I.T. Security Policy
User Responsibilities

These guidelines are intended to help you make the best use of the computer resources at your disposal. You should understand the following.

1. You are individually responsible for protecting the data and information in your hands. *Security is everyone's responsibility.*

2. Recognise which data is sensitive. If you do not know or are not sure, ask.

3. Even though you cannot touch it, information is an asset, sometimes a priceless asset.

4. Use the resources at your disposal only for the benefit of the Organisation.

5. Understand that *you* are accountable for what *you* do on the system.

6. If you observe anything unusual, *tell your supervisor*.

When using the Organisation's computer systems you should comply with the following guidelines.

DO

7. Do choose a password that would be hard to guess.

8. Do log off or lock your PC before you leave your workstation. This is important if you are working on sensitive information or leaving your workstation for any length of time.

9. Do ask people their business in your area, if they look as though they do not belong there.

10. Do protect equipment from theft and keep it away from food and drinks.

11. Do ensure that all important data is backed up regularly. Liase with the I.T. Department if you require assistance.

12. Do make sure that on every occasion floppy disks, CD's, DVD's and USB sticks are brought in to the Organisation that they are checked for viruses before use.

13. Do inform the I.T. Department immediately if you think that your workstation may have a virus.

DO NOT

14. Do not write down your password.

15. Do not share or disclose your password.

16. Do not give others the opportunity to look over your shoulder if you are working on something sensitive.

17. Do not use shareware (software downloaded from the Internet or on PC magazine covers).

18. Do not duplicate or copy software.

19. Do not install any software on your machine or alter its configuration, this work may only be undertaken by the I.T. Department.

Please note the following

Your PC will be audited periodically.
Logins to, and use of the Organisation's network are monitored and audited.

Failure to comply with the organisation's security policy may lead to disciplinary action.

Copyright © Ruskwig – Ruskwig provides you with the right to copy and amend this document for your own use – You may not resell, ask for donations for, or otherwise transfer for value the document.