Tolley's Managing Email & Internet Use

2nd Edition

A practical guide to **employers' obligations** and **employees' rights**

Lynda Macdonald

ROUTLEDGE

Tolley's Managing Email and Internet Use

Second Edition

by

Lynda A C Macdonald MA FCIPD LCM

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published by LexisNexis

First published 2001

This edition published 2011 by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN
711 Third Avenue, New York, NY 10017, USA

Routledge is an imprint of the Taylor & Francis Group, an informa busitness

A CIP Catalogue record for this book is available from the British Library.

ISBN - 978 0 7545 2443 4

Typeset in Great Britain by Columns Design Ltd, Reading

Note About the Author

Lynda A C Macdonald is a self-employed, freelance employment law advisor, management trainer, and writer. For fifteen years, prior to setting up her own consultancy business, she gained substantial practical experience of employee relations, recruitment and selection, dismissal procedures, employment law and other aspects of human resource management through working in industry. With this solid background in human resource management, she successfully established, and currently runs, her own business in employment law and management training/consultancy. She is also appointed as a panel member of the Employment Tribunal service in Aberdeen, where she lives.

Lynda is a university graduate in language and a Fellow of the Chartered Institute of Personnel and Development. Additionally, she has an LLM degree in employment law.

Contents

Table of Cases

Table of Statutes

Table of Statutory Instruments

1 Uses and Abuses of Communication Systems in the Workplace

Introduction [1.1]

Employees in today's workplaces have the facility to communicate quickly and easily with colleagues and outsiders as a result of the advent of modern communications systems such as email and the internet. Although such modern means of communication have brought many benefits, they have also created new problems for employers. Apart from the potential legal liability that employees' use of email and the internet may create for employers (see CHAPTER 2), there may be a rightful concern about the amount of time employees spend surfing the net, playing computer games, or sending emails to their friends.

Although email, when it was first introduced, was a revolutionary method of communication that vastly increased the opportunities for companies to advertise their products or services, keep in touch with clients and customers, conduct research and inform their employees about a wide range of company-related activities and policies, there are many types of communication for which it is not suitable.

Use of the internet has of course given employees in many organisations almost unlimited access to information on unlimited subject matter. Businesses have gained substantial advantages through the use of web-based communications, such as the opportunity to win new customers, set up closer ties with business partners, keep in touch with employees who are mobile and gain access to a vast source of information. All this has brought many benefits, but along with these, a multitude of problems.

Business Email and Internet Use – What is Beneficial for the Business [1.2]

The advent of email and internet access has brought immense benefits to businesses and the employees who work for them. The most obvious of these benefits are described below:

Cost Savings [1.3]

Communication by email is a cost-effective way of sending and receiving information. Because messages and attached documents can be sent to any number of people at the same time, this eliminates the need to print out and send individual packages with the associated postage and packing costs. Messages sent by email to another country can thus save substantial postage costs. In most cases, sending an email costs less than a local telephone call.

There is also a potential cost saving if email messages are retained in electronic format only rather than being printed out in order to form a hard-copy file. This has further advantages for the environmentally-conscious organisation in terms of reducing the amount of paper consumed by the business.

For marketing purposes, advertising a product or service on a website is considerably less expensive than producing a glossy brochure and distributing it to large numbers of potential customers.

Speed [1.4]

Information and documentation can be sent across the world within seconds, whilst a package sent by post or by courier can take many hours (or days) to reach its destination. Even a long fax can take up to an hour to print out at the recipient's office location.

Preparing an email is also quicker than writing a letter in that no time is needed to print the document out – the document is sent following the simple click of a mouse.

Time and place [1.5]

Long and short documents can be sent by email over long and short distances quickly and easily. Time differences between different countries become irrelevant as the email message can be sent during the sender's working day irrespective of time zones and then read by the recipient during their own office hours. Businesses can reach their customers all over the world, increasing trade links and expanding markets whereas budgets may not extend to world-wide marketing by any other means. Internet access too can be achieved 24 hours a day from any location with a computer and a modem.

Convenience [1.6]

Employees can choose when to access their incoming emails and it is open to them to organise their work so that they deal with incoming messages at set times each day, rather than being subjected to continual interruptions by

telephone. Email messages can also be accessed remotely, allowing employees opportunities to communicate with their colleagues irrespective of whether they are working in the office, at home or travelling away from home on company business. Similarly, internet access can be made from any computer with a modem, including portable laptop computers, irrespective of the person's physical location.

Permanent record [1.7]

An email message can, if necessary, be printed out to form a permanent record, and even if it is held only on the computer's hard-disk, this provides a more credible and usable record that someone's vague recollection of a telephone conversation.

Research [1.8]

The internet provides unlimited opportunities for companies to conduct research into the business activities of their potential customers and suppliers, to analyse what the competition is doing and to accumulate information on an infinitely wide range of subjects relevant to the business. Much of the information available on the internet is free, or else accessible on payment of a modest fee.

Abuse of Email and the Internet – Problem Areas [1.9]

Despite the irrefutable advantages and benefits to businesses of email and internet access, there are many problems and disadvantages associated with the granting of access to these means of communication to employees. Sending an email has often been compared to sending a postcard – the message is not confidential and may be intercepted or read by someone other than the intended recipient. One of the other major problem areas is potential time wasting and the consequent loss of productivity. These, together with other problem areas, are analysed below:

Time wasting [1.10]

The internet can be likened to an endless library containing unlimited information on every imaginable topic, providing an indispensable source of knowledge to employees in every sector of business. Although this can greatly enhance employees' effectiveness, it can also, because of the sheer volume of available information, be very damaging to productivity. Locating information relevant to a specific query can be a very time-consuming exercise. Surfing the net in particular can involve a lengthy process of entering words and phrases in the search facility which may then produce literally thousands of possible results. Even once these potential web-sites are scanned through and a suitable selection made, the next level of search may still not produce anything useful or relevant.

Loss of productive time **[1.11]**

The distractions of the internet are many, and there is a growing problem for employers of loss of productive time due to employees surfing the net for both legitimate business purposes and personal entertainment purposes. It can be argued that providing internet access is akin to placing a television on an employee's desk, such is the likely level of distraction. In the case of *Franxhi v Focus Management Consultants Ltd [1998] Case No 2101862/98*, for example, there was evidence that an employee had visited 150 web-sites during working hours whilst trying to book a holiday. The employee's dismissal was fair because she had received previous warnings and knew that this type of conduct was considered unacceptable to her employer.

One survey conducted in 1999 (by Infosec, Netpartners and Secure Computing Magazine) estimated that 76% of workers were using company time to search the internet for a new job. The results of the survey (which covered 200 international companies) also suggested that in a company of 1,000 employees, there was likely to be a loss of some £2.5 million a year as a direct result of employees using the internet for non-business purposes. The same survey reported that 50 per cent of workers were using the internet to visit 'adult sites'. In another survey, conducted the same year by Integralis Network Systems, a company specialising in network security, it was estimated that up to two hours a day were being wasted by employees who used email or surfed the internet for personal purposes. This was estimated to be costing a business with 1,000 employees about £3.9 million. There are thus major practical and cost implications for employers in terms of loss of productive working time.

Downloading material can also be a time-consuming activity, occupying valuable computer access time and running up large telephone bills in the process. Employers should rightfully be concerned about the amount of time employees spend using the internet, and should introduce policies governing such use in order to avoid excessive time-wasting.

Employee distractions **[1.12]**

Email, because of its speed and convenience, has presented employees in all types of organisations with tempting opportunities to send and receive personal and private messages indiscriminately. The world-wide web is crowded with lists of jokes being distributed widely from person to person and from company to company. The total amount of lost working time has been estimated variously as anything from half an hour a day per person up to three hours a day per employee on average.

Computer access can also tempt bored employees into wasting time playing games on screen. Unless the employer has a policy in place governing

employees' use of computer facilities and setting out the parameters, these and other time-wasting activities could cost businesses a great deal of money in terms of lost productivity.

Other problem areas

Availability of inappropriate material **[1.13]**

There is no public body with control over the quality of material that is posted on the internet and there is thus no guarantee that information accessed on a particular site is accurate, reliable, complete or up-to-date. Although the speed with which information can be updated makes the distribution of information via the internet an attractive prospect, it is not uncommon for sites to be abandoned by their creator, thus leaving out-of-date or incorrect information open to anyone who chances upon the site. Employers should be aware of this and take steps to advise their employees to scrutinise all accessed information with a critical mind. Relying on information obtained from unknown and unregulated sources could obviously lead to poor business practices.

It is well known that the internet provides an easy source of pornographic material. Because there are virtually no restrictions on what can be placed on the world-wide web, the transmission of adult and child pornography is widespread.

Individual attitudes **[1.14]**

Although email communication tends to be treated with the same degree of informality as a telephone conversation, it produces a permanent record of any dialogue. Even after an employee has deleted a message from their computer files, it can usually be retrieved because of the way in which computer systems are backed up. An email may also be replicated on several different servers, and its various elements, for example the time and date when it was sent and the subject header, may be retained and pieced together at a later date.

An employer who does not impose minimum standards of professionalism on their employees in terms of how they use email risks damaging their business reputation in the eyes of the outside world. Emails that are sent quickly and without proper thought or care often contain errors of language, spelling or grammar and are frequently constructed without any regard to sentence structure. Additionally, many people have developed the habit of writing emails in a style that is more casual or flippant than the style they would use in a business letter. The result can be that messages become unclear, distorted or ambiguous leading to misinterpretation in terms of content or the conveyance of the wrong tone or attitude. As with all forms of communication, it is not only the clarity of the message that is important, but

also the perceived professionalism and reputation of the sender and, by extension, the organisation for which they work.

Because of the speed with which it is feasible to reply to an incoming email, it is too easy for an over-worked or over-stressed employee to react in the heat of the moment to an incoming message by sending an inflammatory or vitriolic reply. Before the advent of email as a means of communication, the author of such an emotional reaction would have had enough time between printing out the letter and waiting for it to be uplifted from the out-tray to review its wording and create a toned-down and more rational re-draft.

It is advisable for all these reasons for employers to impose minimum standards of professionalism and a set of guidelines for email communication for all employees. Sample policy documents and clauses governing email use are contained in **CHAPTER 8**.

Information overload **[1.15]**

Because of the ease and speed with which email messages can be communicated to large numbers of people, many employees send messages without proper thought, and copy their messages to all and sundry 'just in case' the information may prove useful, or to 'cover their backs'. These practices can lead to severe information overload, which in turn can cause workplace stress for those who are regularly faced with an in-box containing dozens of incoming messages. The Institute of Management recently carried out a study of over 800 managers in Britain, from which it was reported that increasing volumes of email were causing an overload problem for many managers, resulting in stress. The study, titled '*Taking the Strain*', reported that keeping up with email correspondence was one of the top ten major workplace stresses.

The result of this type of overload and stress can be that the messages are not read at all, or are not dealt with promptly. Vital information may be overlooked in favour of volumes of trivia. Employees should be discouraged from forwarding messages to long circulation lists. Apart from information overload, such practices can seriously clog up the employer's communications network.

A recent trend has been for companies to designate Fridays as email-free days in an attempt to combat the overuse of internal email and the widespread stress this can cause. The aim is to reduce the amount of information that moves about from employee to employee, and encourage employees to meet face-to-face and talk about work issues instead of using email to communicate all the time. Arguably the objective behind such an incentive is commendable, although it is questionable whether just banning emails on one day of the week will achieve the desired outcome of encouraging employees to reduce

the volume of emails they send to each other and use other more appropriate methods of communication instead.

Another method of reducing an overload of email communication would be to place a limit on the number of people to whom email messages can be sent. This could be coupled with a facility whereby an employee who believed it necessary to send a particular email to more than a defined number of people to obtain authority to do so from either their line manager or the organisation's IT manager.

System overload **[1.16]**

If employees are given unfettered access to email and the internet, and frequently use these facilities to transmit large files, the system could quickly become overloaded.

Security and loss of data **[1.17]**

It is surprisingly easy to send an email to the wrong address, or accidentally copy it to another party, and even if a message arrives only at its intended destination, there is no guarantee, unless the employer introduces measures to control the distribution of email messages, that the recipient will not forward the message on to others both within and outside the organisation in random fashion. Employers' policies should state whether there are any restrictions on the number of people to whom an email can be sent.

Unlike a telephone call, if an email link fails, the sender is not always aware that the message has not reached its destination. Assumptions should not, therefore, be made by users of email that once a message is sent, the issue to which it relates has been satisfactorily dealt with.

Damage to working relationships **[1.18]**

The availability of email as a means of convenient communication appeals to those whose verbal communication skills, or willingness to engage in face-to-face discussions, are lacking. It can, unfortunately be used as a means of avoiding face-to-face communication or avoiding addressing conflict, whilst at the same time giving the false impression that the person hiding behind their computer is a 'good communicator' because they disseminate lots of information to others.

The practice of sending an email to the person at the next desk or an adjacent office should be discouraged, unless there is a tangible and sensible reason for doing so. Similarly, managers should not use email as the main means of communicating with their staff as this method of communication, used in isolation, will not allow ideas, problems and other issues which may be

important for both the business and for the employees to be properly identified, addressed and resolved.

Working relationships can be problematic enough for many individuals without the added detriment of reduced face-to-face communication. Furthermore, if there are differences of opinion, or a degree of conflict between individuals at work, these are unlikely to be capable of resolution through email communication. Realistically the only way to resolve difficulties of this nature is through open two-way face-to-face communication in which each party is willing to express their views clearly and listen fairly to the views of the other party. Curt, poorly thought out or carelessly written email messages are quite capable of creating animosity where none previously existed, and are highly likely to exacerbate any existing discord.

In summary, email should not be regarded as a replacement for other forms of communication between colleagues, but instead should be used only where it is the most appropriate method of communication for the message in question. Ultimately there is no substitute for two-way face-to-face communication between colleagues.

Company Intranets [1.19]

A company intranet is an internal system of computer communication, similar to the internet in its operation, but separate from the public telecommunications system and thus available only for employees to access through workplace computers and possibly laptops provided to employees who work remotely. Intranets are inexpensive and easy to use and can provide an excellent means for an organisation to keep its employees informed about a wide range of issues.

An intranet may, for example, be used to communicate:

- Up-to-date information about the company's products and services.
- Information about the company's customers, new contracts won and sales successes.
- Company policies and procedures.
- Details of terms and conditions that apply generally, such as holiday entitlement, pension scheme membership, private medical insurance scheme, etc.
- Job vacancies within the organisation.
- Training workshops offered on an open basis by the employer.
- Health and safety information and rules.

- The company's vision, goals and plans for the future.
- General company 'news'.

Using a company intranet to communicate this last item would remove the need for a company newsletter, thereby saving printing and production costs.

Another invaluable use to which an intranet could be put would be for online training, including induction training for new employees.

The efficient and imaginative use of a company intranet can help to foster a culture of openness, knowledge sharing and team spirit between departments and within the organisation as a whole.

Responsibility for the company intranet [1.20]

It will clearly be important for the organisation to appoint a senior manager as the person responsible for managing the intranet and ensuring that all the information posted on it is accurate and up-to-date. This person would also have responsibility for encouraging employees to use the intranet as an effective tool in day-to-day communication. One important decision to be made would be who should have the authority to post information – whether this facility should be offered to all employees, or whether only certain designated senior managers should have the authority to publish information. In either case it may be useful to include a statement within company policy that any employee who notices anything on the web-site that is wrong or out-of-date should bring this to the immediate attention of their line manager.

Security of the intranet [1.21]

One particularly important aspect of operating a company intranet is security. Since much of the information contained on the intranet will be confidential from the organisation's point of view, it will be essential to build in security systems, such as a corporate firewall. If employees are to be permitted to post information, there will also need to be a monitoring system set in place to make sure that no inappropriate information is published. A system of passwords that are changed regularly will help to protect the intranet from misuse.

A full discussion of how to set up, operate and control a company intranet is outside the scope of this book.

Use of Email and the Internet for Personal Purposes [1.22]

Employers should give careful consideration to the question of whether, and to what extent, their workforce should be permitted to use email and the

internet for personal or private purposes. In a small company where the general manager knows every employee personally and has a close involvement in the day-to-day work of each person, formal rules or restrictions may seem inappropriate or unduly burdensome. In a larger organisation, however, where many employees have access to email and/or the internet for business purposes, only the most foolhardy or naïve employer would form the view that some form of restriction was unnecessary.

The problem of employees using their employer's communications systems for personal purposes is not a new phenomenon. Traditionally, most employees have had access to their employer's telephone system to one degree or another, and in many organisations reasonable use of the telephone by employees for personal and private purposes has been accepted as the norm. The difference with the advent of email and internet access is that the scope for undetected overuse and misuse is far greater than ever was the case with telephone communication. Whilst in the old days employees might have been criticised for spending too much time making and receiving personal telephone calls, or taking extended coffee breaks, today's problems tend to centre around issues such as employees surfing the net for their holidays and playing computer games during working time. It is therefore advisable for all employers, whatever their size or business sector, to decide whether:

- to introduce a strict 'no personal use' policy'; *or*
- to permit reasonable personal use of email and the internet, for example for essential purposes or occasional use only; or
- to permit personal use during employees' own time, for example during lunch breaks; or
- to allow employees unrestricted access and unlimited use of the company's email and internet facilities, and deal with any problems of misuse on an individual basis after they have arisen.

The subject of email and internet policies and procedures is dealt with fully in **CHAPTER 8**.

Guidelines and Network Etiquette [1.23]

Irrespective of whether or not an employer decides to introduce a formal policy governing employees' use of email and the internet, it is advisable to draft basic guidelines for employees who use these facilities covering the fundamental principles of how they should, and should not, be used. This section suggests some guidelines which employers may elect to adopt or adapt for their own use.

Housekeeping [1.24]

Guidelines on the use of email should be formulated and communicated to all employees along the following lines:
Employees should:

- Check their incoming email at least once a day, but no more often than three times a day to avoid continuous interruptions.
- Turn off the system that provides an alert to the arrival of a new message.
- Reply to all incoming email messages promptly – perhaps within one or two days – even if the reply consists only of an acknowledgement.
- Refrain from using the 'urgent' prefix or unless the message is genuinely urgent from the point of view of the business.
- Arrange for a colleague to deal with their incoming emails if they are to be away from the workplace for more than one or two days, or alternatively install an automatic reply system advising that they will be unable to reply until a defined date.
- Check all email addresses before an email is sent – bear in mind that once an email has been sent, it cannot be retrieved. If a mistake is made, send an apology.
- Always complete the 'subject' field in an outgoing email message in a way that is meaningful so that the recipient can identify what the email is about quickly and correctly.
- Take care when replying to incoming emails that the existing subject field is still appropriate.
- Use common sense and/or follow any company rules regarding when emails should be retained on the computer system and/or printed out and filed.
- Organise incoming and outgoing email messages that are to be retained on the computer in a properly labelled filing system.
- Refrain from printing out email messages unless there is a specific and tangible reason why a paper copy is needed over and above the electronic copy.
- Delete old or irrelevant email messages regularly so that the computer does not contain large quantities of out-of-date material, and in order to conserve disk space.
- Be told clearly if and when they need to obtain their line manager's approval before sending out an email.

There may also be guidelines on sending attachments, a limit on the size of attachments, or even a ban on opening incoming attachments (in case of virus infection). In particular, it may be prudent to advise employees not to retain incoming attachments on the email system, but instead to save them on the computer's hard disk. This will avoid burdening the company network with large files.

Content [1.25]

In terms of the content of an email message, employees should:

- Assess whether email is in fact the most appropriate means of communication for a particular message and consider whether (for example) it may be more appropriate to arrange a meeting to discuss the matter, or make a telephone call.
- Consider whether the content of a planned email is relevant to the intended recipient – think carefully about what information others need and want, rather than disseminating information randomly to large numbers of people.
- Refrain from automatically copying emails to others within the organisation – do so only if there is a specific valid reason justifying it.
- Take care, when replying to an email that has been circulated to other people, not to automatically copy them all in on the reply.
- Refrain from copying emails to management in order to play politics, score points or land a colleague in trouble – this is likely to cause untold damage to working relationships;
- Refrain from forwarding incoming emails on to other people unless the permission of the sender is first obtained;
- Think carefully whether it is appropriate to include the automatically generated copy of the original message in the response to an email – unless it is necessary, it is often better to delete the 'email trail';
- Limit the length of email messages and refrain from sending numerous or lengthy attachments (especially photographs or graphics) that could take hours for the recipient to download and possibly clog up the system. As a general guideline, anything that cannot fit on to a 1.44 megabyte disk should not be sent by email;
- Limit the content of each email to one subject – if more than one subject needs to be covered, send more than one email;
- Make it clear what action is expected as a result of the email, and within what timescale.

Suggested statements which could be incorporated into a policy document on email use are given in **CHAPTER 8**.

Style and language [1.26]

Employees should be encouraged to treat email communication with the same degree of care, attention and professionalism as they would treat a letter sent out on company-headed notepaper. They should:

- Think before writing and take care to express their message clearly;
- Aim to make a positive impression on behalf of the organisation;
- Aim to be courteous;
- Write as concisely as possible- remembering that the message will be read on screen;
- Start and end email messages in a business-like manner avoiding terms such as 'hi there' in messages that are to be sent outside the organisation;
- Pay proper attention to grammar, spelling and punctuation – mistakes look just as unprofessional on screen as they do on paper.

Research carried out by MSN Hotmail and Debrett's found that nearly half of 2,000 email users questioned did not bother about spelling, punctuation or style when writing emails. At the same time, more than half of email recipients stated that they found such carelessness annoying.

Things to avoid [1.27]

Employees should therefore be advised to refrain from:

- Careless style and poor spelling or punctuation.
- Careless or casual use of humour or sarcasm in email communication – because it may be misinterpreted.
- Sending emails in the heat of the moment.
- Using gimmicks excessively for example the written symbol [:-)] to convey a smile.
- Using capital letters in an email – this is often interpreted as shouting.

Defining Acceptable and Unacceptable Use of Communication Systems [1.28]

It is strongly recommended that every employer should formulate and introduce a policy and rules on email and internet use for all workers within

the organisation. However, even if no formal policy or rules are put in place, there should at least be a written statement distributed to all workers that certain email and internet activities are prohibited. These would include:

- The use of unauthorised or pirated software.
- Downloading pornographic or sexually explicit material from the internet.
- Infringement of copyright through the copying or forwarding of material downloaded from the internet.
- Sending emails or email attachments containing statements or pictures that could be interpreted as sexual or racial harassment.
- Sending emails or attachments that contain derogatory or defamatory statements about any individual or organisation, or which would be likely to cause offence.
- The transmission by email of highly confidential or sensitive information outside the organisation.
- Sending or forwarding chain email messages.
- Excessive personal use.

The subject of policies, rules and procedures is dealt with fully in CHAPTER 8.

Conclusion [1.29]

The advent of email and the internet has brought many benefits and advantages for employers and employees alike, but at the same time has created a range of modern-day problems for employers. One of these problems is time-wasting by employees who may, unless regulated, choose to spend excessive amounts of working time using email and the internet for personal purposes.

Another important issue is the way in which employees treat email communication. Many people use it in a casual or slipshod manner without proper regard to correctness of style and language. This creates the risk that the outside world will gain a negative impression of the organisation. Employers should therefore take appropriate steps to ensure employees pay proper attention to matters of email housekeeping, content and style.

Questions and Answers [1.30]

Question

How can email as a means of communication save money within a business?

Answer

Communication by email is a cost-effective way of sending and receiving information. The costs associated with printing, packaging and postage can be saved and in most cases sending an equivalent email costs less than a local telephone call. There is also a potential cost saving if email messages are retained in electronic format only rather than being printed out. For marketing purposes, advertising a product or service on a website is considerably less expensive than producing a brochure and distributing it to large numbers of potential customers by conventional means.

Question

What other benefits are there to businesses as a result of email and internet access?

Answer

Email enables communications to be sent and received much more quickly than conventional means of communication. Long and short documents can be sent by email over long and short distances quickly and easily irrespective of time differences between different countries. Employees can choose when to access their incoming emails and the internet and can do so irrespective of whether they are working in the office, at home or travelling on company business. Additionally, the internet provides unlimited opportunities for companies to conduct research into an infinite variety of subjects.

Question

Is it right for an employer to be concerned about the amount of time employees spend using the internet?

Answer

There is a growing problem for employers of loss of productive time due to employees surfing the net for both legitimate business purposes and

personal entertainment purposes. Because of the sheer volume of available information, it can be a time-consuming exercise to locate information relevant to a specific query, and even once the relevant information is located, downloading a file can also be a time-consuming activity, occupying valuable computer access time and running up large telephone bills in the process. Employers should rightfully be concerned about the amount of time employees spend using the internet, and should introduce policies governing such use.

Question

Should an employer insist that their employees treat email communication in the same business-like manner as they would approach a business letter, or is it acceptable for emails to be more casual in their style?

Answer

An employer who does not impose minimum standards of professionalism on their employees in terms of how they use email risks damaging their business reputation in the eyes of the outside world. Emails that are sent quickly and without proper thought or care often contain errors of language, spelling or grammar and are frequently constructed without any regard to sentence structure. Additionally, if an email is written in a style that is casual or flippant, the result can be that its message becomes unclear, distorted or ambiguous leading to misinterpretation in terms of content or the conveyance of the wrong tone or attitude. It is therefore advisable for employers to impose minimum standards of professionalism and a set of basic guidelines for email communication.

Question

To what extent is an email message secure?

Answer

Email is not a secure means of communication and has often been compared to sending a postcard. An email message should thus not be assumed to be confidential as it may be intercepted or read by someone other than the intended recipient. Furthermore, it is surprisingly easy to send an email to the wrong address, or accidentally copy it to another party, and even if a message arrives only at its intended destination, there is no guarantee that the recipient will not forward the message on to others both within and outside the organisation in random fashion.

Question

To what extent should a manager use email communication for the purpose of communicating with staff?

Answer

Managers should not use email as the main means of communicating with their staff as this method of communication, used in isolation, will not allow ideas, problems and other issues to be properly identified, addressed and resolved. Email should not be regarded as a replacement for other forms of communication between colleagues, but instead should be used only where it is the most appropriate method of communication for the message in question. Ultimately there is no substitute for two-way face-to-face communication between colleagues.

Question

Should an employer be concerned about the extent to which employees use the organisation's communications systems for personal or private purposes?

Answer

With the advent of email and internet access, the scope for undetected overuse and misuse of communications systems is far greater than ever was the case with telephone communication. It is therefore advisable for all employers, whatever their size or business sector, to decide whether to introduce a strict 'no personal use' policy', to permit reasonable personal use of email and the internet or to allow employees unrestricted access and unlimited use of the company's email and internet facilities, and deal with any problems of misuse on an individual basis after they have arisen.

Question

What sort of guidelines should employers devise for their employees as regards the ways in which they use email?

Answer

Guidelines on the use of email should be formulated and communicated to all employees to cover housekeeping matters (for example replying promptly to incoming emails, filing diligently and deleting out of date messages), content and style and language.

2 Legal Liabilities Arising From Misuse of Email and the Internet

Introduction [2.1]

Employees who are allowed unsupervised use of email and granted unlimited access to the internet at work may inadvertently (or deliberately!) cause legal problems for their employer. One problem is that emails are not secure and they can – and do – go astray and can easily fall into the wrong hands. Another cause for concern is that many employees view email as they would a casual telephone conversation. In a telephone conversation, remarks may be made that can be retracted, modified or subsequently denied. The nature of the communication is transitory. The same is not true of an email message which, once sent, provides concrete and lasting evidence that the remark was made and by whom it was made. Four copies of the email will immediately be created: one on the sender's computer, one on the sender's server, one on the recipient's computer and one on the recipient's server. If the recipient forwards the message on to others, multiple copies will then exist. Once a message has been sent therefore, it is almost impossible to eradicate all the copies.

Even after an email message has been deleted from the computer, including deletion from the 'trash', it will remain within the computer hard-disk for a considerable period of time and can be retrieved by means of software designed specifically for that purpose. Often the various elements of an email, for example the time and date when it was sent and the subject header, are capable of being pieced together long after the email was sent. Furthermore, email messages can be used in evidence in court proceedings and employers may be required by a court or tribunal to produce them in the course of such proceedings.

It follows that email messages should not be viewed in the same way as telephone conversations, but should instead be treated with respect, with serious consideration being given to their content, tone and to whom they should be sent. It is up to each employer to make sure that their employees understand these important principles.

Use of the internet has similarly led to attitudes that 'anything goes' and that individuals have the automatic right to free speech via this medium. Although largely unregulated, the internet is not a law-free zone and legal actions can

be raised on account of inappropriate statements published on the internet, or inappropriate remarks written in an internet message.

Employer Liability [2.2]

Although the world of cyberspace, as it is known, is largely unregulated, this does not mean that employers and their employees can use electronic communication in any way they please without legal repercussions. The range of possible liabilities that can arise through misuse of email and the internet is surprisingly diverse, particularly when it is remembered that companies competing in the global marketplace inevitably use these facilities as mainstream tools. The world-wide web may have no geographical or cultural boundaries, but there are legal boundaries.

Employers may be liable in a number of ways as a result of employees' use of email and the internet. The laws of contract, defamation, copyright, harassment, obscenity and confidentiality apply to email and internet communications in the same way as they apply to traditional methods of communication. This is known popularly as 'cyberliability'.

Another worrying aspect of email and internet use is the risk of the transmission of a virus to the employer's computer system through email attachments being opened, or through software being brought in by employees to the workplace and loaded on to the employer's system without proper virus-checking.

The following is a summary of the main potential areas of liability:

Defamation [2.3]

There may be a liability for defamation if an email sent internally or externally contains material that is defamatory of an individual or of another company. The person who sent the message will be personally liable for any damage the libellous message causes to the reputation of the individual or company concerned, but the employer may also be vicariously liable. This is dealt with fully in **2.18** below.

Bullying and harassment [2.4]

If an employee sends an abusive or obscene email to a colleague, this may give rise to a claim for constructive dismissal, or, if the content of the message has sexual, racial, religious or homophobic connotations, may lead to a complaint of unlawful discrimination against the employer. The same outcome could occur following sexist, racist, religious or homophobic jokes sent by email from one employee to another or following the downloading or distribution

of sexually explicit material from the internet. Harassment is discussed in **2.26** and bullying in **2.29** below.

Publication of obscene material **[2.5]**

If an employee downloads pornographic material from the internet, and/or circulates such material internally or externally by email (or by other means), this may constitute a criminal offence under the *Obscene Publications Act 1959*. Employees who find such material offensive may also bring claims for sexual harassment to tribunal. Further information is available in **2.34** below.

Disclosure of wrongdoing **[2.6]**

Employers should take very seriously any instance of an employee coming forward with a complaint that another employee is using the internet for illegal purposes. Depending on the circumstances, such an employee may be protected against detriment and dismissal under the provisions of the *Public Interest Disclosure Act*. This is further explained in **2.39** below.

The law of contract **[2.7]**

An email message is capable of forming or varying a binding contract and the employer will be liable in contract for any breach of an agreement so formed. Further details follow in **2.47** below.

Misrepresentation **[2.8]**

Any inaccurate or misleading statement (whether deliberate or accidental) about a company's products or services can lead to legal claims of misrepresentation. This principle extends to information provided by email. In particular, if the statements have had the effect of inducing an individual or an organisation to enter into a contractual agreement to purchase the company's products or services, legal claims could ensue. More information is provided in **2.52** below.

Copyright **[2.9]**

If employees are allowed unfettered access to the internet, and randomly download whatever they access, there could be an inadvertent breach of copyright law. Full details are provided in **2.54** below.

Confidentiality **[2.10]**

Where there are no restrictions on employees' use of email, a breach of confidentiality could occur through messages being sent outside the organisation

which might contain confidential information about the company. This can easily happen as a result of a wrong email address being input, or a message being inadvertently copied to recipients on a distribution list. Additionally, employees may inadvertently or deliberately send internal emails containing confidential or inappropriate information about a colleague. The issues surrounding security and confidentiality are explored fully in **CHAPTER 4**.

The concept of vicarious liability [2.11]

Employers are responsible and will have legal liability for their employees' activities when they are using email or the internet in the course of their employment, irrespective of whether or not the employer is aware of each individual's specific activities. This is known as vicarious liability.

The concept of vicarious liability is not contained in any statute, but has developed as a result of case law. It means that an employer will be liable in law for the actions (or omissions) of an employee whenever those actions take place 'in the course of employment'. The notion of vicarious liability can be applied in many areas of the employment relationship, for example in connection with breach of safety standards, negligence in carrying out duties, fraudulent statements made by employees, acts of discrimination, etc. Thus an employer may be vicariously liable for the consequences of a defamatory message transmitted by one of its employees in an email in the same way as they could be vicariously liable for an accident caused by the careless driving of one of their van drivers.

In the course of employment [2.12]

In order for the employer to be liable, however, it must be shown that the employee whose misuse of email or the internet gave rise to legal action was acting in the course of employment when they committed the act in question. An employee can be acting in the course of their employment whether or not they are physically at their workplace, for example they may be working at home or away on company business. Equally, the time of day at which a misdemeanour takes place, and whether it is within or outside normal working hours, is irrelevant in determining whether a particular action occurred in the course of employment.

By contrast, if an employee goes off 'on a frolic of his own' (as one Court put it), and it can be shown that their actions had nothing to do with their job responsibilities or duties, then the employer is unlikely to be held liable for their actions or the consequences of those actions. For example, in the case of *Generale Bank Nederland NV v Export Credits Guarantee Department (Times Law Reports 04.08.97)*, the Court of Appeal judged that the employer could not be held liable for the acts of an employee who had assisted in the fraudulent

scheme of a third party unless those actions were within the employee's actual or ostensible authority. Even though the fraud was committed during the employee's working time and even though the opportunity to commit the fraud had largely been brought about by dint of the employee's employment, these factors were not sufficient to render the employer vicariously liable. The rules relating to vicarious liability for the dishonest acts of an employee are less onerous than those relating to acts of negligence.

In *Lister & ors v Hesley Hall Ltd House of Lords 03.05.01*, a case involving a school where sexual assaults on boy pupils were carried out by a warden employed by the school, the House of Lords held that the employer was vicariously liable for the acts of the warden. The judgment stated that the employer would be vicariously liable whenever there was a close connection between the employee's act(s) and the nature of the job duties the employee was engaged to carry out. This case in effect broadens the scope of vicarious liability.

Case study **[2.13]**

The following case study demonstrates the importance of the question of whether or not an employee is acting in the course of employment:

Case study

Joe is employed as buyer for a major engineering firm. In the course of his duties, Joe corresponds regularly by email with various suppliers both for the purpose of obtaining information about new products and for reviewing price lists and details of any available discounts. Joe has been particularly busy lately because one of his colleagues is off sick, and the pressure of work is mounting. He has received an email from a regular contact, Harry Harman of XYZ Office Supplies Ltd, detailing a special offer on printers, and another on desk-top photocopiers. If 20 or more printers are ordered within 7 days, a discount of 20 per cent will apply. The same discount will be applied to the photocopiers if ten or more are ordered. Joe, whose mind was not fully on his job that morning, has hit the 'reply button' on his computer and inadvertently sent an email to XYZ confirming the company's agreement to purchase 20 printers.

By coincidence, Joe's estranged wife, Josephine, works for the same firm as an evening office cleaner. Josephine is a devious character and is very bitter about her recent separation from Joe. She has, through illicit means, obtained a list of the suppliers with whom Joe regularly deals in his job. Since she is planning to leave the company anyway, and go and live with

her sister in Majorca, Josephine has decided to seek revenge on Joe and create trouble for him at work. She accesses Joe's computer one evening and sends an email to Harry at XYZ Office Supplies Ltd confirming that the company wishes to purchase thirty desk-top photocopiers at the discounted price, typing her own name at the bottom of the email.

Several weeks later, long after Josephine has absconded to Majorca, Joe uncovers both his own mistake and the devious activities of his ex-wife. In the meantime, XYZ Office Supplies has delivered both the printers and the desk-top photocopiers and is insisting that both deals should be honoured, threatening legal action if the company refuses to pay for them.

What would the company's liability be for the actions of Joe and Josephine?

The company would be vicariously liable for Joe's actions because, as company buyer, his job involves purchasing equipment from suppliers. He thus has actual and ostensible authority to commit the company to a contract to buy printers, and the email was sent in the course of his duties. The contract is a binding one which the company would have to honour unless they could persuade the supplier to agree voluntarily to take the printers back.

By contrast, however, the company would not be liable for Josephine's activities, since the job of office cleaner would not, by any stretch of the imagination, involve purchasing photocopiers from a supplier, nor using an office computer for work purposes. Josephine was not acting in the course of her employment when she accessed Joe's computer and placed the order for the photocopiers.

Supply of computer **[2.14]**

Generally, an employer will be vicariously liable for the actions of an employee using email or the internet if the means are authorised, even if the specific act committed by the employee is not. Given that many employees are supplied with a computer by their employer for the performance of their duties, and similarly provided with access to email and the internet by the employer, misuse of these facilities by such employees, i.e. using the facilities in ways that are not authorised by the employer, will mean the employer will be liable in law for the outcome of the misuse. By contrast, an employee who is not supplied with a computer at work, nor with access to email and the internet, (like Josephine in the above case study), will not be acting in the course of

employment for the purposes of vicarious liability if they illegitimately use the computer and create some mischief for the employer.

Checklist **[2.15]**

The following checklist is a guide to establishing whether or not an employee is acting in the course of employment when misusing email or internet facilities. If the answer to the first three questions is 'yes' and the answer to the following three questions is 'no', then it is likely that the employer would be vicariously liable for the actions of the employee.

- Has the employer provided the employee with a computer, and with access to email and the internet?
- Does the employee have authority to send emails, or to communicate via the internet, as part of their job?
- Was the employee's misdemeanour committed whilst they were using email or the internet for purposes associated with their normal job duties (for example was the employee sending a work-related email to a business contact?).
- Does the employer have a clear policy in place governing acceptable and unacceptable uses of email and internet facilities?
- Has this policy been properly communicated to the employee in question such that their misdemeanour is clearly a breach of the policy?
- Has the employee been given clear instructions and/or training in appropriate use of email and the internet?

Liability for acts of harassment **[2.16]**

Employers will also be liable in law for acts of harassment by their employees on grounds of sex, sexual orientation, race, religion or disability. Here the liability in law is wider than the strict limitations of vicarious liability. This is dealt with below under **2.28**.

Reducing liability by introducing a policy **[2.17]**

The likelihood of being held liable in law for employees' email or internet wrongdoings can be reduced if the employer introduces a rigorous policy defining acceptable and unacceptable uses of these facilities, and takes positive steps to communicate and apply the policy in practice. By taking such actions, the employer may be able to show that an employee who commits an act which is in clear breach of the policy was not acting 'in the course of employment'. Email and internet policies are addressed fully in CHAPTER 8.

Defamation [2.18]

Written material will be defamatory (i.e. libellous) if it involves the publication of an untrue statement which tends to lower a person in the estimation of right-thinking members of society generally. Such material is capable of defaming a company as well as an individual. Where a defamatory statement is made verbally, it is known as 'slander', whilst the term 'libel' means a statement that is committed to a permanent form. It is likely that a defamatory statement made in an email message would be regarded as libel rather than slander since email messages are capable of being printed and stored.

Substantial damages can be awarded following a successful claim for defamation, and in the case of defamation by email or on the internet, the sheer speed with which a defamatory statement can reach a large audience may mean that the damage to the reputation of the individual or business augments within a very short time-scale.

There is no distinction in the law of defamation between the content of an internal email and text contained in a printed letter or other written communication. Thus, there may be liability for defamation if an email sent internally or externally contains material that is defamatory of an individual or of another company. Similarly, if a defamatory message is posted on the internet, liability for defamation will accrue. If, however, a statement made is true, this will provide a defence to any claim for defamation.

Who is Liable? [2.19]

The person who sent the message will be personally liable for any damage the libellous message causes to the reputation of the individual or company concerned, but the employer may also be vicariously liable if the employee was acting in the course of their duties when they sent the email. This means that the employer will be regarded, for the purposes of a legal claim, as the author of the offending statement. The *Defamation Act 1996* expressly states that:

> 'Employees or agents of an author, editor or publisher are in the same position as their employer or principal to the extent that they are responsible for the content of the statement or the decision to publish it'.

In practice, it is much more likely that an employer will be sued for defamation than an individual employee since, from the point of view of the defamed party, the employer is far more likely to be in a position to pay out compensation.

The Norwich Union case [2.20]

In 1997, Norwich Union settled a major defamation action brought against them by their competitor, Western Provident Association, as a direct result of a widely circulated internal email message which was defamatory of Western Provident's financial position. The email circulating amongst Norwich Union employees had made untrue and damaging statements alleging there were financial problems at Western Provident and suggested that the firm was being investigated by the DTI. The outcome was that following a law suit by Western Provident for libel and slander, Norwich Union paid out £450,000 in damages and costs to Western Provident for defamation. Interestingly, the courts stepped in and ordered Norwich Union to preserve all the offending messages, and to hand over hard copies of these to Western Provident.

Liability as the publisher [2.21]

In addition to vicarious liability for defamatory statements made by their employees, the employer may be liable as the publisher of any offending statements made via electronic communication. Under the *Defamation Act 1996*, an employer can be held liable if they are the author, editor or publisher of a defamatory statement. A publisher is defined in the Act as someone 'whose business is issuing material to the public, or a section of the public, who issues material containing the statement in the course of that business'. Essentially an employer may be held to be the publisher of an offending statement if they are involved in any way in the dissemination of the defamatory statement. This means that if the employer controls, edits or vets what employees write, they may be held to be the publisher of the material. This does not, of course, mean that employers should give employees a free hand to write whatever they deem appropriate, or turn a blind eye to their employees' electronic communications, but rather that they should take concrete steps to make sure no defamatory messages are written or sent out.

Similarly, the fact that an employer provides their employees with computers and with email and internet access may be sufficient for the employer to be regarded as the publisher of all communications sent out by these media.

Defence against liability for defamation [2.22]

The *Defamation Act 1996, s 1(1)* provides a defence for organisations who use electronic communications against claims of defamation if they can show that:

- they were not the author, editor or publisher of the statement complained of;

- they took reasonable care in relation to its publication; *and*
- they did not know, and had no reason to believe, that what they did caused or contributed to the publication of a defamatory statement.

The Act goes on to say [*s 1(5)*] that:

> 'In determining ... whether a person took reasonable care, or had reason to believe that what he did caused or contributed to the publication of a defamatory statement, regard shall be had to –
>
> (a) the extent of his responsibility for the content of the statement or the decision to publish it,
>
> (b) the nature or circumstances of the publication, and
>
> (c) the previous conduct or character of the author, editor or publisher.'

Example [2.23]

In the case of *Godfrey v Demon Internet Ltd* [*1999*], the High Court held that an internet service provider was liable for a defamatory email posted on a newsgroup site. This was because they had failed to remove the statement from the newsgroup as soon as they received notification that the statement was untrue. Although the internet service provider was neither the originator nor the publisher of the statement, they were still held liable in law for defamation, because, having been notified that the statement was untrue and been asked to remove it, they failed to do so promptly and continued to allow it to be posted. Thus the defence available under the *Defamation Act 1996, s 1(1)* that the publisher of a defamatory statement did not know, and had no reason to believe, that what they did caused or contributed to the publication of a defamatory statement could not be upheld.

Making employees aware [2.24]

Employers should take the responsibility of ensuring that their employees have sufficient awareness of the law on defamation to understand that any information they distribute by email or via the internet must not contain untrue or derogatory statements about, for example, a competitor. Text explaining the fundamental principles of the law on defamation could be included, for example, in an employee handbook. A model statement that could be incorporated into an employee handbook is given in the next paragraph. It is also recommended that employers make it clear to all their workers that the making of defamatory statements, whether in internal or external communications, will be regarded as a disciplinary offence. It may