Social Media

This policy on social media applies to all employees. Social media is the collective term referring to social and professional networking sites (for example Facebook, LinkedIn, Twitter), blogs, boards and other similar online fora and the policy extends to all such sites and incorporates any future developments of such media. Breaches of this policy will be investigated, and the company retains the right to take disciplinary action, up to and including dismissal.

This policy applies to personal social media usage. Employees who have access to Mitie social media accounts for official company purposes must refer to the company's terms of usage which apply to such accounts.

All IT resources are the company's property dedicated to achieving our business objectives. Inappropriate use is not acceptable. Excessive activity is not permitted. Personal use must not interfere with your work commitments.

A limited amount of personal use of the internet and social media is permitted on the company's equipment, provided the following rules are observed:

- Personal use must not occur during working time, but instead must occur during break time and outside of your normal working hours.
- Personal use must comply with the requirements and general principles of this policy and all other internet, IT, security and data protection policies.

Applies to All Employees

Mitie recognises that employees use social media tools as part of their daily lives. Employees should always be mindful of what they are posting, who can see it, and how it can be linked back to the company and work colleagues.

All employees should be aware that the company regularly monitors the internet and social media in reference to its work and to keep abreast of general internet commentary, brand presence and industry/customer perceptions. The company does not specifically monitor social media sites for employee content on an ongoing basis, however employees should not expect privacy in this regard. Mitie reserves the right to utilise for disciplinary purposes any information that could have a negative effect on the company or its employees, which management comes across in regular internet monitoring, or is brought to the company's attention by employees, customers, members of the public, etc.

All employees are prohibited from using or publishing information on any social media sites, where such use has the potential to negatively affect Mitie or its employees. Examples of such behaviour include, but are not limited to:

- Publishing material that is defamatory, abusive or offensive in relation to any employee, manager, office holder, shareholder, customer or client of Mitie.
- Publishing any confidential or business-sensitive information about Mitie.
- Publishing material that might reasonably be expected to have the effect of damaging the reputation or professional standing of the company.

Rules Regarding Usage

All employees must adhere to the following when engaging in social media.

- Be aware of your association with the company when using online social networks. You must always identify yourself and your role if you mention or comment on the company. Where you identify yourself as an employee, ensure your profile and related content is consistent with how you would present yourself with colleagues and clients. You must write in the first person and state clearly that the views expressed are your own and not those of the organisation. Wherever practical, you must use a disclaimer saying that while you work for the organisation, anything you publish is your personal opinion, and not necessarily the opinions of the company.

- You are personally responsible for what you post or publish on social media sites. Where it is found that any information breaches any policy, such as breaching confidentiality or bringing the company into disrepute, you may face disciplinary action up to and including dismissal.

- Be aware of data protection rules – you must not post colleagues' details or pictures without their individual permission. Photographs of company events should not be posted online. Employees must not provide or use their company password in response to any internet request for a password.

- Material in which the company has a proprietary interest – such as software, products, documentation or other internal information – must not be transmitted, sold or otherwise divulged, unless Mitie has already released the information into the public domain. Any departure from this policy requires the prior written authorisation of your senior manager.

- Be respectful at all times, in both the content and tone of what you say. Show respect to your audience, your colleagues and customers and suppliers. Do not post or publish any comments or content relating to the company or its employees, which would be seen as unacceptable in the workplace or in conflict with the organisation's website. Make sure it is clear that the views and opinions you express are your own.

- Recommendations, references or comments relating to professional attributes, are not permitted to be made about employees, former employees, customers or suppliers on social media and networking sites. Such recommendations can give the impression that the recommendation is a reference on behalf of the organisation, even when a disclaimer is placed on such a comment. Any request for such a recommendation should be dealt with by stating that this is not permitted in line with organisation policy and that a formal reference can be sought through HR, in line with the normal reference policy.

- Once in the public domain, content cannot be retracted. Therefore, always take time to review your content in an objective manner before uploading. If in doubt, ask someone to review it for you. Think through the consequences of what you say and what could happen if one of your colleagues had to defend your comments to a client.

- If you make a mistake, be the first to point it out and correct it quickly. You may factually point out misrepresentations, but do not create an argument.

- It is very important that employees immediately report any inappropriate activity or behaviour regarding the organisation, its employees or third parties. Inform your manager or another member of management or your HR representative. All allegations made in good faith will be fully and confidentially investigated. You are required to cooperate with all investigations of alleged policy violations.

- This policy extends to future developments in internet capability and social media usage.

In addition to the above rules, there are a number of key guiding principles that employees should note when using social media tools:

- Always remember on-line content is never completely private.

- Regularly review your privacy settings on social media platforms to ensure they provide you with sufficient personal protection and limit access by others.

- Consider all online information with caution as there is no quality control process on the internet and a considerable amount of information may be inaccurate or misleading.

- At all times respect copyright and intellectual property rights of information you encounter on the internet. This may require obtaining appropriate permission to make use of information. You must always give proper credit to the source of the information used.

Social Media Security

You are responsible for all postings made on or to your social media accounts.

This applies to:

- Postings or activity made directly by you.
- Postings or activity made by any other party but under your username/account, and/or
- Postings made by friends or third parties to your accounts (e.g. Facebook wall posts made by Facebook friends to your timeline).

You must be conscious at all times of your overall online presence and its effect, or potential effect, on the company, its clients or your colleagues. Disciplinary action may ensue, in line with this policy and the disciplinary procedures, for any activity on, or related to, your social media accounts, regardless of how such activity occurred.

You are therefore advised to maintain the security of your personal social media accounts. This includes, but is not limited to:

- Using secure passwords.
- Changing passwords regularly.
- Not disclosing your passwords to third parties.
- Logging out of accounts when leaving your computer/devices unattended.

If you are concerned about any activity on your social media account, however created, and its interaction with your employment, please contact your manager immediately.

Specific Managerial Responsibilities

By virtue of their position, managers have particular obligations with respect to general content posted on social media. Managers should consider whether or not personal thoughts they publish may be misunderstood as expressing the company's opinions or positions even where disclaimers are used. Managers should err on the side of caution and should assume that their teams will read what is written. A public online forum is not the place to communicate company policies, strategies or opinions to employees.

Managers should not make 'friend' requests or other similar requests of their team members, as this may place undue pressure on an employee.

Monitoring of internet usage by the IT department applies to personal use as well as normal business use.