SOCIAL MEDIA, EMAIL AND INTERNET USE

Introduction

The increasing use of social media, email and the internet at work by employees, has created new challenges and risks in the workplace, especially regarding discipline and the legal liability of an employer for the acts of its employees.

Potential risks to employers

Problems associated with social media and misuse of email and the internet in the workplace can include:

- A negative impact on **performance** if employees are distracted or are spending a large amount of time online or sending personal emails;
- **Breaches of confidentiality** if employees are sharing commercial information, private information about customers, or other sensitive information;
- **Damage to the company's reputation** if an employee makes derogatory comments about the company online;
- Risk of a **bullying or harassment** claim if one employee posts comments about another or sends any kind of offensive message to another employee.

It is important to remember that an employer is open to various risks of being held legally liable for the actions of its employees.

Another threat that employers are open to is computer viruses. The primary source of computer viruses is the downloading of certain types of files from the internet or attached to emails. Employees may often unwittingly open emails which contain a virus. In order to protect their interests, employers need to take steps to ensure that employees are exercising caution when using email.

Have a clear policy

In order to manage the potential risks, it is essential to have a clear and **well communicated policy on acceptable use** and to ensure that all employees are aware of this. Such a policy should be clear, concise, remove any expectation of privacy which might exist in the mind of employees, provide for the right of an employer to monitor employees' use of social media, the internet and email and specify that any information obtained through monitoring may be used in disciplinary proceedings.

Having an acceptable use policy can help to avoid problems by making it clear to employees what is and what is not acceptable in terms of use of social media and electronic communications. This may include the amount of time spent, when it is acceptable to use such media and what kinds of site are acceptable. The existence of a policy will also make it easier to deal with any problems which do arise, for example taking disciplinary action when an employee has used social media to make defamatory remarks about the company.

The policy should not be so prescriptive (for example, about certain sites) that it goes out of date quickly. It should specify who is authorised to use social media to communicate on behalf of the company and should also inform employees whether the use of social media will be monitored. Note that any monitoring should comply with the Employment Practices Code issued by the Information Commissioner.

The policy will also need to **link to other organisational policies** such as the disciplinary policy, any bullying and harassment policy etc. It may also be useful to include a clause in **employee contracts** specifying the employee's obligations in relation to **confidential information** and ensuring that this clause refers to social media.

When preparing a policy it is important to **consult a wide section of employees** from different functions in the organisation in order to determine the current extent of social media usage and to ensure that the policy fits with the culture of the organisation.

Once the policy has been finalised, ensure that it is properly communicated both to existing employees and to new employees. It should form part of the contractual documentation given to all employees on joining and be distributed to existing employees with the instruction that it forms part of their terms and conditions and must be read carefully.

Technology is evolving rapidly and this is likely to continue. There have also been several important legal cases which can provide guidance for employers. It is important, therefore, that employers keep up to date with both technological and legal developments and that policies are regularly reviewed and updated to ensure they remain current.

Monitoring staff

Monitoring employees' use of social media, the internet and email is covered in the Data Protection Act 1998 (DPA). The Information Commissioner is responsible for overseeing compliance and has produced 'The Employment Practices Code' which includes guidance on an employer's rights to monitor staff. The Code protects staff from covert monitoring except in exceptional circumstances, such as when there are grounds for suspecting criminal or equivalent malpractice. It can be accessed on the Information Commissioner's website: www.ico.org.uk

The Code allows companies to check staff email accounts in their absence if they have been informed that this will happen. However, employees' privacy must be respected if they clearly mark that an email is personal, unless their employer has a valid and defined reason to examine the content.

Using the internet

The company policy must state any restrictions on using the internet and whether access is allowed for business use only or for private use as well. A problem with browsing, even for business use, is that it can become unfocused and time-consuming. This wastes employees' time and, even when done in their own time, it ties up resources. The policy must also warn about the risks of obtaining and using unsubstantiated information for business use.

The policy should make clear what is acceptable in terms of time spent downloading material.

The policy must state unequivocally that downloading offensive, obscene or indecent material is forbidden and will be subject to disciplinary action.

Policies should also make it clear that the downloading or transmission of certain images is a criminal offence and that the police will be informed where there is any evidence of such activity.

Much of what appears on the web is, or claims to be, protected by copyright. Any reuse of downloaded information without permission is prohibited. Many companies enforce rigorous policies on photocopying and a similar policy must be applied to copying from the internet. Copyright law applies not only to documents but also to software.

Social Media

Online diaries, or blogs, have become increasingly popular as sources of information. Social networks such as MySpace, Facebook and Twitter are also increasingly popular as a means for people to stay in touch and make new contacts.

It is not just time lost which is of potential concern to employers, it is also the content which is posted.

However, involving at least some employees in appropriate use of social media for work-related activities can have important benefits for the employer. Employees may carry out research, promote the company's products and develop important contacts and connections.

Corporate social networking can also be a useful way for employers to communicate and engage their employees. Some businesses are using social networking forums to increase awareness of their activities, to bring staff together from different locations or to introduce energy and 'buzz' into internal communications. If employers set up corporate social networks, a clear distinction needs to be made between corporate social networking which is useful to the business and social networking for personal use.

Employers should decide what approach they want to take to managing the use of blogs and social networks and ensure this is covered in their policy. They should set out whether there are any limits on use, for example, whether access to social networking sites is allowed at lunchtimes or whether there is a total ban.

The policy should also make it very clear that defamatory statements about the company will be treated as a disciplinary offence and emphasise that confidential matters should not be discussed in such forums.

Problems can sometimes arise because employees are naive about the accessibility of content posted on social media and the potential audience. It is easy to forget that even information shared in a closed group or protected by privacy settings can be passed on. **Education** about the potential risks is therefore important to remind employees to behave responsibly online.

Employees are more likely to use social media to voice grievances against the company if they feel they have no alternative outlet. Having clear and fair mechanisms in place for employees to raise grievances and an open culture when managers listen and respond when problems are raised can help to prevent this.

For further information on social media in the workplace see the LRA Guidance on Social Media and the Employment Relationship on their website www.lra.org.uk

Using email

Although email communication has the same speed and apparent informality as using the telephone, it also has the permanence of written communications and, as such, must be controlled to ensure that it meets the same standards as other published documents.

The policy should state whether the email service is to be used for business purposes only or is permitted for personal communication also. If the telephone may be used for personal communications, then it could be difficult to forbid a similar use of email, although there are clearly greater security implications in the widespread use of email.

Some guidelines on email protocol and effective use may be useful. For example, employees should be encouraged to limit group emails, to ensure that all those copied really need to receive the email, that emails are checked periodically and are filed once dealt with.

The policy should make it clear that the same laws apply to email as to any other written document and that employees should avoid making any inaccurate or defamatory statements and that sending offensive emails will not be tolerated.

The sender of a message which causes offence must be subject to normal disciplinary procedures, but in this respect email is no different from any other interpersonal dispute (and has the advantage that, unlike purely verbal communications, it is possible to supply evidence to support a complaint).

For external email it is possible to include a disclaimer but the policy should still emphasise the need to act responsibly when writing email, and to seek advice before sending a message if there is any doubt about its contents.

In spite of the benefits of email, excessive use can mean loss of productivity. The policy should make clear the importance of only sending relevant emails and avoiding the automatic forwarding of all messages to long circulation lists.

The policy should also set out a procedure to cover wrong delivery. For example, it should state that a wrongly delivered message should be redirected to the correct person.

Dealing with breaches of the policy

A response to a disciplinary matter arising from inappropriate use of social media should be dealt with in accordance with the Disciplinary Procedure (see section 18). A full investigation should be conducted before any decision is made and any sanction should be fair and reasonable considering all the circumstances.

See Appendix 21A for a list of key issues which should be addressed in developing your Social Media, Internet and Email Policy and Guidelines. Note that the list is not exhaustive.

See Appendix 21B for Sample Internet and Email Security Policy Guidelines.

For further information on social media in the workplace see the LRA Guidance on Social Media and the Employment Relationship on their website: www.lra.org.uk

APPENDIX 21A

POLICY CONTENTS CHECKLIST

TOPIC	ISSUES
ACCESS	• Who is entitled to use email? In most companies, it would be difficult to justify denying any particular groups access to this valuable communication tool. • How to get access to email? • Who is entitled to access the web and when? • How to get access to the web?
PASSWORDS	• Rules for choosing a password. • Rules for changing a password. • Warning on disclosing passwords. • Rules on password-access to other companies' websites.
WEB	• Prohibition on access to certain websites. • Limitations on browsing the web for non-business purposes. • Rules for adding information to the company website. • Guidelines for responding to website enquiries.
DOWNLOADING	• Prohibition on downloading offensive material. • Information on the implications of copyright laws. • Guidance on the use of unverified information.
EMAIL	• Limitations on private use of email. • Restrictions on content of email. • Rules for email distribution. • Rules on disclosing email addresses. • Legal position regarding defamation and inappropriate advice.
MONITORING	• Notification that website access may be monitored. • Notification that email may be intercepted and read.
DISCLAIMERS	• Wording to use in disclaimer. • Documents which require disclaimers.
DISCIPLINARY PROCEDURES	• Sanctions which will be imposed for breaching the policy.

APPENDIX 21B

SAMPLE INTERNET AND EMAIL SECURITY POLICY GUIDELINES

1. Who is covered by the policy?

This policy applies to all [name of Company] staff including its directors or officers, contractors, home-workers, part-time and fixed-term employees, secondees, temporary staff, casual staff, agency staff and volunteers. This policy does not form part of your terms and conditions of employment and [name of Company] reserves a right to amend the policy at any time.

2. Purpose of the policy

The policy is intended to help employees of [name of company] make appropriate decisions about the use of internet, email and social media such as Twitter, Facebook, Google, LinkedIn, Wikipedia, Whisper, Instagram, Vine, Tumbler and all other social networking sites to include (but not limited to) internet, video, picture and audio postings and blogging.

The policy applies to use of social media for business purposes as well as personal use that affects our business in any way.

This policy outlines the standards [name of company] requires staff to observe when using the internet, email and social media, the circumstances in which [name of company] will monitor your use of these media and the action that will be taken in respect of breaches of this policy. The principles of this policy apply to use of these media regardless of the method used to access it and covers static and mobile IT/computer equipment, as well as work and/or personal smartphones etc.

3. Personnel responsible for implementing the policy

The board of directors of [name of company] OR [POSITION] has overall responsibility for the effective operation of this policy, but has delegated day-to-day responsibility for its operation to [POSITION].

Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks lies with [POSITION] who will review this policy on an [ANNUAL] basis to ensure that it meets legal requirements and reflects best practice.

Managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to [POSITION]. Questions regarding the content or application of this policy should be directed to [POSITION].

4. Using work-related social media

Only the [position of relevant persons/team] is/are permitted to post material on a social media website in the company's name and behalf. Anyone who breaches this restriction will be subject to the company's disciplinary procedure.

Approved social media websites for [name of company] are [insert list of sites e.g. Facebook, Twitter etc].
This list may be updated by [position of relevant person].

Before using work-related social media you must:

- have read and understood this policy and [refer to any other relevant policies and guidelines]; and
- have sought and gained prior written approval to do so from [position of relevant person].

The roles and functions which will be needed moving forward have been identified as follows:

[insert functions and people responsible as applicable such as:

- tweeting corporate news – Marketing Manager
- advertising promotions on Facebook – Sales Manager].

Any employee involved in the organisation's social media activities must remember that they are representing the organisation, use the same precautions as they would with any other communication and adhere to the following rules:

- Ensure that the purpose and benefit for the organisation is clear;
- Obtain permission from a manager before using social media; and
- Ensure the content is checked before it is published.

5. Personal use of social media

Personal use of social media in the workplace is permitted, subject to certain conditions, as detailed below;

- It must not be abused or overused and the company reserves the right to withdraw permission at any time.
- It must not involve unprofessional or inappropriate content.
- It should not interfere with your employment responsibilities or productivity.
- Its use must be minimal and take place substantially outside of normal working hours, for example, breaks, lunchtime [specify appropriate hours].
- It should comply with the terms of this policy and all other policies which might be relevant (to include but not limited to) the [name of company]'s Equal Opportunities Policy, the Anti-Harassment Policy, the Data Protection Policy and Disciplinary Procedure.

You are also personally responsible for what you communicate on social media sites **outside the workplace**, for example at home, in your own time, using your own equipment. You must always be mindful of your contributions and what you disclose about the company. For further details, see Point 6, 'General rules for social media use' below.

6. General rules for social media use

Whenever you are permitted to use social media in accordance with this policy, you must adhere to the following general rules. The same rules would also apply when using social media outside of work:

- Do not post or forward a link to any abusive, discriminatory, harassing, derogatory, defamatory or inappropriate content. This includes potentially offensive or derogatory remarks about any other individual.
- A member of staff who feels that they have been harassed or bullied, or are offended by material posted by a colleague onto a social media website should inform [insert position of relevant person].
- Never disclose commercially sensitive, anti-competitive, private or confidential information. If you are unsure whether the information you wish to share falls within one of these categories, you should discuss this with [insert position of relevant person].
- Do not post material in breach of copyright or other intellectual property rights.
- Be honest and open, but be mindful of the impact your contribution might make to people's perceptions of the company.
- You are personally responsible for content you publish. Be aware that it will be public for many years.
- When using social media for personal use, use a disclaimer, for example 'The views expressed are my own and don't reflect the views of my employer'. Be aware though that even if you make it clear that your views on such topics do not represent those of the organisation, your comments could still damage our reputation.
- The employee's online profile must not contain the company name.
- You should avoid social media communications that might be misconstrued in a way that could damage our business reputation, even indirectly.
- Do not post anything that your colleagues or our customers, clients, business partners, suppliers or vendors would find offensive, insulting, obscene and/or discriminatory.
- Do use privacy settings where appropriate but bear in mind that even comments in a restricted forum may be passed on.
- If you have disclosed your affiliation as an employee of our organisation you must ensure that your profile and any content you post are consistent with the professional image you present to client and colleagues.

If you are concerned or uncertain about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your manager.

If you see social media content that disparages or reflects poorly on us, you should contact [your manager or department]

7. Use of the internet and email

Limited personal use of the internet and of email at work is acceptable provided it does not interfere with or impede your normal duties. Such use should take place substantially outside of normal working hours, for example, breaks, lunchtime [specify appropriate hours].

Users may access non-business related sites, but are personally responsible for what they view.

You should not engage in any activity which is illegal, offensive or likely to have negative repercussions for the company.

[Name of Company] employs software to block some non-business related and offensive websites.

You must not use company equipment to access the internet either from within or from outside the company network using a 3rd party dial up ISP on your company computer (e.g. Freeserve, AOL).

Always ensure that [Name of Company] is neither embarrassed nor liable in any way by your use of the internet.

You may not upload, download, use, retain, distribute or disseminate any images, text, materials or software which:

- Are or might be considered to be indecent, obscene or contain profanity;
- Are or might be offensive or abusive in that the context is or can be considered to be a personal attack, rude or personally critical, sexist, racist, or generally distasteful;
- Encourage or promote activities which make unproductive use of your time;
- Encourage or promote activities which would, if conducted, be illegal or unlawful;
- Involve activities outside the scope of your responsibilities, for example the unauthorised selling/advertising of goods and services;
- Might affect or have the potential to affect the performance of, damage or overload [Name of Company] system, network and/or external communications in any way; or
- Might be defamatory or incur liability on the part of [Name of Company] or adversely impact on the image of [Name of Company].

You must not include anything in an email which you cannot or are not prepared to account for.

You must not make any statements on your own behalf or on behalf of [Name of Company] which do or may defame or damage the reputation of any person.

Care should be taken when adding attachments to your Outlook email. It is company policy that no attachment should exceed 25Mb in size.

The auto-forwarding facility within the corporate email system should not be used to forward work emails to private accounts (e.g. Hotmail or Yahoo).

Attachments to emails should only be used when strictly necessary. When hyperlinks are available these should be used. Large files should be compressed and key information from small files may be cut and pasted into the email itself.

Remember that a phone call or face to face discussion may often be more appropriate than an email, bearing in mind that an email may be misinterpreted or lead to a chain reaction. Also, consider carefully who really needs to be copied on emails. Unnecessary email can be a major distraction.

Access to all email internet sites (e.g. Hotmail, Yahoo mail etc.) is restricted to your ‘own time’ as defined above.

You must not download any software, executable files or potentially offensive graphic image files (GIFs and JPGs) unless you have obtained prior permission from [Name of Company].

The following activities are expressly prohibited:

- The introduction of network monitoring or password detecting software on any [Name of Company] user machine or part of the network;
- Seeking to gain access to restricted areas of the network;
- The introduction of any form of computer virus;
- Other hacking activities;
- Knowingly seeking to access data which you know, or ought to know, to be confidential and therefore would constitute unauthorised access.

8. Monitoring use of social media, email and the internet

Staff should be aware that emails and any use of the internet and social media websites (whether or not accessed for work purposes) may be monitored and, where breaches of this policy are found, action may be taken under the company's Disciplinary Procedure.

The company reserves the right to restrict or prevent access to certain internet sites including social media websites if personal use is considered to be excessive. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

Misuse of social media and other websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against you and the company.

If you notice any use of social media by other members of staff in breach of this policy please report it to [position of relevant person such as line manager].

9. Recruitment

[Name of Company] may use internet searches to perform due diligence on candidates in the course of recruitment. Where we do this, [Name of Company] will act in accordance with its data protection and equal opportunities obligations.

10. Breaches of policy

Where it is believed that an employee has failed to comply with this policy, they will be subject to the company's disciplinary procedure. If the employee is found to have breached the policy, they may face a disciplinary penalty ranging from a verbal warning to dismissal.

The penalty applied will depend on factors such as the seriousness of the breach; the nature of the posting; the impact it has had on the organisation or the individual concerned; whether the comments cause problems given the employee's role; whether the employer can be identified by the postings; other mitigating factors such as the employee's disciplinary record etc.

Any member of staff suspected of committing a breach of this policy will be required to co-operate with [Name of Company]'s investigation, which may involve handing over relevant passwords and login details.

You may be required to remove any social media content that [Name of Company] consider to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.