

(Draft)  
**ELECTRONIC COMMUNICATIONS POLICY**  
Employment Law Training Ltd  
[www.eltraining.co.uk](http://www.eltraining.co.uk)



## **INTRODUCTION**

The use of electronic communications within the Company is encouraged, as its appropriate use facilitates communication and improves efficiency. Used correctly, it is a facility that is of assistance to many employees. Its inappropriate use, however, causes many problems, ranging from minor distractions to legal claims against the company. This policy sets out the company's view on the correct use of the electronic communication systems and explains how this can be achieved, as well as the company's response to inappropriate use.

This policy addresses the following forms of electronic communication:

- Company computers
- Email
- Internet
- Facsimile
- Corporate and Personal Social Networking ('Blogging')
- Land-line and Mobile Telephones (including 'Voicemail')

## **COMPANY COMPUTERS**

The Company has licences for the use of computer software from a variety of outside companies. The Company does not own this software or its related documentation and, unless authorised by the software developer, neither the Company nor any of its employees have the right to reproduce it. To do so constitutes an infringement of copyright. Employees will be held responsible for any action taken against the Company in respect of any breaches of copyright and, if employees are discovered to have breached this condition in any way they may face disciplinary action under the Company's disciplinary procedure, which may result in their summary dismissal.

Employees are authorised to gain access to certain computer systems and, within those systems, certain programs and data. Employees must not attempt, alone or in concert with others, to gain access to data or programs to which they have not been authorised. Similarly, no computer file or program originating from the Company is to be copied or installed on computers outside the ownership of the Company without written approval from (name).

The Company's computer network makes it vulnerable to viruses. Therefore, only duly authorised personnel have the authority to load program software or files onto the network system. Data compatible with the Company's system may be loaded only after being checked for viruses by authorised personnel. A list of authorised personnel may be obtained from (name).

The Company reserves the right to audit computers and associated IT equipment from time to time. Any equipment issued to employees for use outside their normal place of work remains the property of the Company. The Company may recall this equipment at any time and the employee must take all reasonable precautions to protect the equipment from theft and damage. Employees may be issued with a password and this must not be written down or disclosed unless authority by (name) has been given.

There are computer games on the network. Employees may only access these outside their normal working hours (eg, during lunch breaks or before and after work).

## **INTERNET, EMAIL, FACSIMILE AND VOICEMAIL**

The Internet has been installed by the Company in order to increase the efficiency of information searches. Employees should follow these guidelines when using the Internet, the Company's electronic mail system ('email'), voicemail ('voicemail') and facsimile equipment ('fax'):

The email, fax equipment and voicemail systems are the Company's property and have been installed by the Company solely to facilitate business communications. Although employees have an individual password to access certain systems, their email and voicemail messages are accessible at all times by the Company.

All messages composed, sent or received on the email, fax or voicemail systems are and remain the property of the Company and may be disclosed within or outside the Company without employees' permission. They are not employees' private property. Back-up copies of email and voicemail may be maintained and referenced by the Company at any time for business reasons.

The style and content of messages must be consistent with the standards that the Company expects from written communications.

Email should not be used as a substitute for face-to-face communication. 'Flame-mails' (emails that are abusive) can be a source of stress and damage work relationships. Hasty messages, sent without proper consideration, can cause unnecessary misunderstandings.

As the Company provides the email and voicemail systems to assist employees in the performance of their job, employees should only use them for official Company business. Email messages should only be sent to those for whom they are particularly relevant. While the Company recognises a certain amount of incidental and occasional personal use of email, voicemail and fax may occur, these messages will be treated the same as other messages, and should not be considered as private. Therefore, employees should never use email, fax or voicemail to transmit any messages they would not want read or heard by a third party. Any incidental personal use must only take place outside normal working hours and not at any time which interferes with the proper performance of employees' duties.

Employees may never use the Company's email, fax or voicemail systems to transmit inappropriate messages that are seen as insulting, obscene, sexually explicit, degrading, disruptive or offensive by other persons, or harmful to morale, or contrary to the Company's business interests or in any way unlawful. Examples of inappropriate transmissions include, but are not limited to:

- sexually-explicit messages, cartoons or jokes;
- ethnic, sexual, religious or racial slurs;
- any other message that can be construed to be offensive or the harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability or religious or political beliefs;
- any communication which disparages the Company or its business, or any employees, clients or customers.

If employees are discovered to have breached this condition in any way they may face disciplinary action under the Company's disciplinary procedure, which may result in their summary dismissal.

The Company's email system must not be used to send (upload) or receive (download) confidential information in an unauthorised manner without prior authorisation from (name).

Access to the Internet is granted based on legitimate business requirements. Employees should avoid downloading information on the Internet that is not job specific or business-related. In particular, employees should not download, retain or display any materials that are derogatory, obscene, defamatory and/or harassing. In addition employees should not download, or attempt to download any music, nor carry out any financial transactions including banking, any purchases of goods, on-line gaming etc. Any accidental or unintended accessing of such sites should be reported immediately to (name). Also, time used to surf the Internet should be reserved for business needs and concerns. Explorer should only be open if the Internet is actually being used to avoid the Company incurring unnecessary line charges.

Employees should also be aware that while there are certain safeguards to prevent unauthorised access, the Company's email system, the Internet and the Company's fax and voicemail systems are not totally secure, and access by unauthorised persons is possible. The privacy of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message. Further, the use of passwords for security does not guarantee confidentiality.

While employed by the Company, employees will have access to confidential information as a result of electronic communications on email, fax and/or voicemail. The same duty of non-disclosure of confidential information applies with respect to these electronic transmissions as with all other the Company files, records, lists and documents. Unauthorised disclosure of any confidential information by use of the email, fax or voicemail systems is strictly prohibited and will subject you to disciplinary action, up to and including termination of employment.

Employees are prohibited from the unauthorised use of the passwords and encryption keys of other employees to gain access to any other employee's email management. Employees are not authorised to retrieve or read any email, fax or voicemail messages that are not sent to them. Any exception of this policy must receive prior approval from (name).

## **CORPORATE AND PERSONAL SOCIAL NETWORKING (IE. 'BLOGGING')**

### **What is Social Networking (or 'Blogging')?**

A blog (short for web log) is a user-generated website, where entries are made in a journal style and displayed in reverse chronological order.

Blogs often provide commentary or news on a particular subject (corporate social networking), while some function as more personal, online diaries (personal social networking).

A typical blog combines text, images and links to other blogs, web pages and other media related to its topic. Some focus on photographs (photoblog), videos (vlog) or audio (podcasting) and are part of a wider network of social media.

A crucial part of the blog is for readers to be able to leave comments in an interactive format.

A Corporate blog can enhance collaboration internally and with clients, increase work efficiency, lead to a dramatic reduction in email traffic, enhance employee participation, improve recruitment and contributes to marketing.

### **Guidelines For Corporate and Personal Social Networking (ie. 'Blogging')**

The Company has a Corporate Social Networking system but it also understands that some employees may wish to take part in a separate personal social networking system outside of work.

Despite the benefits outlined above there is a need to have the following guidelines in place to ensure that employees are consistent in their use of both the Corporate and their personal social networking systems. They are not intended to restrict the benefits and Managers will not adopt an unnecessarily restrictive approach.

Blogs or websites which do not identify the person as a Company employee, do not discuss the Company (including clients and customers) and are purely about personal matters would normally fall outside these guidelines.

#### Corporate Social Networking

*(Either)* The company has an internal blog which serves as strong communication and information sharing tools within the Company. Generally speaking, anyone can write comments to any post in this corporate blog as long as the general guidance below is observed. Although the system is

effective it does not substitute for conversation and employees are encouraged to use this form of communication if it is more appropriate.

(Or) The Company has an external blog which is used as participatory communications tools that can build networks, connections and links between the key audiences of a company, helping it to leverage market conversations and improve the overall business. Generally speaking, anyone can write comments to any post in this corporate blog as long as the general guidance below is observed.

All employees must adhere to the following Company ethics when using the system:

Blogger Code of Ethics:

1. We will tell the truth.
2. We will acknowledge and correct any mistakes promptly.
3. We will not delete comments unless they are spam, off-topic, or defamatory.
4. We will reply to comments when appropriate as promptly as possible.
5. We will link to online references and original source materials directly.
6. We will disagree with other opinions respectfully.

*(External Blog only)* To protect against spam, off-topic and profane comments, all comments are reviewed by *(name)* before being posted to the blog. Comments are continuously approved during normal business hours.

### Personal Social Networking

Employees are allowed to update their personal blogs from a company computer at work outside their normal working hours as long as the general guidance below is observed.

### General

Employees who already have a personal blog or website which indicates in any way that they are employed by the Company should inform their manager.

If employees wish to start blogging, and the blog/website states that they work for the Company they should inform their manager.

Where employees' blogs make it clear that they work for the Company (either on the corporate or personal blogs), it should include a simple and visible disclaimer such as *"these are my personal views and not those of the Company"*.

Unless there are specific concerns about the nature of their job, employees are free to talk about the Company on their blog. Employees must consult their manager if in any doubt.

Employees must not reveal confidential information or trade secrets. This might include aspects of Company policy or details of internal Company discussions, as well as any information on customers or clients. Employees must consult their manager if they are unclear about confidential information or trade secrets.

Employees must not use offensive, defamatory, discriminatory or otherwise inappropriate comments in a blog (whether corporate or personal). This will not be tolerated and such behaviour may result in both disciplinary action which may lead to dismissal and personal liability for the employee.

Employees who believe that something on their blog or website gives rise to concerns about a conflict of interest and in particular concerns about impartiality or confidentiality, this must be discussed with their manager.

If an employee is offered payment for blogging this could constitute a conflict of interest and they must consult their manager.

If an employee is approached by the media or press about posts on their blog that relate to the Company employees should talk to their manager before responding.

Although employees are encouraged to participate in blogging, this should only take place during lunch breaks or before and after working hours and not at any time which interferes with the proper performance of their duties.

## **COMPANY TELEPHONES**

### **Land-Line Telephones**

The Company's telephone lines are for the exclusive use by employees in connection with the Company's business. Whilst the Company will accept essential personal telephone calls concerning an employee's domestic arrangements, excessive use of the telephone for personal calls is prohibited. This includes lengthy, casual chats and calls at premium rates. Not only does excessive time engaged on personal telephone calls lead to loss of productivity, it also constitutes an unauthorised use of the Company's time. If the Company discovers that the telephone has been used excessively for personal calls, this will be dealt with under the Company's disciplinary procedure and the employee will be required to pay to the Company the cost of personal calls made.

Acceptable telephone use should be no more than five minutes of personal calls in each working day. Personal telephone calls should be timed so as to cause minimum disruption to the employee's work and should, as a general rule, only be made during breaks except in the case of a genuine emergency.

As telephone calls are monitored and recorded, employees wishing to make or take a particularly sensitive, private or confidential personal telephone call, they are advised that they can use the following telephones: *(details – employers may wish to install a pay phone for these purposes)*. These telephones will not be subject to any form of monitoring or recording by the Company.

### **Mobile Telephones**

Particular attention is called to the need for extra security for mobile telephones. When not in use, they must be securely locked away. Under no circumstances should they be left in an unattended vehicle (even if locked), as this would invalidate the insurance.

Company mobile phones are provided for Company use only, but may be used for reasonable personal calls on occasion. The Company reserves the right to require employees to repay, or to deduct from employee's wages, the cost of any personal calls.

It is illegal that a driver should use a hand-held microphone or telephone handset whilst his or her vehicle is moving.

Whilst The Road Vehicles (Construction and Use) Regulations permit the use of hands-free mobile phone devices in vehicles, the Company's foremost consideration is the safety of its staff. The

Company has consequently adopted the policy recommended by the Royal Society for the Prevention of Accidents, which is set out below:-

You must not make or receive a call on a mobile phone (whether hand-held or hands-free) as the driver of a vehicle unless it is parked in a safe place. No line manager shall require an employee to receive a call on a mobile phone whilst driving.

If a Company phone is lost, stolen or damaged as a result of an employee's negligence, the Company may require the employee to repay the cost of the phone or deduct this amount from the employee's wages.

Failure to comply with these rules may lead to disciplinary action. You will also be called upon to indemnify the Company for any loss or liability it incurs as a result of your failure to abide by these rules. The Company will accept no liability for criminal prosecutions, fines (whether fixed-penalty or otherwise) or other sanction imposed on the employee as a result of a breach of these rules.

## **MONITORING AND INTERCEPTION OF COMMUNICATIONS**

Employees must be aware that their incoming and outgoing email messages, whether internal or external, the internet sites accessed during the course of their employment, telephone calls and voicemail may be intercepted by the Company. The Company may also track the history of internet sites that employees have visited. The Company will take all possible steps to ensure that monitoring is carried out as unobtrusively as possible and will treat the results of monitoring in confidence. Personal messages will not knowingly be intercepted.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the Data Protection Act 1998 allow the Company to reasonably monitor your communications. While we are required to inform you that interception or monitoring may take place, it is not necessary to gain individual consent when we are monitoring your communications for the following reasons:

- To ensure effective operation of a system.
- To detect the unauthorised use of a telecomms system.
- To ensure that all employees are treated with respect and dignity at work, by discovering and eliminating any material that is capable of amounting to harassment under the terms of the Company's anti-harassment policy.
- To provide evidence of a transaction.
- For quality control or training purposes.
- To check messages for an absent member of staff.
- To monitor calls to a confidential support line.
- To prevent or detect a crime.
- In the interest of security.
- To prevent the unauthorised use of the computer/telephone system – ie. ensuring that the company e-mail and telephone policies are not breached.

To ensure compliance with the regulations, in cases where interception is carried out for any reasons other than those stated above, we will ensure we obtain your consent, or implied consent of both the sender and recipient of any message intercepted so there is no breach of privacy under the Human Rights Act.

## **LEGAL ACTION AGAINST THE COMPANY**

Messages sent via any electronic communication system can give rise to legal action against the Company. Claims such as defamation, breach of confidentiality, copyright or contract, for example,

could arise from misuse of the systems and employees also need to understand that this could lead to personal liability. It is, therefore, vital for electronic messages to be treated like any other form of correspondence and where necessary hard copies to be retained. Employees are also reminded that messages are disclosable in legal action commenced against the company.

#### **FAILURE TO ADHERE TO THE POLICY**

Failure to follow this policy is a disciplinary matter and will be dealt with under the Company's Disciplinary procedure. In very serious cases this could result in summary dismissal for gross misconduct after the formal processes have been followed.

**2010**

**Employment Law Training Ltd**  
[www.eltraining.co.uk](http://www.eltraining.co.uk)

| -