INTERNET AND E-MAIL POLICIES

Updated by Don Bridle, April 2012 *(reviewed October 2011)*

Many organisations have not yet taken the simplest of steps to protect themselves against legal liabilities from the misuse of e-mail by employees. This includes problems of viruses and breaches of confidentiality but also e-mails being admissible as evidence in a dispute.

The Data Protection Act and a draft Code of Practice need to be considered. Along with the potential impact of the Regulation of Investigatory Powers Act 2000 and the Human Rights Act 1998, which came into force in October 2000, they all have implications for the Golf Club. In addition employers will need to consider their employees' expectation of privacy if and when monitoring their e-mails.

Golf Clubs should consider introducing an e-mail policy in order to maintain security and to provide guidelines for employees. An employee could use the computer system to send personal e-mails which could give rise to liability for the employer.

The main areas of concern facing employers are:

- Viruses
- Confidentiality
- Discrimination and sexual harassment
- Pornography
- Copyright
- Defamation, evidence and disclosure
- Disclaimers
- Business correspondence regulations

VIRUSES

Organisations must be vigilant as to new viruses which are being developed. Employees need to be warned about opening computer systems to others simply by logging on to the Internet. Only a few years ago it was assumed that viruses were 'caught' by opening attachments from external sources without using the relevant virus scanning software which should be in place. Now merely the sending and receiving of e-mails allows external influences to gain access to the individual computer/system.

CONFIDENTIALITY

Confidentiality can be compromised, especially when using Internet based e-mail systems. Employees must be clearly aware that anything sent electronically is normally susceptible to interception. Also if confidential information is sent it is important to make the recipient aware. A generalised notice of confidentiality is not considered adequate as it does not distinguish confidential from non-confidential information.

DISCRIMINATION AND SEXUAL HARASSMENT

The EC Commission's Code or Practice on protecting the dignity of women and men at work defined sexual harassment as, "physical, verbal or non-verbal conduct" which is "unwarranted, unreasonable and offensive to the victim" and "which creates an intimidating working environment for the victim".

E-mails which contain racist jokes, unwanted communications or explicit language have become the basis for an increasing number of claims of sexual harassment. When such harassment happens in the workplace the employer must show that reasonable steps to avoid such actions have been in place. The introduction of a policy outlining the use of e-mails within the working environment will clearly be of help in such situations.

PORNOGRAPHY

The downloading of pornographic material from the Internet will give rise to criminal liability under the Obscene Publications Act 1959. Employers need to be aware and prohibit such activities.

COPYRIGHT

Under the Copyright Designs and Patents Act 1988 copyright can be infringed by making an electronic copy and making a "transient" copy (which occurs when sending an e-mail). Copyright infringement is now very common, as more and more people forward text, graphics, audio and video clips by way of e-mail systems. Therefore employees must be warned that the copying of a third party work without consent will in most cases constitute copyright infringement.

DEFAMATION

The ease of using e-mail may encourage individuals to take a more relaxed attitude which can lead to unguarded comments being made. Such a relaxed, open attitude can encourage employers and their employees to forget that such electronic "conversations" can produce a record which is absent in telephone conversations (although the parties may keep a record of the call). Any comments made in an e-mail can be used in support, or in defence of, an organisation's legal position in the event of a dispute. E-mails are potentially discoverable documents in this event.

DISCLAIMERS

A disclaimer is a pre-emptive assertion designed to limit an organisation's potential liability with respect to information being communicated. A general disclaimer which tries to cover everything

may well not be effective. However, a statement disclaiming liability for any action taken in reliance on the content of a message could give effective legal protection.

BUSINESS CORRESPONDENCE REGULATIONS

E-mail should be treated in the same way as other forms of business correspondence.

SECURITY OF INFORMATION

Although most of the recommendations would apply particularly to organisations larger than a Golf Club, nevertheless the principles are the same. Decisions on what to include in a policy document depends on the level of development and access to technology in the individual club.

The British Standard Guidelines for IT security cover the following ten points:

1. Clear allocation of responsibility
2. Adequate training of users
3. Consistent reporting of security incidents
4. Policy for virus checking
5. Existence of business continuity plan
6. Consideration of copyright issues
7. Protection of important organisational records
8. Compliance with data protection legislation
9. Regular security reviews
10. IT codes of practice for employees.

Best Practice includes:

- Access rights: Employees need to be aware of areas of permitted access.
- Protection of passwords: Users need to be reminded that leaving their password by their monitor/keyboard makes the security system redundant.
- Switching off terminals: this cuts down unauthorised access.
- Virus checking: Obviously the deliberate importation of a virus must be made a disciplinary offence but employees should also be warned against importing non-text files or unknown messages without first having scanned them for viruses.
- Home Working: With the increasing amount of home working it is important to have an agreement that IT materials and systems are returned on termination of employment.

DEVELOPING AN E-MAIL POLICY

The policy should:

- Prohibit the sending of personal e-mails
- Prohibit the sending of offensive messages or downloading offensive material
- Advise that sending highly confidential or sensitive information by the normal e-mail system should be avoided
- Advise the use of a relevant disclaimer

- Inform staff that imported software and files must be scanned for viruses before being opened
- Advise that e-mail messages may have to be disclosed in court
- Advise staff should not discuss any dispute or associated issues especially by e-mail
- Confirm that an employee's use of the e-mail system is not private and could be subject to scrutiny.
- Advise staff that breaches of the policy may lead to disciplinary proceedings or even dismissal in extreme cases.

E-MAIL POLICY AND DISCIPLINARY PROCEDURES

If an e-mail policy is abused this may result in disciplinary proceedings against the offender. Therefore any policy must include clear warnings to that effect. To protect the employer from claims of unlawful dismissal, the policy should spell out what offences will be regarded as justifying dismissal.

Email Policy of [the Golf Club]

The following policy will cover the use of all Email communication. It is vital that every employee understands all parts of it as Email is so fundamental to office routines and service to our members. Any breach in security may compromise the confidentiality on which much of our work is based. This is in addition to loss of work time and inconvenience caused.

Introduction

All staff have a responsibility to ensure that Email services are used in a sensible and appropriate way.

Computers and Email accounts are the property of the employer and are designed to assist in the performance of your work. You should therefore have no expectation of privacy in any Email sent or received, whether it is of a business or personal nature. Your manager may be given authority to examine Emails at any time.

Any document sent or received or any decision involving Email must be regarded as, and dealt with as though it was, a permanent written record. Where in similar circumstances a paper copy of correspondence would be retained, a copy of the electronic communication must be retained. In law, a message sent via Email is identical to a memo or letter.

Your employer has an Equal Opportunities Policy. Email must not be used for harassing, bullying, threatening, gossip or personal jokes. Staff abuses of the Email system will be taken seriously and may lead to disciplinary procedures.

Code of Practice

For full-time staff the general expectation is that Email is checked at least twice a day. If practicable, when absent from the office, arrangements should be made for a colleague to deal with your mail.

Confidential information should not be sent by Email. Regard Email as a postcard, open to view.

The priority of an Email will be no greater than an item of paper-based mail or other communication. If earlier response is required, this should be indicated.

Where a message is particularly important ensure confirmation of receipt is obtained.

The following standard disclaimer message is the minimum recommended for external Emails:

> 'The information contained in the Email, including any attachments, is confidential and may be legally privileged. It is intended for the addressee only and other access to it is unauthorised. If you have received this Email in error, we apologise, and ask you to notify the sender immediately. Please also destroy any copies and delete the message from your computer systems. Thank you.

When sending or receiving Email please consider:

- People are not necessarily who they say they are
- They can read what you send and change it
- The information you receive is not necessarily genuine
- Viruses can easily be obtained inadvertently via Email
- Data Protection legislation

When communicating by Email, remember to:

- Phrase text according to your audience, and use the spell check facility
- Use appropriate language, avoiding profanities
- Direct requests to an individual, as requests to a distribution list rarely result in a response
- Send Email 'high priority' if it is urgent. If it is very urgent use the phone! Overuse of 'high priority' means none of your messages will be seen as urgent
- Keep text brief. But not so short as to be abrupt which could be interpreted as rudeness
- Avoid CAPITALISING as this reads like shouting. Consider italics for emphasis instead
- Recognise Email ping-pong; pick up the phone instead
- Include distribution lists in the Bcc: line rather than the To: or Cc: lines
- Avoid sending large documents to distribution lists as this clogs up the system

You must not:

- Load or transmit programs (.exe files) received or sent as Email attachments
- Disclose personal data which may be incompatible with the Data Protection Act
- Send or obtain mail which is
  a) Illegal or fraudulent
  b) Obscene, sexually explicit, offensive or harassing
  c) Embarrassing to your employer or to individuals
  d) Defamatory, abusive, intimidating or discriminatory
  e) Known to be infected with a virus
- Use Email for
  a) Personal business interests
  b) Taking part in chain Email
  c) Distributing copyright material without the owner's approval
  d) Conducting trivial debates
  e) Private broadcasts or mail shots

Legislation which may be breached by inappropriate use of Email includes:

- Copyright Law – do not automatically store or reproduce copyright material. You must comply with conditions imposed by the copyright owner

- Data Protection Act 1998 – [the Golf Club] is registered under this act. Do not store personal information relating to identifiable individuals
- Computer Misuse Act 1990 – related to tampering with data owned by others
- Civil Law – including libel laws

The Regulation of Investigatory Powers Act (the RIP Act 2000) means your employer can monitor Emails for certain legitimate purposes.

Please Note:
This is a sample Email Policy document. The suggestion is that you make choices from the text, and make appropriate amendments, including changing all occurrences of [the Golf Club]. Sometimes more detail will be required on particular points.

Staff induction and training should include this policy, and a signature with date obtained from the employee to show their agreement.