and Harassing or Discriminatory Activities Are Banned.**

Employees are prohibited from using e-mail to engage in activities or transmit content that is harassing, discriminatory, menacing, threatening, obscene, defamatory, or in any way objectionable or offensive. Employees are prohibited from using e-mail to:

- Send, receive, solicit, print, copy, or reply to text or images that disparage others based on their race, religion, colour, sex, sexual orientation, national origin, veteran status, disability, ancestry, or age.

- Send, receive, solicit, print, copy, or reply to jokes (text or images) based on sex, sexual orientation, race, age, religion, national origin, veteran status, ancestry, or disability.

- Send, receive, solicit, print, copy, or reply to messages that are disparaging or defamatory.

- Spread gossip, rumours, and innuendos about employees, clients, suppliers, or other outside parties.

- Send, receive, solicit, print, copy, or reply to sexually oriented messages or images.

- Send, receive, solicit, print, copy, or reply to messages or images that contain foul, obscene, off-colour, or adult-oriented language.

- Send, receive, solicit, print, copy, or reply to messages or images that are intended to alarm others, embarrass the Company, negatively impact employee productivity, or harm employee morale.

**Confidential, Proprietary, and Personal Information Must Be Protected.**

Unless authorized to do so, employees are prohibited from using e-mail to transmit confidential information to outside parties. Employees may not access, send, receive, solicit, print, copy, or reply to confidential or proprietary information about the Company, employees, clients, suppliers, and other business associates.

Confidential information includes but is not limited to client lists, credit card numbers, employee performance reviews, salary details, trade secrets, passwords, and information that could embarrass the Company and employees were it to be made public.

**Business Record Retention.**

E-mail messages create written business records, and are subject to the Company's written and consistently applied rules and policies for retaining and deleting business records. See the Company's electronic business record retention policy for more information.

**Violations.**

These guidelines are intended to provide Company employees with general examples of acceptable and unacceptable use of the Company's e-mail system. A violation of this policy may result in disciplinary action up to and including termination.

**Acknowledgement.**

If you have questions about the above policies and procedures, address them to the Compliance Officer before signing the following agreement.

I have read the Company's E-Mail Acceptable Usage Policy and agree to abide by it. I understand that a violation of any of the above policies and procedures may result in disciplinary action, up to and including my termination.

_____

User Name

_____

User Signature

_____

Date

**The ePolicy Institute**

**www.epolicyinstitute.com**

The ePolicy Institute is dedicated to helping employers limit electronic risks, including litigation, through the development and implementation of Acceptable Usage Policies and employee training programs. An international speaker and trainer, Executive Director Nancy Flynn is the author of 8 books published in 4 languages. As a recognized authority on workplace e-mail and Web usage, Nancy Flynn is a popular media source who has been interviewed by *Fortune, Financial Times, The Wall Street Journal, US News & World Report, Business Week, USA Today, New York Times*, National Public Radio, CNBC, CNN, CBS, ABC, and Fox News among others. ***ePolicy Best Practices: A Business Guide to Clean & Compliant, Safe & Secure E-Mail and Web Usage and Content*** is based on material excerpted from author Nancy Flynn's books *E-Mail Rules, Blog Rules*, *Instant Messaging Rules, The ePolicy Handbook*, *Writing Effective E-Mail,* and *E-Mail Management*.

**MessageLabs**

**www.messagelabs.com**

MessageLabs is a leading provider of integrated messaging and web security services, with over 14,000 clients ranging from small business to the Fortune 500 located in more than 80 countries. MessageLabs provides a range of managed security services to protect, control, encrypt and archive communications across Email, Web and Instant Messaging.

These services are delivered by MessageLabs globally distributed infrastructure and supported 24/7 by security experts. This provides a convenient and cost-effective solution for managing and reducing risk and providing certainty in the exchange of business information.

Every day, huge amounts of information move in and out of organizations via email and the Web. If business-critical information were to fall into the wrong hands, it could cost a company its existence. MessageLabs Control services help you enforce your email, web and IM usage policies and help ensure regulatory compliance by controlling both image and text-based email content.

**www.messagelabs.com**
**info@messagelabs.com**

Freephone UK
0800 917 7733

Toll free US
1-866-460-0000


**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**
Cullinganlaan 1B
B-1831 Diegem
Belgium

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

**DACH**
Feringastraße 9
85774 Unterföhring
Munich
Germany

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





**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