

Beacon's Acceptable use of IT policy is designed to promote safe and appropriate practices and uses of IT through establishing clear and robust acceptable use guidelines for Beacon staff and contractors.

Beacon's Acceptable use of IT Policy covers the use of email, mobile phones, Beacon databases and the internet while under the employment of Beacon or while conducting business on behalf of Beacon as a contractor or employee.

## **Email**

Use of email by employees of Beacon is permitted and encouraged where such use supports the goals and objectives of the business.

However, Beacon has a policy for the use of email whereby the employee, contractor or user must ensure that they:

- comply with current legislation
- use email in an acceptable way
- do not create unnecessary business risk to the company by their misuse of the internet

## **Unacceptable behaviour**

- forwarding of company confidential messages to external locations
- distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal
- distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment
- accessing copyrighted information in a way that violates the copyright
- breaking into the company's or another organisation's system or unauthorised use of a password/mailbox
- broadcasting unsolicited personal views on social, political, religious or other non-business related matters
- transmitting unsolicited commercial or advertising material
- undertaking deliberate activities that waste staff effort or networked resources
- introducing any form of computer virus or malware into the corporate network

## **Monitoring**

Beacon accepts that the use of email is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business.

In addition, all of the company's email resources are provided for business purposes. Therefore, the company maintains the right to examine any systems and inspect any data recorded in those systems.

In order to ensure compliance with this policy, the company also reserves the right to use monitoring software in order to check upon the use and content of emails. Such monitoring is for legitimate purposes only and will be undertaken in accordance with a procedure agreed with employees, contractors and users.

## **Sanctions**

Where it is believed that an employee, contractor or user has failed to comply with this policy, they will face the company's disciplinary procedure. If the employee, contractor or user is found to have breached the policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal. The actual penalty applied will depend on factors such as the seriousness of the breach and the employee's, contractors or users disciplinary record.

## **Accessing the Internet and Beacon's Intranet**

Beacon employees and contractors are expected to use the Internet responsibly and productively.

Internet access provided by Beacon is limited to job-related activities only and personal use is not permitted. Any internet access undertaken during working times or while undertaking work on behalf of Beacon should also be limited to job-related activities only.

All Internet data that is composed, transmitted and/or received by Beacon's computer systems is considered to belong to Beacon and is recognised as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties. The equipment, services and technology used to access the Internet are the property of Beacon and Beacon thus reserves the right to monitor Internet traffic and monitor and access data that is composed, sent or received through its online connections or equipment.

All sites and downloads may be monitored and/or blocked by Beacon if they are deemed to be harmful and/or not productive to business.

The installation of software such as instant messaging technology is strictly prohibited.

## **Unacceptable use of the internet**

Unacceptable use of the internet by employees and contractors includes, but is not limited to:

- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via Beacon's email service or from a Beacon computer.
- Using computers to perpetrate any form of fraud, and/or software, film or music piracy.
- Stealing, using, or disclosing someone else's password without authorization.
- Downloading, copying or pirating software and electronic files that are copyrighted or without authorization.
- Sharing confidential material, trade secrets, or proprietary information outside of the company.
- Hacking into unauthorized websites.
- Sending or posting information that is defamatory to the company, its products/services, colleagues and/or customers.
- Introducing malicious software onto the company network and/or jeopardizing the security of Beacon's electronic communications systems
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.
- Passing off personal views as representing those of Beacon's.

If an employee or contractor is unsure about what constituted acceptable Internet usage, then he/she should ask one of the Directors of Beacon for further guidance and clarification.

All terms and conditions as stated in this document are applicable to all users of Beacon's network and Internet connection. All terms and conditions as stated in this document reflect an agreement of all parties and should be governed and interpreted in accordance with the policies and procedures

mentioned above. Any user violating these policies is subject to disciplinary actions deemed appropriate by Beacon.

### **Mobile Use**

It is recognised that mobile phones can cause an unnecessary distraction during the working day and can be intrusive when used in the company of others.

Beacon employees are permitted to have their personal mobile phones about their person; however there is a clear expectation that all personal use is limited to allocated lunch and/or tea breaks.

Other than in agreed exceptional circumstances, phones must be switched off and personal calls and texts must not be taken or made during work time.

### **Agreement**

All company employees, contractors or temporary staff who have been issued Beacon Acceptable of IT policy and then begin to use Beacon's email services, internet access or intranet confirm their understanding and acceptance of this policy.