UK Intranet

AUDIT • TAX • ADVISORY

[redacted]

21 August 2008

KPMG's IT policy; sent to me by KPMG in Aug 08

MyLife Home
MyLife index

Policies and processes
IT Security

[redacted]

[redacted]

Policies and tools

Background: my 03.04.08 Employment Tribunal Claim against KPMG and its undated PACK OF LIES Defence... ...that was preceded by its 22.05.08 dismissal of my 17.01.08 Grievance. Events discussed on the KPMG page

IT Security Policy and Guidelines

- IT Security policy
  - Conducting personal business
  - Passwords
  - Connecting to Client IT Networks
  - Use of email
    - Request to forward emails
    - Policy of the UK Firm - Leavers' emails
  - Use of the Internet and website browsing
  - [redacted]
- IT Security guidelines

This link details further need to know IT Security information.

Both the security policy and the guidelines are mandatory for all KPMG partners and staff.

IT Security policy

Version Number 23 - Dated 29 August 2007

The following rules are contractual obligations, mandatory for all staff, when using KPMG's IT equipment.

Any breach of the restrictions contained in this policy may result in the application of KPMG's Disciplinary Procedure, up to and including summary dismissal, and could give rise to criminal and/or civil liability.

Staff have a general responsibility when using computers, computer software and information/data held on computer systems only to act in a way which is legal. In particular:

- staff must not access a computer system or computer held

information and data without proper authority

- staff must not make unauthorised modifications to the contents of any computer system, including deleting or changing data
- staff must not make or use, nor permit others to make or use, unauthorised copies of computer software, including associated documentation and back-up copies: and
- "data storage" on "removable media" should be kept to a minimum.
- staff must ensure that any information under their control that is confidential, critical, commercially sensitive, or may have contractual or other legal implications for KPMG remains secure.

Offensive and inappropriate material must not be stored on any of KPMG's IT equipment, including servers and PCs.

TOP

Conducting personal business

Staff should be aware that no computer network can be guaranteed as being absolutely secure. Whilst KPMG has a number of processes and controls in place which have been designed to help ensure the security of its network (details of which can be found in the IT Services Security Guidelines), staff using the KPMG network for personal business (such as conducting online banking or shopping) do so at their own risk. If you have any concerns, about the security of KPMG's network, you should use alternative means or systems for conducting your personal business.

TOP

Passwords

[redacted]

TOP

Software Down-loading

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

TOP

[redacted]

TOP

Use of email

When using KPMG's email system internally or externally, staff may not send any email, attachment which:

- Makes representations or express opinions purporting to be those of KPMG.
- May damage KPMG's reputation or its relationships with its clients, or which may embarrass clients of KPMG.
- Is illegal, defamatory, obscene, pornographic, offensive, or damaging, or which may be considered by others to cause distress, sexual, racial or other harassment or discrimination.
- May infringe copyright.
- May introduce a virus or other malicious software to any KPMG or client network.
- Constitutes 'junk' email (usually non-business messages posted to multiple addresses) or is posted to multiple news groups.
- Is for private commercial purposes unrelated to KPMG.

In addition, even where none of the above categories of email traffic are involved, where an individual has excessive amounts of personal email traffic on their system (defined as levels of personal email activity sufficient to cut into their working time or to interfere with the performance of their duties), this may also be treated as a disciplinary offence.

KPMG reserves the right to monitor and read the content of all traffic

passing through the KPMG email system both internal and external (any system external to KPMG including but not limited to the Internet), for the purpose of ensuring that these rules are adhered to.

TOP

Email Archiving

[redacted]

TOP

[redacted]

TOP

[redacted]

[redacted]

TOP

Use of the Internet and website browsing

The KPMG Internet gateway is the only means by which Internet services are to be accessed within KPMG. Staff may not access personal Internet accounts from within KPMG premises, home or any other remote sites using KPMG equipment.

- Staff accessing any system external to KPMG (including but not limited to the Internet) using KPMG's equipment may not, under any circumstances, access websites which are, or may be: illegal, defamatory, obscene, pornographic, offensive;
- considered by others to cause distress or to constitute sexual, racial or other harassment or discrimination;
- otherwise inappropriate in the workplace;

- [redacted]
- [redacted]

In order to ensure that staff do not access any of the above sites (either deliberately or inadvertently), KPMG employs firewall blocking software. Staff who attempt to access any blocked sites will receive a warning from the system. Staff who repeatedly attempt to access these sites may be subject to disciplinary action, up to and including dismissal. If, through a failure of the firewall blocking software, or for other reasons, you inadvertently reach a website which falls into the categories above, you should not explore further, but report the incident to the IT call centre, giving the address of the website (the address can be copied and pasted from the address box near the top of the Windows Explorer page).
KPMG reserves the right to monitor websites being accessed by staff, for the purpose of ensuring that these rules are adhered to.

TOP

Data Protection Act

- The Data Protection Act 1998 defines personal data as any 'data which relate to (an identifiable) living individual'. It places obligations on all staff with regard to processing personal information, and its security, regardless of any judgement which we may make about its sensitivity.

Staff may not disclose or use computerised personal data relating to individuals for any purpose other than those purposes for which the information was originally collected, and for which KPMG is registered with the Data Protection Registrar. All staff who have the responsibility for managing personal data must be aware of their responsibilities under this act. The following rules apply:

- personal information held must be accurate, relevant and not in excess to KPMG's needs
- personal information when no longer required by KPMG must be deleted and removed from the system
- information stored must be kept confidential, secure and not disclosed to unauthorised enquirers
- personal information must only be stored and used for the purposes for which it was originally collected, unless the express permission of the data subject is obtained for its extended or additional use
- individuals to whom the personal data relates are entitled to have access to the data, under the terms of 'subject access' within the