OPTIMUM
RECRUITMENT

CANDIDATE ACCEPTABLE USAGE POLICY

EMAIL, WEB BROWSING AND THE INTERNET

Please sign form upon reading Candidate Acceptable Usage Policy

Signed: _____

Date: _____

Name (print): _____

The terms and conditions of acceptable usage for email, web browsing and internet whilst on a client's premises are outlined below.

These systems are owned and maintained by the client for the exclusive purpose of conducting the Client's business and must not be used in any manner that could reasonably lead to damage to either the client or its reputation.

The client retains the right to monitor any and all stored messages, transmissions, searches and routine backup copies of its internet access systems to ensure proper usage. Consequently, employees should assume that these communications are non-confidential and that that the client will monitor traffic to ensure usage conforms with this policy. In addition, employees are reminded that email communications sent from the client travel on the client's electronic stationery and should be treated in the same manner as if they were sent on client letterhead. The same level of professionalism that is applied to written communications is to be applied to email.

The following provisions set out the policy with regard to acceptable usage of the internet access system and to ensure good citizenship.

i. Each employee using the internet must comply with this policy

ii. Software, Internet sourced or otherwise, is not to be installed on client computers without the prior approval of the client. Software will only be installed on client computers in strict accordance with copyright and property ownership laws. You should inform yourself of the terms of particular software licenses and the general provisions of copyright laws before using client software.

iii. You must at all times act to protect information that could reasonably be construed as being confidential to the client. This means that confidential information is not to be transmitted to recipients who should not be in possession of the information and do not have a right to it. Transmission or copying of records from the client's system is specifically prohibited.

iv. You must not offend, harass or threaten any other person, nor store or transmit material designed or likely to do so. This provision specifically applies to racist, discriminatory, pornographic and similar material, and includes abusive and derogatory email messages. Think carefully about creating emails "in anger" as email provides a fantastic audit trail that the recipient can later use against you.

v. Client management retains the right to determine what is, and is not, acceptable use of the internet within their areas of responsibility. This right to curtail non- business uses will include restrictions on personal 'chat' sessions, personal email and other non-productive activities such as on-line shopping, facebook; and share trading. Employees who repeatedly infringe this aspect of the policy will become subject to disciplinary procedures, but it is hoped that staff members will recognise that time-wasting activities adversely affect the achievement of our goals.

vi. Employees bear the responsibility for backing up personal data. The client accepts no responsibility for loss or damage or consequential loss arising from use of the internet access system or the loss of data. The client will normally make provision for employees to regularly backup data to the server but data retained on local hard drives (including those in portable notebook computers) is the responsibility of the individual. The individual should clearly understand where their data is physically stored and the possible consequences of incorrect storage practices.

vii. Employees have a duty to ensure that important client data is correctly managed and preserved. This means that messages and documents that you receive from or send to external parties must be filed in appropriate folders on the server and not stored in local personal folders. You must ensure that you are aware of internal standards and policies for data storage and that you abide by them.

viii. Personal email and other data is not to be stored on client servers. Personal information may be stored on local disk drives in personal folders, but this is done at the entire risk of the individual. The client will not carry out data backup procedures for personal data, and this data should be periodically removed by the individual to ensure that storage requirements remain insignificant. Employees should also remove personal data prior to leaving the client.

ix. You must not use the email system to transfer very large files, as these files may be blocked by the Internet Service Provider which places size limits on intermediate mail-boxes within their post offices (keep items below 2 Mb). It is better to place the file in a folder in a shared location where other users can retrieve it – when and if they need it.

x. You must keep message and item stores such as folders under control. Failure to do so will mean that your PC will become sluggish and unresponsive. If the data store becomes corrupt you will lose even more data, and/or you will eventually not be able to send new mail. And after that, you won't be able to receive mail either, so it's in your own interest to maintain your data.