CHARTERED INSTITUTE
OF PUBLIC RELATIONS

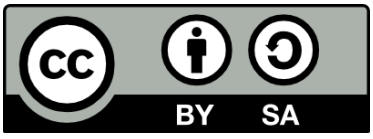
SOCIAL MEDIA BEST PRACTICE GUIDE

#CIPRSM

CIPR

TABLE OF CONTENTS

Published by the Chartered Institute of Public Relations Social Media Panel, December 2013.



INTRODUCTION

This document was originally published in 2011 and was designed to help members of the Chartered Institute of Public Relations (CIPR) navigate a rapidly evolving communications landscape.

This update ensures that the challenges faced by the public relations profession have been reviewed against an evolving set of tools, technologies, legal and governance frameworks.

It is still intended as an introductory guide to highlight core principles that must be considered when developing a communications strategy and campaigns including social media in the United Kingdom. For international activity, members are advised to review the guidelines and legal considerations of their respective countries.

The CIPR social media advisory (CIPRSM) panel would like to thank all those who contributed to updating these guidelines.

As part of the CIPRSM panel's commitment to best practice, this document will be reviewed, updated and developed to ensure the guidelines are not simply a snapshot of practice at a particular point in time, but a resource that provides practitioners with relevant, timely guidance.

DEFINITION OF SOCIAL MEDIA

The CIPRSM panel defines social media as:

"Social media is the term commonly given to Internet and mobile-based channels and tools that allow users to interact with each other and share opinions and content. As the name implies, social media involves the building of communities or networks and encouraging participation and engagement."

CIPR CODE OF CONDUCT

Principles to be applied to social media

All CIPR members are bound by the Code of Conduct, which is based around three core principles: Integrity, Competence and Confidentiality. The Code of Conduct should be adhered to when engaging in any public relations practice. The CIPR advises that these core principles are applied to all elements of a communications campaign including social media activity.

Further information about the CIPR Code of Conduct can be found on the CIPR website.

DOs AND DON'Ts OF SOCIAL MEDIA

This section provides practical advice on how the CIPR Code of Conduct can be applied to social media activity and engagement. These set of dos and don'ts are by no means extensive; they aim to cover the basics.

DO

1. **Listen**

   The first stage in developing a social media strategy is to identify and listen to conversations related to your organisation, brand, competitors, industry and stakeholders. Social Media and all its various platforms and tools allow for online listening on a massive scale, across countries and demographics. You must consider the tools, techniques and timeframes required to do this. A good place to start is the CIPRSM's Social Media Monitoring Guide.

2. **Understand**

   Communications professionals must aim to understand who is saying what to whom, through which channels and why. Knowledge of the different social media platforms available, the tools to manage or monitor conversation, the language used, and assets shared by participants are only a handful of the critical elements that will affect your strategy. Be open to using social media platforms personally - it's tough to be strategic without 'getting your toes wet'.

3. **Plan**

   Don't be tactical - ensure that you align your social media strategy to your business objectives and effectively plan communications cascades, risk mitigation, content, resources, measurement and evaluation, and engagement. (See Section 5 – Planning Social Media).

4. **Engage in conversation**

   Interacting with audiences and stakeholders through various social media channels is a rewarding part of building a brand online. Creating a proactive and reactive content plan and regularly contributing to relevant conversations are both key to creating a strong dialogue with stakeholders. Make sure you are clear about the required resource, guidelines, and governance and security issues.

5. **Ensure a brand is consistent across networks and platforms**

   If practitioners confuse their audience, they will lose their audience. Different social media platforms lend themselves to different tones of voice. It is good practice to ensure your various social media profiles keep the style and tone of voice as consistent as possible – this will help an audience identify and engage with you.

6. **Disclose relationships when endorsing an organisation/client/ customer**
   For example, if a practitioner tweets (or re-tweets) client news, it is best to include [client] at the end of the tweet. If a practitioner tweets (or re-tweets) its employers news on a regular basis, it is best they declare their relationship by including the name of their employer in biography section of the Twitter profile.

7. **Be honest about who 'manages' social media channels**
   An individual: if a practitioner is updating a Twitter account, LinkedIn Profile, Google+ Page, Facebook Page/Profile or a YouTube channel on behalf of another individual (for example, a client or CEO) it is best to be open and clearly state '@person' typically 'manages' the channel. Preferably, this information should be outlined in the biography or 'about' sections of the social media platforms.

   For an organisation: if a practitioner is updating a Twitter account, LinkedIn Company Page, Google+ Page, Facebook Page/Profile or a YouTube channel on behalf of an organisation or movement, then it can be assumed that the person or people managing the channel have a vested interest in the organisation. It is preferable to declare who 'manages' the channel but not necessary.

8. **Outline content approval process from the offset**
   Work with the parties involved in social media activities to agree the process of content approval at the earliest stage. For example, each blog entry that has been written must be approved by 'x', 'y' and 'z' executives. In addition, 'a' has permission to update Twitter account / LinkedIn Company Page / Google+ Page / Facebook Page / YouTube channel on a regular basis, and individual tweets / status updates /comments do not need to be approved.

9. **Be transparent when updating information**
   If a practitioner is working with a community to update company or client related information it is important they are upfront about whom they are and their intentions. For example, if a practitioner is looking to comment in a forum on behalf of a company or a client, they should either work with the forum moderator or post sympathetically and explicitly with full disclaimers. The CIPR has published separate Wikipedia guidelines for PR professionals.

10. **Correct errors openly and in a timely manner**
    Always admit errors and openly 'put them right'. It is advisable to tackle an online issue or crisis as soon as possible to stop it escalating out of control. With social media monitoring in place you should be able to identify issues rapidly.

11. **Consider adding 'views are my own' disclaimer where appropriate**
    This disclaimer is typically used if a practitioner uses an individual social media account to share both personal and professional opinion on matters.

For example, it can be advisable to add a 'views are my own' disclaimer to a Twitter biography, if a practitioner tweets about client and industry related news / opinions, [professional] and also shares their personal views on a subject that lies outside of their work remit [personal], through the same Twitter account.

However, practitioners should be aware that this will not remove the risk of association with an employer, potentially damaging their reputation, and that adding this to a profile has no legal standing in the UK.

12. **Be upfront about conflicts of interest and paid for opportunities**
    If writing or contributing to a blog which recommends a service supplier, make extra effort to make readers aware of any conflicts of interest, such as a financial or a partnership link between the client / member and the supplier. The IAB & ISBA's Guidelines on Paid Promotion in Social Media (2011) advise how to approach sponsored or paid for social media activity including the use of #ad hashtag for paid for tweets. (See Section 6 – Legal Considerations).

13. **Be respectful**
    Always seek permission when updating information or uploading images and videos featuring colleagues or clients to various social media platforms including, but not exclusive to, Twitter, Facebook and YouTube. Always seek permission for any copyright protected content or assets. (See Section 6 – Legal Considerations).

DON'T

1. **Forget that a social media presence becomes part of a brand legacy**
   Posts, pictures, images, tweets, status updates (content in general) can stay online forever. Plan ahead and think about which messages to share via social media channels and their lasting legacies for an organisation.

2. **Make an audience feel uncomfortable**
   It is good to be authentic, develop a tone of voice and provide a hint of personality but continuously being grumpy or openly criticising people can put an audience off and deter them from engaging with an individual or organisation.

3. **Bring a company into disrepute**
   It is likely that most legally binding contracts include a clause about employees not bringing an organisation into disrepute. It is important to remember this clause relates to online activity as well as offline activity. Refer to employee and social media guidelines to understand the online boundaries at a specific organisation.
4. **Reveal company / client sensitive information or intellectual property**

Offline information that should be kept confidential such as new business wins or is governed by disclosure legislation (e.g. publicly trading company financial positions) should not be disclosed. In non-legislated cases, there may be exceptions if specific permission has been granted by the parties concerned; or it is in the public interest; or unless required to do so by law. In all cases, you should seek legal advice before posting.

5. **Be fake**

   Using 'flogs' (fake blogs created by a PR agency or organisation to promote a service or product) or 'astroturfing' (the practice of falsely creating the impression of independent, popular support by means of orchestrated and disguised public relations activity) is illegal. CIPR strongly advises practitioners to steer clear of these tactics.

6. **Rewrite your social media history**

   Do not delete negative comments on social media channels unless they contravene the terms and conditions of the social platforms containing them (e.g. racial hatred comment on a Facebook Page status update). In all cases, understand your legal position, review the social media platform's terms and conditions and apply a measured view - will deletion or allowing the comments to stand serve to escalate potential issues?

PLANNING SOCIAL MEDIA

For many organisations, social media activity has evolved organically rather than as a result of a comprehensive and detailed strategy.

Many are assessing both the long and short-term impact of social media and now understand what it can deliver, how to benchmark it and measure ROI and the risks that must be considered.

Planning social media activity should mirror any strategic element of marketing and communications. The key areas for consideration are:

Setting aims and objectives

Aligning your social media aims against long and short-term business goals, departmental goals and objectives.

Defining audiences

Defining and segmenting your audiences to detail how social media can play an integral part in communicating with these audiences. Audiences will be a complex mix of internal and external stakeholders for most organisations.

Gathering insights

An exercise to gather and analyse both internal and external information that will impact your strategy. What information is available to your organisation? Who can provide this information, and which tools are used to gather and evaluate the information? (E.g. competitor benchmarking, website analytics, social analytics, audience insights, long term business and departmental plans, agency activity, measurement dashboards etc.)

Defining resource

Who will be responsible for social media within the organisation and which support roles exist for staff, agencies, partners etc.? Do you have workflows for content creation, communications cascades and issues management? How will social media activity and engagement be resourced?

Creating guidelines

Creation of workflows, guidelines and guidance for those responsible for your social media activity and all staff to support and protect them in equal measures. (See Section 8 – Advice for Employers). Development of community policies in line with your chosen social media platforms.

Governance and security

An understanding of how governance frameworks for regulated industries, broader legal frameworks and guidance from relevant trade bodies should be applied. Your strategy should also include the impact of social media on crisis and issues

management plans and consider security, safety and passwords. (See Section 6 – Legal Considerations and Section 7 – Security Considerations).

Creating content

Content calendars should ensure that the organisation is prepared to create and curate content for their social media channels. They also ensure that practitioners plan for and take advantage of reactive engagement opportunities.

Managing social platforms

Which resources and tools are required to manage engagement in your chosen social media channels as well as to manage the workflows and cascades around them?

Measuring and evaluating success

Choose measurement tools. Creation of frameworks to measure whether social media is enabling the organisation to reach its goals and to evaluate relative effectiveness. (See Section 9 – Social Media Measurement).

Creating an ongoing knowledge and evaluation loop

Business insights determined from social media monitoring, engagement and measurement must be 'looped back' into the organisation to ensure ongoing efficiencies and effectiveness. Consider the best ways to do this.

LEGAL CONSIDERATIONS

As brands and organisations' adoption of social media continues to grow, the legal and regulatory frameworks affecting the social space are also maturing. This has meant an increased clarification of hitherto untried or untested areas of practice; the updating and tightening of statutory regulations; and development of new advice and guidelines from industry bodies.

This section of the guidelines will outline and address important aspects of the legal, regulatory and advisory domains affecting public relations and marketing communications.

It should be noted that these guidelines do not constitute legal advice. Action should be taken only after specific legal advice has been sought. The CIPR accepts no liability for any action taken or not taken as a result of this information.

Legal Considerations

While social media is often perceived as a unique and different communications environment, many of the legal considerations associated with more conventional print and broadcast media remain relevant. In the absence of legislation relating specifically to social media, English law has tended to use established areas of the law as a starting point in cases to date. This section details the legal considerations to take into account when working with social media.

There are several areas of legislation to consider:

1. Intellectual Property (Creative Commons, copyright and trade marks)
2. Law of Confidence
3. Defamation
4. Consumer Protection from Unfair Trading Regulation (2008)
5. Data Protection (1998)
6. Privacy (Human Rights 1998).

1. Intellectual Property (IP)

The use of visual and audio assets Intellectual property (IP) describes ownership of an intellectual 'product' which may have commercial value. There are four main areas to consider: Creative Commons; copyright; trademarks and designs.

i) Creative Commons

As social media is built upon interaction, information and content sharing, specific protocols have been developed to facilitate and encourage the widespread and free distribution of content providing certain conditions are met.
This protocol is called Creative Commons and social media best practice suggests practitioners should strongly consider distributing and using Creative Commons licensed content where possible and appropriate.

Further information about the specific conditions for Creative Commons content usage can be found online and members can search for freely licensed assets.

ii) Copyright

Copyright covers material including photographs, literature, music, film, audio and art. Copyright is automatic and does not need to be registered – unlike trademarks, for example. The copyright owner has certain economic and moral rights – for example, the right to be credited as the creator of the material and the right to be financially rewarded if another party uses the material.

In most cases, the copyright owner needs to give permission for the material to be used, although there are exceptions to this. The concept of fair use in copyright law allows for certain actions; for example, there is provision for quoting from publicly available material if the source is cited, its use can be justified and only the necessary amount is included.

Information from Government websites may often be covered by Crown Copyright, which generally sets out terms for free use of material.

Further information about Copyright can be found on the UK Copyright Service website.

'Rights managed' (RM) as well as 'royalty free' (RF) assets can be found on stock photography websites such as:

- Getty Images
- istock
- Corbis Images

iii) Trade marks

Trademarks include logos, slogans and words, and are 'signs' used to distinguish products or services of one company from another. A trade mark owner has the right to prevent unauthorised use of that trade mark. Further information about trademarks and Intellectual Property in general can be found on the Intellectual Property Office website.

iv) Design

Design rights relate to the way a product looks – its shape, colour and patterns. Designs can be protected in a similar way to copyright, or can be registered. Owners of design rights have similar rights to trade mark owners and permission to use or reproduce a design should be sought from the owner.

You can find more information about design rights here:

- Intellectual Property Office – Design Page
- ACID

2. The Law of Confidence

The Law of Confidence in the UK is an important right, recognised by the courts and in the world of Intellectual Property. The law requires that a duty of confidentiality is established – this could be in the form of a written contract, for example an employment or business contract. However, the absence of a written document does not necessarily mean a duty of confidentiality does not exist.

Practical examples of circumstances where disclosure / confidentiality laws could be applied include:

- Announcing a new client account before all details have been finalised
- Posting financial information or reports for your own or a client's company
- Revealing information about a competitor
- Revealing information that is not in the public domain

Public relations practitioners should bear in mind issues around disclosure and confidentiality when posting information to any social media platform about their own company, a client or a competitor. If in doubt, it is best to seek permission from senior members of staff, a client, or on some occasions, a legal team.

3. Defamation

Defamation is the act of making a statement about a person or company that is considered to harm reputation, for example by lowering others' estimation of the person or company, or by causing them to lose their rank or professional standing. If the defamatory statement is written down (in print or online) it is known as libel. If it is spoken, it is known as slander. There are exceptions to this – for example, posting a defamatory statement online or recording it on a podcast would both be examples of libel.

Points to note:

- A company may be held responsible for something an employee has written or said if it is on behalf of the company or on a company-sanctioned space including a blog, tweet or website

- Action can also be taken against you for repeating or linking to libellous information from another source. Check carefully before quoting or link to statements from other online sources
- A member should consider whether a statement can be proved before writing or using it (in print or online) – in English law, the onus is on the person making the statement to establish its truth
- A company that provides a forum for blogging can be liable for defamatory statements they host
- Individual members can be held liable by contributing to a defamatory press release, either through preparing a draft of the document, providing a quotation for or issuing a statement
- Speculating or adding the term 'allegedly' to online content that links to or repeats defamatory information does not exempt it from the law

- Retweeting, reposting or linking to defamatory content previously shared by others does not exempt you from the law
- You do not have to name an individual to be considered in breach of the law. Providing sufficient information to make an identification or taking you remarks in the context of others that have named an individual may be enough for a claim to be considered

The way that you respond to any claims of defamation is important too. Often, removal of offending material and an apology can be enough to settle a dispute. Although not tested or applied, it is also worth noting that this principle has been highlighted in cases of social media use in criminal law.

Discussing the *Crown Prosecution Service's interim Guidelines on Prosecuting Cases involving communications sent via social media (2013),* the Director of Public Prosecutions, Keir Starmer, suggested that deleting offending content and expressing remorse may result in no legal action being taken.

Further information can be found in Chapter 17, 'Social Media and the Law', in the CIPR's book, *Share This Too: More Social Media Solutions for PR Professionals*.

4. Consumer Protection from Unfair Trading Regulations (2008)

The Consumer Protection from Unfair Trading Regulations sets out how commercial practices can be unfair through misleading or aggressive practices and lists 31 specific practices that are banned.

This regulation does not specifically relate to social media however any practice used online which is deemed unfair, misleading or aggressive will fall under these rules. For example, 'astroturfing' and 'flogs' are not best practice and would be deemed misleading.

Further information about Consumer Protection law can be found on the National Archives Website.

5. Data Protection

Some social media campaigns may allow members or their clients to collect data from consumers'. For example, clients may run competitions where consumers must register through a website. In cases such as these, it is important for members to be aware that UK data protection laws state (amongst other things) that visitors to websites must be aware of how their details are being used.

Further information about the Data Protection Act (2008) can be found on the Information Commissioners Office website.

6. Privacy

The legal concept of privacy in the UK is complex as there is no one privacy law. However, the Human Rights Act (1998) incorporates the right to privacy for both individuals and companies. The law of confidence is bound with the right to privacy, and many legal cases centring around the right to a private life focus on breaches of confidentiality.

It is advisable to seek permission from colleagues or clients before disclosing information on a blog, website or social network.

Further information about the Human Rights Act 1998 can be found on the National Archives website.

Regulatory Considerations

Advertising Standards Authority's (ASA) Code of Practice

As of the 1st March 2011, the Advertising Standards Authority (ASA) extended its digital remit to cover marketing communications on companies' own websites and in other third party space under their control, such as Facebook and Twitter. This move has a significant impact on marketing communications and PR practitioners as the extension empowers the ASA to apply the UK Code of Non-broadcast Advertising, Sales Promotion and Direct Marketing (the CAP Code) to marketing messages online.

Stephen Waddington, European Digital and Social Media Director for Ketchum and a member of the CIPR's Social Media Advisory Panel, reviewed ASA's extension to the CAP code. Stephen summarised what does and doesn't fall under the CAP code:

- **Websites**: For example, all copy and messages on your web site or in social media channels where a business is promoted must be "legal, decent and honest". All claims must be qualified and any statistical data must be properly referenced

- **Press releases**: Press releases however are excluded from the CAP Code. The distinction lies in the labelling of the document and the fact that it is intended primarily for bloggers and journalists, and not consumers

- **Search engine optimisation**: Natural search results that turn up via a Bing or Google search are excluded from the CAP Code however paid for advertisements are a form of advertising and fall within the remit of the code

- **Social media conversations**: Here's where it gets tricky; user generated content falls within the new remit only if it is adopted and used proactively within an organisation's own marketing communications, on its own website or in other non-paid for space online under the organisation's control. Comments about a brand on a company's Facebook page or on Twitter by consumers as part of a natural conversation, for example, don't fall under a

code, but if a company used those quotes to promote its business on its home page or via social media channels then they would fall under the ASA's scrutiny

- **Video**: Promotional videos such as adverts or content aimed at selling a product or search are covered by the code but editorial video content intended to communicate an opinion are not

The full article can be found on the CIPR website.

Advice and further information about digital remit can be found on the CAP website.

Industry Advice and Guidelines

IAB and ISBA Guidelines on Paid Promotion in Social Media (2011)

The Internet Advertising Bureau's (IAB) Social Media Council and ISBA, the Voice of British Advertisers, created unenforced guidelines designed to offer advertising practitioners with practical advice for using social media with a view to enhancing organisational transparency and securing greater trust from consumers.
Although the guidance is issued by advertising trade bodies there are fundamental implications for public relations, marketing and communications practitioners as the guidelines apply to any circumstance where "a payment has been made in order for someone to editorially promote a brand, product or service within social media".

Where this occurs, the IAB and ISBA require that three clear steps are followed to ensure transparent and ethical practice:

1. Ensure that the author or publisher of the message discloses that payment has been made. This will ensure that it is clear to consumers that it is a marketing communication
2. Ensure that authors adhere to the appropriate terms and conditions of the social media platform or website that they are using in relation to promoting a product or service. This includes search engines likely to index the content
3. Ensure that the content of the 'marketing communication' adheres to the principles of the CAP Code (see the above section in this document on the ASA's CAP Code for further guidance from a PR perspective)

What This Looks Like In Practice

The following outlines some possible examples as to ways in which these over-arching guidelines can be understood in practice:

- **Video content** - The brand or organisation should ensure that there is a clear acknowledgement in the video content that it is the result of paid for placement

- **Blog content** – The brand or organisation should ensure that there is a clear acknowledgement in the blog post that content is the result of paid for or commercially sourced content

- **Forums** – Follow individual forums' community guidelines, moderation policy or similar. Where these are not available, or do not detail how brand representatives should conduct themselves, brand or organisations should approach the forum administrators or moderators directly to seek permission to post content or agree a commercial arrangement making sure to clearly identify themselves as representatives of a brand or organisation

- **Twitter** – Where Twitter users are paid to promote a brand, product or service the practitioner should ensure that payment or sponsorship is disclosed by including the #ad hashtag within the tweet. This maximises space for the original message while making clear to consumers that it is paid for
- **Facebook** – Brands or organisations are advised not pay anyone to post content on individual's Facebook pages or profiles, even with disclosure, as this breaches Facebook's T&Cs

Paid Links and Google's T&Cs

While much of this guidance supports general social media best practice, the IAB and ISBA guidance draws practitioners' attention to Google's terms and conditions, which prohibit the use of 'paid for' links in improving website's search rankings.

They advise that "If hypertext links to a website commissioned by the brand owner or marketing practitioner are included [...] in the blog post or page, these should have the 'nofollow' attribute."

What constitutes exactly 'buying and selling' links is potentially a grey area, but practitioners should be aware that Google can issue sanctions against brands or organisations for undertaking what it perceives to be prohibited linking practices. Sanctions can include:

- Lower PageRank in the Google Toolbar
- Lower rankings
- Removal from Google's search results

Moreover, a number of high-profile organisations have recently been penalised by Google using such sanctions and experienced potential damage to their reputation as a result.

Read more via the Internet Advertising Bureau UK.

Other industry guidelines

Practitioners should also be aware that other industries and sectors may have their own guidance or regulatory requirements for the use of social media in public relations or marketing activity, particularly in heavily regulated sectors.

For example, the Financial Services Authority, the former regulatory body for the finance sector, produced a briefing in 2010 titled *Financial Promotions Using New Media*, which guides brands or organisations in the use of social media. Crucially, this covers "all communications by regulated firms to clients, not just promotional ones" and so should be reviewed by any practitioners operating in this sector.

In the pharmaceutical sector the Association of the British Pharmaceutical Industry's (ABPI) Pharmacovigilance Expert Network (PEN) has issued updated guidance in on the use of owned and earned digital media in the management of safety information for pharmaceutical products.

Titled, *Guidance Notes On The Management Of Adverse Events And Product Complaints From Digital Media* and has been published today' the informal guidance is designed to help communications practitioners comply with updated European legislation.

Additionally, the Prescription Medicines Code of Practice Authority (PMCPA) - the self-regulatory body administering the ABPI's Code of Practice - issued 'informal guidance' on the use of digital communications.

SECURITY CONSIDERATIONS

Social media governance

PR practitioners and their employers should take a proactive approach to addressing security risks by developing a social media privacy and security strategy as a part of an overall social media governance framework.

Social media brings a host of benefits to an organisation, so ensuring data protection and privacy requirements form part of the framework means these benefits can be realised safely and securely.

Your social media security governance should take into account certain challenges:

- Staying abreast of the evolving regulations and terms and conditions of the social media channels you're using
- Managing social media data throughout its life-cycle from initiation through usage, storage, transfer, archiving and destruction
- Ensuring sensitive organisational or personal data is not exposed
- Using tools to monitor, evaluate and take action in sensitive situations. The CIPR Social Media Panel's Guide to Social Media Monitoring explains this in detail.

e-crime

When using social media, PR practitioners need to remain vigilant against the evolving threat of e-crime. New threats are emerging almost daily and maintaining a better understanding of the risks will have a significant effect on your ability to respond to them if the need arises.

Any device on which you can access the internet - be that PC, Mac, smartphone or tablet – and any online platform or channel (email, Facebook, Twitter etc.) can open individuals and organisations up to e-Crime

Social media passwords

One of the easiest ways to compromise online security is through choosing weak passwords for social platforms. Fortunately, it's also one of the easiest things to guard against. Human beings are inherently not good at choosing passwords, or keeping them secret.

Here are some tips for choosing strong password:

- Don't just use a word, create a combination of letters, numbers and keyboard symbols
- Aim for a password containing sixteen characters or more. The longer the passwords, the harder it is to guess or break

- Use a mix of upper and lower case letters, numbers and keyboard symbols (i.e. ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] : " ; ' < > ? , . /)
- Don't use your name, your company name, your mother's maiden name, your children's name or the name of your favourite sport team
- Non-English words are harder to guess
- Establish procedures that require changing passwords at least every quarter
- Multi-factor authentication systems can be costly, but both Twitter and Google has a two-step verification process which requires the user to pass a second check through their mobile phone to log-in
- When sharing passwords across teams, best practice is to use a robust online password manager vault. There are scores of services and some of the most popular include LastPass and KeePass
- The majority of password hacking occurs through 'phishing' (online identity theft which takes users key information by masquerading as a trustworthy entity) and 'trojan attacks' (malware which plants viruses on your device); ensure your anti-virus software is updated to protect yourself from such threats

App security

Some of the most popular applications available for smartphones suffer from serious security issues; whether you're accessing them from work or personal devices, check with your IT team about which your organisation deems safe.

Here are five tips on how best to stay secure when using apps:

1. Awareness

Although the volume of identified smartphone malware is small compared to desktop or laptop malware, with more of our online visits coming from mobile devices e-Criminals are increasingly targeting apps. Staying aware of the growing threat is the first step towards preventing malware infections.

2. Verify before installing

Keen for their campaign to benefit from social media straight away, the average PR practitioner is likely to install first and worry about security later. It doesn't take long to research apps and the sources from which they originate before installing. A rudimentary way is to check reviews in the app store offering the software.

3. Shop at reputable stores

Different mobile platforms have different restrictions around the sources you can use to install apps. Best practice is to stick with your official app store when downloading software e.g. the Apple App Store for iPhone; Google's Android Market for Android; RIM's BlackBerry World for BlackBerry. Android users can actually block the installation of non-Market apps by un-checking the 'Unknown sources' option in the Android Applications Settings menu on their devices.

4. Know the app permissions

When you install a new app on your smartphone, generally an app 'permissions' screen pops up, informing of the potentially sensitive resources which the app will look to access. Don't take these at face value and accept just to get the app. e.g. if a card game requests access to your contacts, you can, and should, block the request. While it can be difficult to determine if the app really needs this access, and some apps won't work without being granted certain permissions, take the time to assess whether handing over your data is worth the trade off.

5. Update your antivirus

If you're accessing the Internet on your device, it's at risk of e-Crime. Ensure antivirus is updated not just for your desktop, but your smartphone and tablet too.

ADVICE FOR EMPLOYERS

There is much debate over the boundaries companies should set for their employees' use of social media, and there is no definitive answer. Indeed there cannot be a definitive one-size-fits-all answer as the best way for any employer to combine managing risk and utilising opportunities depends on the employer's specific circumstances.

The CIPR advises that both the employer and employee are responsible for understanding and adhering to social media best practice, but the employer should not shirk from their responsibility to support their employees and ensure they know what good practice, and company policy, is.

It is therefore advisable for an employer to:

1. Understand the circumstances under which employers can be held legally responsible for the online content published by their employees. Situations that may apply include action taken as part of their role for the company and material published on an official company space or somewhere that has been previously sanctioned by the company

2. Beyond legal responsibilities, employers should also understand the circumstances under which their customers, stakeholders or other key audiences may hold them responsible for online content published by their employees even if there is no direct legal responsibility. This applies particularly when employees may publish information which is legal but which reflects poorly on them as individuals – and which therefore some people may feel justifies action by their employer

3. More positively, Employers should be aware of the opportunities there are for employees to act as positive advocates for the firm online. This usually goes beyond people directly acting in their specific job role as, for example, a marketing person responding helpfully to a tweet from a customer with a problem can boost the company's reputation even though strictly speaking it was a customer service and not marketing issue

A good approach for employers therefore is to:

1. Ensure employee induction, training and terms of employment cover what is and isn't acceptable behaviour. This should cover legal requirements, appropriate industry regulation guidelines, such as the CIPR code of conduct, and employer-specific guidance - given that such rules and regulations can and do change, policies should also be kept under regular review

2. Include guidance on where the line is between personal and professional use of social media; for example to make clear in personal social media updates when they are talking about a client

3. Include guidance on when issues about tone of voice may cause an issue for employees; for example, if clients in Scotland are important for the employer than making anti-Scottish comments, even on a private social media account, may cause problems.

Making sure that such policies are incorporated into staff terms or contracts both provides employers with an appropriate framework to use if there is a problem and also protects employees from inadvertently making mistakes. Consideration should be given to what steps will be taken if the policy is disregarded by an employee.

SOCIAL MEDIA MEASUREMENT

As is clearly stated in item six of the Barcelona Declaration of Measurement Principles in PR: social media can and should be measured.

Even if there are no universally accepted social media metrics, that should not prevent any organisation from putting in place robust measures to determine the economic value of its social media activity.

By clearly defining concrete and measurable objectives, all social media activity can and should be evaluated through the lens of these goals.

The ever increasing amount of time spent by all individuals using social media puts even more pressure on organisations to better understand the contribution it makes to communication and organisational objectives.

Any social media measurement approach must be careful to validate the metrics being used in relation to original goals. Social media metrics to date have also been prone to defaulting to easy to measure metrics such as reach and/or followers, fans, etc.

We must be on guard at all times against 'vanity metrics' that can seriously undermine the credibility of our measurement efforts.

Take Twitter followers as an example. Having a link Re-tweeted by an account with a large number of followers may lead to claims that a certain number of 'impressions' have been achieved, and by implication, that a certain number of people have been made 'aware' of the message.

But this is a dangerous assumption. Take the example of the New York Times Twitter account which appears to have just over 10 million followers (November 2013). However, according to Statuspeople.com, an estimated 44 per cent of these followers are fakes, and a further 40 per cent are inactive, leaving a "true" follower base of around 16 per cent - or 1.6 million followers. Even this "true" follower base is all unlikely to be online at the same time - say, perhaps 10 per cent at most. Given the estimated "shelf life" of a Tweet is now an estimated 18 minutes (in other words, the likelihood of any kind of interaction with a Tweet is going to happen within 18 minutes), then the "true" reach of any set of Twitter followers at any one point in time is doing to a small sub set of the overall follower base. Thus the use of raw Twitter followers as a social media metric is fundamentally flawed. Such caveats apply to similar metrics such as Facebook fans.

Any social media measurement approach must therefore attempt to reflect the reality of the genuine audience interaction and its impact on previously define concrete and measurable goals.

Fortunately, techniques such as attribution analysis (via free tools such as Google Analytics) allow organisations to determine both the direct and indirect economic contribution that social media makes towards these goals. The adoption of these kinds of approaches (even in the absence of universally accepted metrics) should in principle lead to more accurate and credible insight into the value delivered by social media activity.

For further information on how to measure social media, can be found here:

The CIPR research, planning and measurement toolkit

The CIPR social media measurement guidance

USEFUL LINKS

Resources for CIPR Members

- CIPR Code of Conduct
- The CIPR research, planning and measurement toolkit
- CIPR Social Media Measurement Guidelines
- CIPRSM Social Media Monitoring Guide
- CIPRSM Wikipedia best practice guidance for public relations professionals
- CIPR skill guides for practical advice on blogging, online videos and much more
- Stephen Waddington's blog post for CIPR – Is your digital PR ready for the ASA regulations

Useful links

Disclaimer: The links listed below are not controlled by the CIPR. The content of these websites is intended as a helpful starting point in your research; the content is not controlled or endorsed in any way by the CIPR and the websites listed are not under CIPR control.

Example social media corporate guidelines

- BBC's Social Media Guidelines
- Coca-Cola Social Media Principles

Example community standards

- Guardian's Community standards and participation guidelines (10 guidelines all participants in the Guardian's community areas are expected to abide by)

Further information on legislation and laws to consider

- Creative Commons information
- Copyright information
- Trademarks and Intellectual Property information
- Crown Prosecution Service's interim Guidelines on Prosecuting Cases involving communications sent via social media (2013)
- Consumer Protection from Unfair Trading Regulations 2008
- Data Protection Act 2008
- Human Rights Act 1998
- Advertising Standards Authority CAP Code
- IAB and ISBA Guidelines on Paid Promotion in Social Media 2011

Further advice on social media measurement

- AMEC's Social Media Valid Framework 2013

CIPR social media books

- Share This: The Social Media Handbook for PR Professionals
- Share This Too: More Social Media Solutions for PR Professionals

With thanks to the CIPRSM panel

Stephen Waddington MCIPR (@wadds)
Matt Appleby FCIPR (@mattappleby)
Richard Bagnall MCIPR (@richardbagnall)
Rob Brown FCIPR (@robbrown)
Stuart Bruce MCIPR (@stuartbruce)
Dominic Burch MCIPR (@dom_AsdaPR)
Simon Collister MCIPR (@simoncollister)
Russell Goldsmith MCIPR (@russgoldsmith)
Michelle Goodall MCIPR (@greenwellys)
Gemma Griffiths MCIPR (@gemgriff)
Garbielle Laine-Peters MCIPR (@gabrielleNYC)
Rachel Miller MCIPR (@AllThingsIC)
Mark Pack MCIPR (@markpack)
Julio Romo MCIPR (@twofourseven)
Andrew Smith MCIPR (@andismit)
Dan Tyte MCIPR (@dantyte)
Robin Wilson MCIPR (@robin1966)