Compass Group UK and Ireland
Social Media Policy

1 PURPOSE

This policy on using social media should be used in conjunction with the Company's IT Acceptable Usage Policy. For the purposes of this policy, 'the Company' refers to Compass Group UK & Ireland Ltd and all its subsidiary companies including Vision Security Group Ltd and ICM.

The purpose of this policy is to offer guidance on when and how these websites should be used, in and out of the workplace, for business and personal use. It also provides guidance on using these sites safely; highlights the potential risks of using these sites; outlines what activity is prohibited; and outlines the consequences of a breach of this policy.

This policy covers all Company workers.

Reference to the 'client' means any third party to whom the Company is contracted to provide catering, security, cleaning and any other services. The term 'client employees' refers to any workers of the client.

Reference to 'other third party' means any other third party with whom the Company is associated that is not the client, such as a supplier.

2 WHAT IS SOCIAL MEDIA?

For the purposes of this policy, social media is a type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. This includes but is not limited to online social forums such as Twitter, Facebook, MySpace and LinkedIn. Social media also covers blogs and video- and image-sharing websites such as Tumblr, Flickr and YouTube. A blog is a web-based publication consisting primarily of periodic entries, or articles, regarding a particular subject.

Employees should be aware that there are many more examples of social media than can be listed here and this is a constantly changing area. Employees should follow these guidelines in relation to any social media that they use.

3 WHAT ARE THE DANGERS OF USING SOCIAL MEDIA?

3.1 Identity theft

People often post a great deal of personal information on social media sites, including their address, telephone number and interests. This information can be easily accessed by anyone, anywhere, and can be used for criminal activity such as identity theft.

In addition, some users post information on social media sites that can be used to identify important security information. For example, many people share which football team they support or the name of their dog. Such information is often used as an individual's password or security question to retrieve lost passwords for internet banking or shopping accounts; and can leave the individual vulnerable to identity theft or online fraud.

3.2 Legal

A written comment about an individual that is potentially damaging or untrue can be classed as libel. A written comment about a third party (such as a client) can damage their reputation. The individual or third party about whom/which the comment has been made can sue for damages. Blog entries, such as entries on Twitter, have featured in court proceedings where libel is alleged.

Individuals have legal privacy rights, and it is important that any social media posting does not undermine someone else's privacy. For example, publishing the telephone number of a friend could infringe this right.

3.3 Employment

Social media sites often encourage individuals to disclose information about their work. Most organisations, including the Company, will consider any information about work as confidential, meaning it should never be disclosed online.

Posting information about the Company or a third party on social media sites could also damage the reputation of the Company or the third party with

which the Company is connected.

3.4 Harassment/Discrimination/Bullying

Social media sites have featured in court cases related to discrimination and harassment, where derogatory, abusive and intimidating comments have been posted about individuals. Such conduct is known as cyber bullying.

Lastly, employees are reminded that once an entry is made on a social media site it is technically accessible forever, so posts that are embarrassing, defamatory, discriminatory or malicious might never be completely deleted.

4 GUIDANCE FOR SAFE USE OF SOCIAL MEDIA SITES (PERSONAL & BUSINESS)

Check what you are signing up to. By accepting the terms and conditions of a social media site, you may be giving other parties rights to use or sell things (such as personal data, details of friends, pictures) that you place on the site.

Watch out for add-ons. Be wary of loading additional features or applications that can change the original terms and conditions that you signed up to, or that can alter security settlings.

Withhold elements of your personal life you do not want to make public. Imagine that your personal details were to be published in a newspaper – what would you not want to see in that paper?

Take control of your information. Many social media sites offer ways of protecting your information. It often only takes a moment to check to see how you can secure your information.

Resist the urge to make a status update, a tweet or blog entry when you are tired or upset. It is very hard to remove an entry on social media sites; and they can lead to legal action.

Avoid placing sensitive information relating to the work you are doing on social media sites. It may include information that you or the Company would not want out in the public domain.

Consider how social media sites mimic the day to day interaction between people in the real world. If behaviour is not acceptable in real life, then it is unlikely to be acceptable online behaviour.

5 PERSONAL USE OF SOCIAL MEDIA WEBSITES ON PERSONAL PCS, LAPTOPS AND OTHER DEVICES

5.1 Code of Personal Conduct

The Company recognises that many employees use the Internet at home for personal purposes and that many employees use social media websites. The Company respects an employee's right to a private life.

However, the Company must also ensure that confidentiality and its reputation are protected. Employees must be aware that they can build or damage the reputation of the Company or a third party (such as a client or supplier) by the way they conduct themselves on social media sites. The Company therefore requires employees using social media websites to adhere to the following rules:

Employees should ensure that they do not conduct themselves online in a way that is detrimental to the Company or to a third party; or in a way that damages working relationships between colleagues, customers and clients of the Company. Examples of inappropriate conduct include:

- Any comments or actions that could jeopardise the Company's relationship with its client or is likely to bring the Company, client or other third party into disrepute
- Any comments or actions that could contravene the Company's Bullying and Harassment Policy or Equal Opportunities Policy
- Posting critical, negative and/or malicious comments about the Company, the client company, other third parties, client employees, customers or colleagues online
- Posting photographs or videos online of customers, colleagues, client employees or other third party employees without

prior permission of the customer, Company, client company or other third party company

- Posting photos or videos online taken during work time without prior permission of the Company, client company or third party company (employees are reminded that personal mobile phones should be switched off during work time)
- Posting confidential or sensitive Company information or sensitive information about your colleagues, client company, other third party company, client employees or customers
- Discussing any aspect of your employment or making statements regarding any part of the Company, or its client companies, to press, radio, television reporters or investment analysts without the express authorisation of the Company communications team

The above list is not exhaustive.

Employees are reminded that anyone making a defamatory statement on the Internet may be legally liable for any damage to the reputation of the individual or company concerned.

Unless it is a requirement of an employee's job role to manage a branded social media account on behalf of the Company, any social media or online username should not reference the Company or the client company.

Unless you are an authorised spokesperson for the Company, employees must not post in such a way which could be viewed as a Company statement.

If employees do discuss their work on social media sites (for example, giving opinions on their specialism or the sector in which they operate), they must include on their profile a statement along the following lines: "The views expressed here are mine alone and do not necessarily reflect the views of my employer."

For further information, please refer to the Acceptable IT Usage Policy.

Personal use of social media sites in contravention of these guidelines can result in disciplinary action under the Company's disciplinary procedure, including summary dismissal if the breach is particularly serious and extensive.

6 USING SOCIAL MEDIA WEBSITES ON COMPANY PCS, LAPTOPS AND OTHER DEVICES

6.1 Background

Websites that come under the grouping of social media websites have historically been inaccessible on Compass Group PCs, laptops and other devices unless specifically required to be used by the employee in their job role.

Employees are now able to access social media sites from their Company PCs, laptops and other devices. These sites currently include Facebook, Twitter, Pintrest, Instagram and Flickr, but the list may be updated from time to time and is not exhaustive. This policy should be taken to cover any social media sites that are accessible. This section of the policy provides guidance for accessing and using these websites for business and personal use.

6.2 Business Use

You will be advised by your Line Manager if and how you are required to use social media sites as part of your job role; if you are not advised by your Line Manager that using these sites forms part of your job, you should not use these sites for business purposes. Always seek clarification from management before using social media sites for business purposes.

A series of guidelines on social media for business use must be followed if you are expected to use social media as part of your job role (Communications Policies). Please refer to these guidelines before using social media for business purposes.

6.3 Use of Social Media in the Recruitment Process

Unless it is in relation to finding candidates (for example, if an individual has put his/her details on social media websites for the purpose of attracting prospective employers), the resourcing/recruitment department should conduct searches, either themselves or through a third party, on social media sites only when these are directly relevant to the applicant's skills or claims that he/she has made in the recruitment process. For example:

- A prospective candidate might claim that he/she has used social media in his/her previous job (for example as a publicity tool); or
- A prospective candidate's social media use may be directly relevant to a claim made in his/her application (for example, if he/she runs a blog based around a hobby mentioned in his/her CV or a skill in which he/she claims to be proficient).

There should be no systematic or routine checking of prospective candidate's online social media activities, as conducting these searches during the selection process might lead to a presumption that an applicant's protected characteristics (for example, sexual orientation or religious beliefs) played a part in a recruitment decision. This is in line with the Company's equal opportunities policy.

Only members of the Company's resourcing department are permitted to use social media in the ways outlined above.

6.4 Personal Use

Employees are only permitted to access social media sites for personal use during authorised break times, subject to receiving their Line Manager's authorisation which must be obtained on each occasion prior to using social media sites. Line Managers may restrict or prohibit a user's personal use of social media sites, if appropriate. Employees are reminded to follow the guidance in sections 4 and 5 if using social media sites for personal purposes during authorised break times. Employees must log off and close down any social media sites when they are not actively being used. Social media sites must not be left open and running when not in use.

Business use of a Company PC, laptop or other device takes precedence over any personal use of the same piece of hardware. Personal use of social media sites during working hours must not be excessive and must never impact on productivity or work.

Using Company PCs, laptops or other devices to access social media sites in contravention of these guidelines can result in disciplinary action under the Company's disciplinary procedure, including summary dismissal if the breach is particularly serious and extensive.

The Company reserves the right to withdraw personal use of social media sites on an individual or global basis at any time without notice or explanation.

This policy does not prohibit the employee from using their own devices to access social media sites during authorised break times providing that the guidelines in sections 4 and 5 are adhered to.

6.5 Monitoring of Usage of Social Media Sites on Company PCs, Laptops and Other Devices

IT systems and infrastructure are the property of the Company. The Company therefore reserves the right to monitor and record use of these facilities, within government guidelines, to ensure the social media policy is being adhered to. Users should be aware that access to social media sites will be subject to the same monitoring procedures applied to business related access and email correspondence.

If concerns arise about the level of activity on social media by a user during working hours, then the user's Line Manager will be informed and action may be taken under the Company's disciplinary procedure, including summary dismissal if the breach is particularly serious and extensive.

6.6 Summary

Company laptops, PCs and other devices can now be used to access social media sites for limited personal and/or business use. Follow Company

guidelines when using social media sites for business and/or recruitment purposes (as above). Personal use is permitted only during authorised break-times, subject to authorisation from Line Management and subject to the above conditions outlined in 6.4.

7 BREACH OF GUIDELINES AND RULES

All employees are required to adhere to this policy. A breach of any of the above rules may lead to disciplinary action being taken in line with the Company's Disciplinary Procedure, including summary dismissal if the breach is particularly serious and extensive.

8 GRIEVANCES

In the event of any dispute or grievance with management or colleagues, employees are reminded that grievances should be raised in accordance with the Company grievance procedure. Employees should not in any circumstances raise a grievance on the Company's social media feeds or sites.

For enquiries about this policy, please contact the HR Support Centre on 0121 457 5747.

Dennis Hogan

Dennis Hogan
Managing Director UK & Ireland