5.10.1 Example IT policy document for a company

1. Why do we need a policy?

As our dependence on technology increases, so do the risks and opportunities for misuse. We are increasingly vulnerable to threats from outside and inside the organization, both due to carelessness and malice.

From our clients' viewpoint: we need to be perceived as competent and professional in our ability to conduct our business electronically.

From our company's perspective: we need to maximize the benefits and reduce the risks of using information technology and protect company assets (including reputation).

From your viewpoint: we need to protect your interests as an individual in a community, and reduce the risk of your liability for legal damages.

These policy guidelines must be adhered to at all times to ensure that all users behave in a professional, legal and ethical manner. Failure to
do so may result in disciplinary action, including dismissal and legal action.

2. The network For the purpose of this policy, we define 'the network' to mean the company
computer and telephone network, including all of its hardware and software.

The use of the network is not private. The company retains the right to monitor the use of the network by any user, within the boundaries of national law. All users are obliged to use company resources in a professional, ethical and lawful manner.

Material that is fraudulent, harassing or offensive, profane, obscene, intimidating, defamatory, misleading or otherwise unlawful or inappropriate may not be displayed, stored or transmitted using the network, by any means, or in any form (including SMS).

3. Security Any hardware or software that is deemed a security risk may be disconnected
or de-installed at any time, by the system administrator.

User accounts are set up, managed and maintained by the system administrators.

Users accessing the network must have authorization by access-rights, pass- word or by permission of the owner of the information.

Users must take reasonable precautions to prevent unauthorized access to the network. This includes leaving equipment unattended for extended periods while logged on.

Users must not attempt to gain unauthorized access to restricted information.

Passwords are provided to help prevent unauthorized access to restricted areas of the network. Users must not log on to any system using another user's password or account without their express permission.

Under no circumstances should any user reveal his/her password to anyone else, even by consent.

Users have a responsibility to safeguard passwords. They must not be written down on paper, stored unprotected online, or be located in readable form anywhere near a network terminal.

4. Copyright

Copyright is a statutory property right which protects an author's interest in his or her work. The right exists as soon as the work is created and continues to exist for the lifetime of the author and beyond, during which time the owner of the copyright may bring actions for infringement.

International copyright law protects a copyright owner's interest by preventing others from unlawfully exploiting the work that is protected. There are no registration requirements for the legal existence of copyright. Copyright subsists in most materials that are found on the Internet, including imagery and databases.

Copyright is infringed when a copyright work is copied without the consent of the copyright owner. Downloading information from any source constitutes copying. Unauthorized copy-cut-pasting from any text, graphical or media source may be in breach of copyright, as may copying, distributing or even installing software.

Many information sites express legal terms by which materials may be used. Users should refer to those terms and conditions before downloading any materials.

5. Data protection (e.g. UK)

Any person using a computer may be a data processor. Every individual is responsible for maintaining confidentiality of data by preventing unauthorized disclosure.

Personal data are legally defined as data that relate to a living individual who can be identified from those data, or from those and other data in possession of the data user. The use of personal data is governed by law (e.g. the UK Data Protection Act 1998).

The act lays out the following principles of data protection:

• Personal data shall be processed fairly and lawfully and such processing must comply with at least one of a set of specified conditions.

• Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be processed in any manner incompatible with that purpose or those purposes.

• Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

• Personal data shall be accurate and, where necessary, up to date. • Personal data processed for any purpose

or purposes shall not be kept
for longer than is necessary for that purpose or those purposes.
• Personal data shall be processed in accordance with the rights of data subjects under the Act.
• Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
• Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
The rules concerning the processing of personal data are complex. If in any doubt as to their interpretation, users should consult legal advice.

6. E-mail and SMS

All electronic messages created and stored on the network are the property of the company and are not private. The company retains the right to access any user's E-mail if it has reasonable grounds to do so.
The company E-mail system may be used for reasonable personal use, provided it does not interfere with normal business activities or work, and does not breach any company policy.
Users should be aware that:
• E-mail is a popular and successful vehicle for the distribution of computer viruses.
• Normal E-mail carries the same level of privacy as a postcard.
• E-mail is legally recognized as publishing and is easily recirculated.
• Users should take care to ensure that they are not breaching any copyright or compromising confidentiality of either the company or its clients or suppliers by sending, forwarding or copying an E-mail or attachment.
• Nothing libelous, harassing, discriminatory or unlawful should be writ- ten as part of any message.
E-mail is often written informally. Users should apply the same care and attention as in writing a conventional business correspondence, including ensuring accurate addressing.
Users must not participate in chain or junk E-mail activities (spam); mass E-mailing should be avoided whenever possible.
E-mail attachments provide a useful means of delivering files to other users. However, careful consideration should be paid to ensure that the recipient can read and make use of the data.
• Not all file types are readable by all computers.
• Many sites have a maximum acceptable file size for E-mail.
• The recipient must have suitable software installed in order to display a file.
In order to prevent the spread of viruses, users should not attempt to open any attachment from an unknown or unexpected source. Certain file types may be blocked by mail-filtering software.
Users must not disguise themselves or falsify their identity in any message.
Where provided, users must ensure that company disclaimers are included when sending E-mail.

7. The World Wide Web

Access to the World Wide Web is provided for business purposes. The World Wide Web may be accessed for limited personal use provided that such use does not interfere with normal business practice or work, and that personal use complies with all aspects of this policy.
The company may monitor individual use, including visits to specific web sites.
Access may only be sought using an approved browser, which is installed on the user's computer by the system administrator.
The World Wide Web is uncontrolled and unregulated. Users should therefore be aware that there is no guarantee that any information found there is accurate, legal or factual.
Software may only be downloaded by an authorized system administrator.

8. Transactions Any commercial transaction made electronically must adhere to standard ordering policy.

The company will not accept liability for any commercial transaction which has not been subject to the appropriate approval.
The company will not accept liability for any personal transaction.

9. Hardware and software

The company provides computer, telecommunications equipment and soft- ware for business purposes. It is the responsibility of the system administrator to select, provide and maintain computer equipment in accordance with the work required.
Users must not connect unauthorized equipment to the network, use software that has not been provided or installed by the company, or attempt to alter the settings of any software that compromise security or reliability. No attempt should be made to alter the software or hardware, copy or distribute software, or download software, including screen-savers.
Installations and upgrades may only be performed by an authorized system administrator.

10. Surveillance

Digital cameras or audio input devices must not be connected to any computer that is not specifically authorized to have one. Users must not bring any possible surveillance device into an area where the company's private assets, intellectual or otherwise, are developed or stored. Employees must not disclose

any such information to persons or transmit it to any machine or information storage device not authorized to receive it.
11. Usage The company reserves the right to view any data stored on the network.
Users may not store personal files on the network. Any personal files can be deleted at any time.
The network is provided to enable
• Authorized users to store and retrieve work • Authorized users to share/exchange assets • Backup and recovery • Security and confidentiality of work.
All users must store files in the appropriate areas of the network. Users who create files on mobile devices should transfer their data to the appropriate area on the network as soon as possible.
12. Management Managers must ensure that they are fully aware of any potential risks when assessing requests by users for permission to: • Download files from the Internet
• Access additional areas of the network. Managers may not request any action by any system administrator which could result in a breach of any of the company policies.

5.10.2 Example IT procedure following a breach of policy

IT policy ought to contain instructions as to how users will be dealt with when they breach policy. There are many ways of dealing with users, with varying degrees of tolerance: reprimand, dismissal, loss of privilege etc. Clear guidelines are important for professional conduct, so that all users are treated either equally, or at least predictably.

5.10.3 When an employee leaves the company

A fixed policy for dismissing a member of staff can be useful when the employee was harmful to the organization. An organization can avoid harmful lawsuits by users who feel that they have been treated unfairly, by asking them to sign an acceptance of the procedure. The issue of dismissal was discussed in ref. [254].
Users typically have to be granted access to disparate systems with their own authentication mechanisms, e.g. Windows, Unix, key-cards, routers, modems, database passwords. These must all be removed to prevent a user from being able to change data after their dismissal.
A clear procedure is important for both parties:
• To protect an organization from a disgruntled employee's actions.
• To protect the former employee from accusations about what he or she did after their dismissal that they might not be responsible for.
It is therefore important to have a clear checklist for the sake of security.
• Change combination locks.
• Change door keys.
• Surrender laptops and mobile devices.
• Remove all authentication privileges.
• Remove all pending jobs in `at` or `cron` that could be logic bombs.

Principle 26 (Predictable failure of humans). All systems fail eventually, but they should fail predictably. Where humans are involved, we must have checklists and guidelines that protect the remainder of the system from the failure.

Human failures can be mitigated by adherence to quality assurance schemes, such as ISO 9000