|  |  |
| --- | --- |
| **Policies and Procedures** |  |

**Digital Security**

**Network Use**

All users have an individual logon username that is password protected. The individual username provides rights and privileges such as Internet, personal mail and work folders, access to the company’s business folders, common areas such as document templates, printing and digital communications.

Activities are always monitored through the logon of usernames. This monitoring consists of:

* Formal monitoring: By user logon details including proxy logs, printing records, workstation records, etc.
* Informal monitoring: Access to folders, application of filters and regular searching to remove harmful data.

**User logon integrity**

Each employee must keep their passwords secret. No user may share their password or give others access to their account even by logging into the computer for another person.

No user must attempt to gain access to another user’s account.

Users are responsible for selecting a password that complies with our company’s minimum standards for password complexity as set by the network administrator or when informed during a password reset.

**Network security**

No employee or guest on our network may create, access, store, transfer, download, digitally communicate or use files that are illegal, offensive, dangerous or harmful in any way.

Employees must always ensure files, however transferred, are used for the purposes of this business and are scanned for viruses prior to use.

Employees are to immediately inform the Office Manager of a suspected inappropriate activity.

**Computer workstations**

The settings of our workstations are not to be altered in any way.

**Saving of files**

Input devices such as thumb drives or other external memory devices should only be used if they come from a trustworthy source.

Before opening any external data storage device, ensure that a company anti-virus and malware scan is run on it.

Files that are to be modified should first be saved to the computer’s desktop and the thumb drive ejected before beginning work on the files.

All files should then be saved to the relevant network folder before work on the file commences and are not left on the desktop.

Back up of network data and the ‘My Documents’ of each staff member’s computer is performed at the end of every week. The data is automatically backed up to our server’s ancillary (duplicate) server located in the Network Server room.