EMAIL AND INTERNET POLICY AND PROCEDURE

Introduction

This document does not form part of your contract of employment and may be changed from time to time in line with current best practice and statutory requirements, and to ensure that organisational needs are met. You will be consulted and advised of any changes as far in advance as possible of the change being made, unless the change is required by statute.

The Organisation encourages its employees to use e-mail and the internet at work where this can save time and expense. However, it requires that employees follow the rules below. It is a term of each employee's contract that he/she complies with these rules, and any serious breach could lead to dismissal. Any employee who is unsure about whether something he/she proposes to do might breach this e-mail and internet policy should seek advice from his/her manager.

Although the Organisation encourages the use of e-mail and the internet where appropriate, their use entails some risks. For example, employees must take care not to introduce viruses on to the system and must take proper account of the security advice below. Employees must also ensure that they do not send libellous statements in e-mails as the Organisation could be liable for damages.

These rules are designed to minimise the legal risks to the Organisation when its employees use e-mail at work and access the internet. Where something is not specifically covered in this policy, employees should seek advice from their manager. Employees with access to personal data are in a particularly sensitive position and must bear in mind at all times the provisions of the Data Protection Act 1998.

Technology and the law change regularly and this policy will be updated to account for changes as and when necessary. Employees will be informed when the policy has changed but it is their responsibility to read the latest version of this document.

Use of e-mail

Contents of e-mails

E-mails that employees intend to send should be checked carefully. E-mail should be treated like any other form of written communication and, as such, what is normally regarded as unacceptable in a letter is equally unacceptable in an e-mail communication.

The use of e-mail to send or forward messages which are defamatory, obscene or otherwise inappropriate will be treated as misconduct under the disciplinary procedure. In serious cases this could be regarded as gross misconduct and lead to dismissal.

Equally, if an employee receives an obscene or defamatory e-mail, whether unwittingly or otherwise and from whatever source, he/she should not forward it to any other address.

Statements to avoid in e-mails include those criticising other organisations or their staff, those stating that there are quality problems with goods or services of suppliers or customers, and those stating that anyone is incompetent.

Corporate information to be included in e-mails

Employees should ensure that official corporate information is given on any e-mails that they send. An example of the e-mail layout is provided below:

Adele Scott

Development Officer

ABC Ltd

Organisation No. 123456789

123 Big Road, Bigtown, Big County, AB1 1BA, UK

Tel (+44) (1) 11 1111 111

Fax (+44) (1) 11 1111 111

Registered Scottish charity number…….

Company limited by guarantee registered in Scotland number….

This message is intended for the use of only the person(s) ('Intended Recipient') to whom it is addressed. It may contain information that is privileged and confidential. Accordingly any dissemination, distribution, copying or other use of this message or any of its content by any person other than the Intended Recipient may constitute a breach of civil or criminal law and is strictly prohibited. If you are not the Intended Recipient, please contact the sender as soon as possible.

CCing

Employees should exercise care not to copy e-mails automatically to all those copied in to the original message to which they are replying. Doing so may result in disclosure of confidential information to the wrong person.

Attachments

Employees should not attach any files that may contain a virus to e-mails, as the Organisation could be liable to the recipient for loss suffered. The Organisation has virus-checking in place but, if in doubt, employees should check with the IT department.

Employees should exercise extreme care when receiving e-mails with attachments from third parties, particularly unidentified third parties, as these may contain viruses.

Personal use of e-mail

Although the e-mail system is primarily for business use, the Organisation understands that employees may on occasion need to send or receive personal e- mails using their work address. When sending personal e-mails, employees should show the same care as when sending work-related e-mails.

Monitoring of e-mail

The Organisation reserves the right to monitor employees' e-mails, but will endeavour to inform an affected employee when this is to happen and the reasons for it. The Organisation considers the following to be valid reasons for checking an employee's e-mail:

- If the employee is absent for any reason and communications must be checked for the smooth running of the business to continue.

- If the Organisation suspects that the employee has been viewing or sending offensive or illegal material, such as material containing racist terminology or nudity (although the Organisation understands that it is possible for employees inadvertently to receive such material and they will have the opportunity to explain if this is the case).
- If the Organisation suspects that an employee has been using the e-mail system to send and receive an excessive number of personal communications.
- If the Organisation suspects that the employee is sending or receiving e-mails that are detrimental to the Organisation.

When monitoring e-mails, the Organisation will, save in exceptional circumstances; confine itself to looking at the address and heading of the e-mails. Employees should mark any personal e-mails as such and encourage those who send them to do the same. The Organisation will avoid, where possible, opening e-mails clearly marked as private or personal.

The Organisation reserves the right to retain information that it has gathered on employees' use of e-mail for a period of [one year].

Use of internet

Authorised internet users

Where an employee has been provided with a computer with internet access at his/her desk, he/she may use the internet at work.

Not everyone in the Organisation needs access to the internet at work. Anyone who does not have access but believes that he/she requires it should contact his/her manager and make a written request, setting out the reasons why access should be allowed.

Sensible internet use

Where employees are allowed access to the internet at work they are expected to use it sensibly and in such a manner that it does not interfere with the efficient running of the Organisation. For example, where it would be quicker to make a telephone call than to engage in an internet search for the required information, then the telephone call should be made.

Employees may be called upon to justify the amount of time they have spent on the internet or the sites that they have visited.

The Organisation encourages employees to become familiar with the internet and does not currently impose any time limitation on work-related internet use. It trusts employees not to abuse the latitude given to them, but if this trust is abused it reserves the right to alter the policy in this respect.

Removing internet access

The Organisation reserves the right to deny internet access to any employee at work, although in such a case it will endeavour to give reasons for doing so.

Registering on websites

Many sites that could be useful for the Organisation require registration. Employees wishing to register as a user of a website for work purposes are encouraged to do so. However, they should ask their manager before doing this.

Licences and contracts

Some websites require the Organisation to enter into licence or contract terms. The terms should be printed off and sent for approval in advance or e-mailed to the CEO before an employee agrees to them on the Organisation's behalf. In most cases, there will be no objection to the terms and it is recognised that the free information provided by the website in question may save the Organisation money. Employees should, however, always consider whether the information is from a reputable source and is likely to be accurate and kept up to date, as most such contract terms will exclude liability for accuracy of free information.

Downloading files and software

Employees should download files on to only those PCs with virus checking software and should check how long the download will take. If there is any uncertainty as to whether the software is virus-free or whether the time the download will take is reasonable, the relevant line manager and the Organisation's IT personnel should be consulted.

Using other software and hardware at work

The Organisation does not allow employees to bring software or hardware into the office without the CEO's or IT personnel's consent.

Personal use of the internet

Although the e-mail system is primarily for business use, the Organisation understands that employees may on occasion need to use the internet for personal purposes. Employees may access the internet at work for personal purposes provided that:

- such use is limited to no more than [20 minutes] in any day;
- the internet is not used to access offensive or illegal material, such as material containing racist terminology or nudity;
- they do not enter into any contracts or commitments in the name of or on behalf of the Organisation;
- they do not arrange for any goods ordered on the Internet to be delivered to the Organisation address or order them in the Organisation's name.

Optional

[*Employees should not use the internet for personal purposes before working hours begin or after they end. The Organisation has security concerns about staff arriving early and leaving late and it is harder to monitor use of the internet at such times*].

Disciplinary action

Misuse of computers is a serious disciplinary offence. The following are examples of misuse:

- Fraud and theft
- System sabotage
- Introduction of viruses and time bombs
- Using the system for excessive private work or any game playing
- Breaches of Data Protection Act

- Sending abusive, rude or defamatory messages via electronic mail
- Hacking
- Breach of Organisation security procedures and email and Internet Policy.

This list is not exhaustive. Depending on the circumstances of each case, misuse of the computer system is likely to be considered a gross misconduct offence, punishable by dismissal. Misuse amounting to criminal conduct may be reported to the police.

Monitoring of internet access at work

The Organisation reserves the right to monitor employees' internet usage, but will endeavour to inform an affected employee when this is to happen and the reasons for it. The Organisation considers the following to be valid reasons for checking an employee's internet usage:

- If the Organisation suspects that the employee has been viewing offensive or illegal material, such as material containing racist terminology or nudity (although the Organisation understands that it is possible for employees inadvertently to view such material and they will have the opportunity to explain if this is the case).
- If the Organisation suspects that the employee has been spending an excessive amount of time viewing websites that are not work related.

The Organisation reserves the right to retain information that it has gathered on employees' use of the internet for a period of [one year].

General

The aim of these rules is to be helpful, and to set guidelines on the use of e-mail and the internet at work for the smooth and efficient running of the business.

If there is anything in these rules that an employee considers to be unworkable or does not understand, he/she should notify his/her manager.

Self-employed contractors, agency workers or any other individuals working temporarily in the Organisation should be made aware of the rules regarding the use of e-mail and the internet.

New members of staff should be shown this policy as part of their induction.

Related Policies and Procedures

- Disciplinary Policy
- Data Protection Policy / Confidentiality Policy

Implementation Date: _____

Review Date: _____

Signed: _____

(for and on behalf of the Management Committee)