

Policy Info Pages

SOCIAL NETWORKING & EMAIL USAGE



Purpose of Policy

This policy is to set out clear guidelines for employees of Incident Management Solutions (IMS) on how to use of social networking media and email communication in relation to your employment with IMS.

These new ways of communication are changing the way we talk to each other and even to our consumers, target audiences and clients.

In order to avoid any problems or misunderstandings, we have come up with a few guidelines to provide helpful and practical advice for you when operating on the internet as an employee of IMS.

All employees have a responsibility to follow the guidelines set out in this policy.

Anyone who is found to have breached them may face disciplinary action in line with our disciplinary procedure.

What is Social Networking?

Social networking for the purpose of this policy includes and is not restricted to the following;

Public social sites such as;

Facebook,

LinkedIn,

Tumblr,

SnapChat,

Instagram,

Personal and public blogging sites

Comment boxes on newsfeeds and discussion forums on websites.

Emails.

Social media and email at work

Social media is permissible to be accessed in personal time; employees must not access the Internet for use personal during their working hours.

Use of personal devices to access social media sites is limited to allocated break times only.

- Ø Accessing Social Media at break times should only be done using personal devices; employees cannot control what is visible in a news feed and therefore cannot control offensive material and images.

For the purpose of safeguarding, IMS do not permit the access to Social Media via desktop or IMS provided devices.

Social Networking should not be used as form of communication to voice opinions or thoughts about IMS, its people or its associations.

Social networking should not be used as avoiding face-to-face conversations. Many of the issues that could lead to disciplinary and grievance problems at work can often be dealt with by a manager in a 1:1 setting informally for quick resolve.

Note to managers: Be mindful of becoming over-reliant on electronic communication between yourselves and your team members. You need to keep aware of not widening the gap between close working relationships.

Private usage of Social Media

Social media has blurred the boundaries between a person's private and professional lives. Employees who use social media in their personal life should therefore be mindful that inappropriate use could damage their own reputation and that of Incident Management Solutions (IMS).

When a member of staff identifies their association with IMS – for example, by stating they work for the IMS or posting pictures of themselves at work - and/or discusses their work, they are expected to behave professionally, and in a way that is consistent with the organisation's values and policies.

Even if a staff member does not directly associate themselves with IMS, their link with the organisation can become known through images on friends' social media.

Employee Guidelines:

- Ø It is best practice not to discuss confidential information relating to the business of IMS or that of any employee, association, customer or client of IMS. We have direct and clear processes in place for you to air your thoughts and feelings through our Managers and the HR Department.

- Ø You should seek permission from colleagues before posting personal details or images that may link you to IMS and should not post anything about someone if you have been asked not to.
- Ø You should not upload information or pictures about any colleague and must always remove information about a colleague if you have been asked to do so.
- Ø You should carefully consider what you want to say before you publish anything, and work on the basis that anything you write or post could be shared more widely without your knowledge or permission.
- Ø You should configure your privacy settings and review them regularly because:
 - Social media sites cannot guarantee confidentiality, and do change settings the public, employers or any organisation you have a relationship with may be able to access your personal information, once information is online, it can be difficult to remove it.
- Ø You should be careful when sharing or retweeting posts, as they could be seen to be endorsing someone else's point of view.
- Ø You could face legal proceedings for posted comments aimed at named individuals or an organisation that are considered to harm reputation.
- Ø You must not use the IMS logo anywhere on your social media sites, or copy photos from IMS's internet or intranet sites – these are copyright protected.
- Ø You must seek confirmed authority before using any artwork belonging to the Company.

- Ø You should not air grievances or publish anything that risks bringing IMS into disrepute.
- Ø Posts made by employees must not encourage behavior that could be linked to safeguarding issues, for example:
 - Bullying,
 - Defamation
 - Luring and exploitation□,
 - Theft of personal information□
 - Encouraging self harm or violence
 - □Glorifying activities such as excessive drinking or drug taking
- Ø These kinds of posts may be investigated and result in disciplinary action.

What does this mean?

Generally speaking, what you do outside of work is your own business. However, you never stop being an employee of IMS. Most social media “incidents” are the result of a failure to appreciate that your actions and behaviour impact (and potentially reflect negatively on) yours and IMS's reputation

Being harassed, bullied or victimised via a social networking site?

If you believe you are being harassed, bullied or victimised as a result of another colleagues post to an internet site, you can take action!

- Ø Employees should notify a Manager or the HR Department; the dignity at work policy outlines the informal and formal action that can be taken.
- Ø Alternatively, employees can report the incident to the police or to the social media site.

Misconduct

Any member of staff found to be using social media sites inappropriately, as outlined in the guidelines and policy above, may be subject to disciplinary action and will be managed in line with the IMS disciplinary procedure

Any employee who is in any doubt about what they should or should not post on social media sites – particularly about their work – or who discover online content that may harm the reputation of IMS, should contact the HR department