QMS MEDIA PTY LTD

SOCIAL MEDIA & IT POLICY

INTRODUCTION

QMS Media Pty Ltd (**QMS**) has established a policy with regards to access and disclosure of electronic mail messages or information created, sent or received by Company employees and contractors using the company's information technology systems ("**IT systems**").

All users must accept full responsibility for using the Company's IT systems in an honest, ethical and legal manner and with regard to the privacy, rights and sensitivities of other people. Use must be in accordance with Company policies and all relevant federal and state legislation. Such legislation shall include, but not be limited to legislation covering privacy, copyright, freedom of information, equal employment opportunity, intellectual property and occupational health and safety.

QMS also expects its employees to maintain a certain standard of behaviour when using Social Media for work or personal purposes.

Social Media includes all internet-based publishing technologies. Most forms of Social Media are interactive, allowing authors, readers and publishers to connect and interact with one another. The published material can often be accessed by anyone.

Forms of Social Media include, but are not limited to, social or business networking sites (i.e. Facebook, LinkedIn), video and/or photo sharing websites (ie. YouTube, Instagram), business/corporate and personal blogs, micro-blogs (i.e Twitter), chat rooms and forums.

For the purposes of this policy, the following guidelines apply:

USE OF IT SYSTEMS

The Company IT systems are provided to assist employees and other authorised users to assist in the conduct of business for the Company

Users are permitted to use IT systems for limited and reasonable personal use. However, any such personal use must not impact upon the User's work performance or Company resources or violate this policy or any other Company policy.

A User must not use Company systems for personal use if that use interferes with the efficient business operations of the Company or relates to a personal business of the User.

The Company gives no warranty or assurance about the confidentiality or privacy of any personal information disclosed by any User in the course of using the computer network or systems for the User's personal purposes.

REQUIREMENTS FOR USE

Users are responsible for:

- all activities which originate from their account;
- all information sent from, intentionally requested, solicited or viewed from their account;
- publicly accessible information placed on a computer using their account.

Users must:

- show restraint in the consumption of resources;
- respect intellectual property and the ownership of data and software;
- respect other's rights to privacy and freedom from intimidation, harassment and annoyance;
- abide by the Company's policies

No user shall:

- attempt to subvert the security of any of the Company's IT systems;
- attempt to create or install any form of malicious software (for example worms, viruses, sniffers) which may affect computing or network equipment, software or data;
- attempt to interfere with the operation of any of the Company's IT systems;
- attempt to subvert any restriction or accounting control of any of the Company's IT system
- attempt unauthorised access to any Company IT systems or files/drives without express permission of the holder;
- send an e-mail in the name of another person without the other person's express permission and unless the action is authorised by your manager;
- create or transmit any material or data which could reasonably be deemed abusive, offensive, obscene, defamatory or indecent;
- upload or download copyrighted materials, trade secrets, proprietary financial information, or similar and confidential materials of the company without prior authorisation;
- use the Company IT systems for unauthorised private gain or for financial gain to a third party.

EMAIL & INTERNET USE

All emails composed, sent or received on the IT system are and remain the property of the company. They are not the private property of any employee and/or contractor.

You must be aware that e-mails, unlike internal telephone calls, create a permanent written record of communications. E-mails containing commercially sensitive material written to customers, suppliers or other stakeholders must be approved by your Manager. If in doubt, do not send any e-mail.

Staff may not use internet or email access provided by the Company to:

- create or exchange messages that are offensive, harassing, obscene or threatening;
- visit web sites containing objectionable (including pornographic) or criminal material;
- exchange any confidential or sensitive information held by the Company (unless in the authorised course of their duties);
- create, store or exchange information in violation of copyright laws (including the uploading or downloading of commercial software, games, music or movies);

- use internet-enabled activities such as gambling, gaming, conducting a business or conducting illegal activities;
- create or exchange advertisements, solicitations, chain letters and other unsolicited or bulk email;
- use the computers to play games in work time.

PERSONAL MOBILE DEVICES FOR BUSINESS USE

The Company acknowledges the importance of mobile technologies in improving business communication and productivity. Personal mobile devices can only be used for business purposes provided you agree to abide by the Company's IT policy for appropriate use and access.

All employees who have a personal mobile device for business use acknowledge that the Company:

- owns all intellectual property created for business purposes on the device;
- has first right to buy the device where the employee wants to sell the device;
- has the right to deregister the device for business use at any time.

PRIVACY, CONFIDENTIALITY & SECURITY

The Company seeks to comply with privacy requirements and confidentiality in the provision of all IT Services, but privacy and confidentiality cannot be assured.

The Company reserves and intends to exercise the right to review, audit intercept, access and disclose all messages created, received or sent over the IT system for any purpose including when investigating system problems or potential security violations, and to maintain system security and integrity, maintain business continuity and prevent, detect or minimise unacceptable behaviour on that facility. The contents of which may be examined without the permission of the employee and/or contractor.

Notwithstanding the company's right to retrieve and read any electronic mail messages or information, such messages or information should be treated as confidential by other employees and/or contractors and accessed only by the intended recipient. Employees and/or contractors are not authorised to retrieve or read any e-mail messages or information that are not sent to them.

SOCIAL MEDIA

PROFESSIONAL USE OF SOCIAL MEDIA

Overview

This section of the policy applies to all employees who contribute to or perform duties such as:

- maintaining a profile page for QMS on any social or business networking site (including, but not limited to LinkedIn, Facebook, Instagram, Youtube or Twitter);
- making comments on such networking sites for and on behalf of QMS;
- writing or contributing to a blog and/or commenting on other people’s or business’ blog posts for and on behalf of QMS; and/or
- posting comments for and on behalf of QMS on any public and/or private web-based forums or message boards or other internet sites.

Procedure

No employee of QMS is to engage in Social Media as a representative or on behalf of QMS unless they first obtain written approval from the Group's Chief Marketing Officer.

If any employee of QMS is directed to contribute to or participate in any form of Social Media related work, they are to act in a professional manner at all times and in the best interests of QMS.

All employees of QMS must ensure they do not communicate any:

- confidential information relating to QMS or its clients, business partners or suppliers;
- material that violates the privacy or publicity rights of another party; and/or
- information, (regardless of whether it is confidential or public knowledge), about clients, business partners or suppliers of QMS without their prior authorisation or approval to do so; on any social or business networking sites, web-based forums or message boards, or other internet sites.

Confidential Information includes any information in any form relating to QMS and related bodies, clients or businesses, which is not in the public domain.

PRIVATE / PERSONAL USE OF SOCIAL MEDIA

QMS acknowledges its employees have the right to contribute content to public communications on websites, blogs and business or social networking sites not operated by QMS. However, inappropriate behaviour on such sites has the potential to cause damage to QMS as well as its employees, clients, business partners and/or suppliers.

Procedure

All employees of QMS must refrain from posting, sending, forwarding or using, in any way, any inappropriate material including but not limited to material which:

- is intended to (or could possibly) cause insult, offence, intimidation or humiliation to QMS or its clients, business partners or suppliers;
- is defamatory or could adversely affect the image, reputation, viability or profitability of QMS or its clients, business partners or suppliers; and/or
- contains any form of Confidential Information relating to QMS or its clients, business partners or suppliers

BREACH OF POLICY

All employees of QMS must comply with this policy.

Any reported, alleged or apparent incidences of breach of this policy may be subject to an investigation, with appropriate action taken in accordance on the outcome of the investigation.

All employees are advised that breaches of this policy will result in disciplinary action, which may include immediate dismissal. It may also expose you to personal liability.

REVIEW OF POLICY

This policy will be reviewed as required having regard to the changing circumstances of QMS Media and to ensure continued compliance.

Developed: 1st July 2015
Reviewed: 12th July 2023