Focus Consultants: ICT Policy

The firm's ICT investment is considerable, and our dependency on computer technology in the delivery of our services is a fundamental part of our operation. All Focus offices operate via virtual private networks (VPN) to allow access to the server and email. Access is only available at Partner and Senior level and to other staff under exceptional circumstances and must first be approved by a Partner.

The purpose of the ICT Policy is to ensure the effective protection and proper usage of our computer systems. The ICT Policy will assist in maintaining systems at operational level. Contraventions of the ICT Policy could seriously disrupt the organisation's operation and any breaches will be treated seriously. The Partners are responsible for ensuring adherence to the ICT Policy within their Departments.

Responsibilities of Focus

1. The Partners are responsible for ensuring compliance with Data Protection legislation regarding data processed within their Departments.
2. The safe use of computer equipment and individual workstations is included within Focus Health and Safety policies and procedures and is a part of our monitoring procedures.
3. The Partners are responsible for ensuring Health and Safety legislation and procedures in relation to computer equipment are implemented within their Departments.
4. The organisation is responsible for providing all employees with hardware and software sufficient to enable them to carry out their responsibilities in an efficient manner.

Responsibilities of Employees

Hardware and software utilised by Focus Staff is the property of Focus Consultants. As such, all Employees are expected to comply with Focus policies and procedures in all respects as follows:

1. Software must not be installed without prior permission. Installation of unlicensed software is regarded as a serious breach of ICT Policy.
2. Regular virus/ spyware scans must be run on all computer workstations in accordance with Focus Policies and Procedures.
3. Passwording is part of the organisation's security strategy. Users are responsible for the security of their password which they should not divulge. Staff must not change their password without informing the ICT Co-ordinator.
4. Focus Consultants e-mail system is a core business application and should not be used for political, business or commercial purposes not related to Focus Consultants or its operation.
5. Focus Consultants e-mail system must not be used to distribute illegal, junk mail or inappropriate material which is viewed as a disciplinary offence. Staff should not make inappropriate use of their access to the Internet. Abuse of Internet access will be dealt with severely relative to its seriousness.
6. Staff should be aware of their responsibilities under the Data Protection Act, Computer Misuse Act[1] and the Copyright Design and Patents Act. Contravention of the Focus Consultants ICT Policy or any act of deliberate sabotage to Focus Consultants' computer systems may be considered a disciplinary offence.

[1] Computer Users shall not, by any wilful or deliberate act, jeopardize the integrity of the computing equipment, its systems programs or any other stored information to which they have access. Under the Terms of the Computer Misuse Act (1990), unauthorised access to a computer (sometimes called "hacking") or other unauthorised modification to the contents of a computer (such as the deliberate introduction of viruses) are criminal offences punishable by unlimited fines and up to 5 years imprisonment