The Clear Desk Policy applies to all The Write Time users to any of The Write Time information assets, systems or services that are managed. The Clear desk policy is also part of the individual user agreement.

The Clear Desk Policy is one of the primary methods to prevent data leakage or unauthorised disclosure of security assets. Secondary restrictions of data controls include restricting access to information, employees are only provided access to data and information on a "Business Need Principle" i.e., access to the minimum data required for individual roles.

The main reasons for the policy:

- It reduces the threat of a security breach and information theft as confidential information gets locked away
- It ensures compliance with data protection regulations - keeping personal data secure
- It reduces the chance of identity theft
- It demonstrates customer care, by showing customers that The Write Time is taking responsibility for the personal data in its care.

Clear desk policy

All employees are required to understand and implement actions which ensure that no protected, restricted or confidential information (in paper or removable storage media format) is left on desks, in unsecured drawers or trays. This also includes reproduction equipment (photocopiers, fax machines, scanners) all employees are to ensure that any security labelled materials which are printed are collected immediately from the device.

Screen savers and information reproduction

All employee desktops and Laptops are subject to use restrictions, for data security, employees are to ensure that no one can gain unauthorised access to a workstation when they are not in attendance. All desktops and Laptops are subject to an automatic password-protected screen save activated by the inactivity of 5 minutes. When leaving a workstation unattended PCs and laptops must be locked.

All employees are to terminate active computer sessions when work is finished, and it is required to log off (i.e., not simply turn off the computer screen). Whenever an employee leaves the office for a period of over an hour they must ensure that the workstation is protected by appropriate locks and security.

Employees accept that they may not be allowed to use/bring into the office personal storage media, MP3 players, digital cameras and mobile phones with photographic capability.

Employees accept that they may only use The Write Time's reproductive equipment (photocopiers, fax machines, scanners) for proper organisational purposes (subject to specific personal use requests) and that will ensure that they will use facilities that are appropriate for the classification level of any information with which they are dealing.

Software

All employees are forbidden to make attempts to disable or over-ride any of The Write Time's installed software, which has been put in place to assure data security, including automatic time outs, screen saver applications and automatic log out etc.

Secure Storage

If you are issued with a set of keys for a filing cabinet or a cupboard it is your responsibility to make sure that any files or documents are kept locked and secure. NEVER leave your keys in a filing cabinet or cupboard or give your keys to another person

Creation of data/materials

When an employee is in a role that requires the creation of documents/materials with security-labelled content, that employee becomes the document owner and as such is responsible for security labelling to be applied and suitable storage is organised. Note the same requirements for uncompleted materials apply to work in progress. Failure to abide by this policy will result in disciplinary action being taken.

Audit and Security Monitoring

On both a contact-based and center level, security auditing and center visits will be required. Individual workstations and desks will be searched, as well as checks for unsecured goods. If materials are found, disciplinary action will be taken.