



# Clear Desk & Desktop Policy

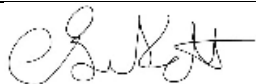
---

3.0

Author: David Office  
Date Published: 19/04/2019

## 1.0 Version Control

<b>Version:</b>	3.0	<b>(Author) Issued By:</b>	David Office
<b>Issued Date:</b>	19/04/2019	<b>Review Date:</b>	19/04/2020
<b>Document Owner:</b>	David Office	<b>Document Number</b>	ISMS006

<b>Approved By:</b>	Chris Birkett	<b>Position:</b>	Chief Operating Officer
<b>Signature:</b>		<b>Approved Date:</b>	19/04/2019

## 2.0 Document Revision History

Version Control Note: All documents in development are indicated by minor versions i.e. 0.1; 0.2 etc. The first version of a document to be approved for release is given major version 1.0. Upon review the first version of a revised document is given the designation 1.1, the second 1.2 etc. until the revised version is approved, whereupon it becomes version 2.0. The system continues in numerical order each time a document is reviewed and approved.

Version Number	Date	Author Title	Status	Comment/Reason for Issue
1.0	12/03/2018	David Office	Initial Draft	Legacy Policy
1.1	01/06/2018	David Office	Updated	ISGC Review and amendments
2.0	01/06/2018	David Office	Released	Policy Released
2.1	19/02/2019	David Office	Updated	ND Review and amendments
3.0	19/02/2019	David Office	Approved	Approved by C. Birkett
3.0	19/02/2019	David Office	Released	Policy Released
3.0	19/04/2019	David Office	Review	Policy Reviewed. No Changes
3.0	19/04/2019	David Office	Released	Policy Released

## 2.1 Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. **Any printed copies of this document are not controlled.**

As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

### 3.0 Table of Contents

1.0	Version Control .....	1
2.0	Document Revision History.....	1
2.1	Document Status.....	1
3.0	Table of Contents .....	2
4.0	Introduction .....	3
5.0	Objectives, Aim & Scope .....	3
5.1	Objectives.....	3
5.2	Aim .....	3
5.3	Scope.....	3
6.0	Clear Desk Policy .....	4
6.1	Requirements.....	4
6.2	Confidential Waste.....	4
6.3	Electronic Storage Devices & IT Hardware .....	5
6.4	Printers, Photocopiers and Fax Machines.....	5
6.5	Physical Measures.....	5
7.0	Clear Desktop Policy.....	6
8.0	Exemptions.....	6
8.1	Public Domain Items .....	6
8.2	Internal Items.....	6
8.3	Stationary.....	7
8.4	Personal Artefacts.....	7
8.5	Unlockable Drawers/Cabinets/Book Cases.....	7
8.6	External Clients and Visitors .....	7
11.0	Audit & Breach Reporting .....	8
7.0	Responsibilities .....	8
7.1	Information Security Officer .....	8
7.2	All Staff .....	8
8.0	References .....	9

## 4.0 Introduction

Winn Group is required at all times to comply with the GDPR and Data Protection Act (2018) to ensure all data and information it holds is protected.

In order to ensure the protection of data, all physical media, and media held on corporate IT systems accessed via desktop computers must be safeguarded against disclosure, theft, or damage. Risk mitigation controls include appropriate clear desk and clear desktop controls to protect all forms of media used, taking into account the information classification and legal/contractual requirements of Winn Group.

## 5.0 Objectives, Aim & Scope

### 5.1 Objectives

The objective of this policy is to ensure that all paper and electronic records containing person identifiable information, or any other confidential/sensitive information (including corporate or commercially sensitive information) is suitably secured when not in use and is not left visible to unintended parties.

This policy applies in particular to working areas, such as desks, tables, and exposed book cases, which should not have confidential, sensitive, commercially sensitive or person-identifiable information left on them whilst unattended for an extended period.

The objective of this policy is also to ensure that Winn Group adheres to the obligations placed upon it by the GDPR and Data Protection Act (2018), as well as its Clients, Suppliers and Stakeholders.

### 5.2 Aim

The aim of this policy is to:

- Reduce the risk of a security breach or information theft;
- Reduce the risk of confidential or sensitive information/documentation being stolen or accessed by unauthorised individuals which could damage the integrity of Winn Group;
- Help demonstrate compliance with the relevant Data Protection Legislation and ISO27001;
- Create a culture of staff responsibility in relation to the handling and care of personal data and other confidential information.

### 5.3 Scope

This policy applies to all employees of Winn Group and associated subsidiaries, contractors, volunteers, vendors and partners.

## 6.0 Clear Desk Policy

### 6.1 Requirements

Confidential or sensitive information, whether held electronically or on paper records and other valuable resources should be secured appropriately when staff are absent from their workplace and at the end of each working day.

The following criteria must be followed in order to meet the requirements for a clear desk when the desk is unattended, to keep information secure and not readily accessible to non-authorised staff:

- Desks must be cleared at the end of each working day of any confidential or personal identifiable information;
- Any paper record or other media containing confidential information must be locked securely in desks, filing cabinets or designated secure rooms at all times, other than when being used by staff;
- No notepads or notebooks with visible contents must be left on the desk;
- No notes or Post-It notes should be on the desk, attached to monitors, or attached to desk divider boards;
- Any information about any Winn Group-related contacts, should not be on display;
- Information relating to Winn Group processes or specifics of case management should not be left on display;
- Personal drawers (where possible) should be locked, with the key removed from the locking mechanism and stored in a secure place;
- Health & Safety – desks and other work spaces should be sufficiently tidy at the end of each working day to permit the cleaning staff to perform their duties;
- Personal items (i.e. keys, handbags, wallets etc.) should be locked away safely in the interests of security. It is the responsibility of the owner to ensure all security precautions are taken.

### 6.2 Confidential Waste

To reduce the risk of a breach of confidentiality and adherence to Data Protection Legislation, when disposing of person identifiable information, ensure that it is destroyed securely by placing in a secure waste bin.

Most desk areas throughout Winn Group have been provided with a small blue bin designated for the disposal of confidential waste:

- These should only be used during the day when the desk area is attended.
- At the end of the working day these small bins should be emptied in to the larger, locked blue bins within the work area.

This is the responsibility of the member of staff occupying the desk area and NOT any cleaner contracted by Winn Group as there is potential for a breach of information.

### 6.3 Electronic Storage Devices & IT Hardware

For the purposes of this policy electronic data and equipment will not be treated differently from manual records and equipment, if they contain the same type of confidential, sensitive and/or personal information. Computing and all other equipment containing data will therefore be treated with the same level of security as paper-based resources.

- To ensure the security of information held electronically, lock away portable computing devices such as Laptops or PDA devices when not in use and where appropriate;
- To ensure the security of information held on mass storage devices such as CDROM, DVDs or USB drives, lock these away in a secure drawer or cabinet at the end of the working day;
- USB drives and other such items must be locked away even if they are encrypted.

### 6.4 Printers, Photocopiers and Fax Machines

Where there is a shared printer or multi-functional device available, all printing should be locked by default, requiring the users to enter a 4-digit PIN to release their documents.

To avoid accidentally printing to an unintended network device, computer users should additionally check that their default printer is correct before printing any documents.

Where documents are scanned using photocopiers or multi-functional devices, ensure that scanned documents are correctly sent to the document owner, and then cleared from the device memory (where applicable).

Personal data must be cleared from printers, photocopiers and fax machines immediately on completion. If these documents are no longer required, the items must be securely disposed.

It is the responsibility of the person who sends information to be printed to ensure they collect their documents. If information is of a confidential/sensitive nature and it is misplaced or missing, this should be logged as an incident.


### 6.5 Physical Measures

Preventative measures must also be taken outside the working desk area, these include:

- All internal doors shall be closed when working areas are unattended and at the end of the working day;
- Office/work area windows shall be closed when working areas are unattended and at the end of the working day;
- All 'white boards' containing Personal Identifiable Information or an information combination that could identify someone should be wiped clean or redacted when working areas are unattended or at the end of the working day;
- All 'flip charts' containing Personal Identifiable Information or an information combination that could identify someone should be wiped clean or redacted when working areas are unattended or at the end of the working day.

## 7.0 Clear Desktop Policy

For all Winn Group IT systems, the following must be followed:

- Computers and laptops must not be left logged on when unattended. When staff have to leave their desks for **any** reason, they must lock the computer by using the 'Control+Alt+Del' keys simultaneously and selecting *Lock* or by pressing the  key and the letter 'L';
- When sensitive or confidential information is being worked on, computer screens should be angled away from the view of unauthorised persons. If this is not possible, screens must be cleared or locked when talking to unauthorised persons;
- If another person needs to see a user's screen or if the user has a visitor, the user should ensure that any confidential data that is not appropriate for the visitor to see is minimised or closed
- All computer terminals shall have the auto screen saver set to activate when there is no activity for 5 minutes;
- Users are required to re-authenticate by entering their password to unlock screens;
- Workstations must be shut down if the user will be knowingly absent for periods longer than 2 hours;
- Workstations must be shut down at the end of the working day.

## 8.0 Exemptions

There are several exceptions that are also applicable to the Clear Desk Policy as these items do not have a bearing on potential security breaches or are controlled by individual members of staff.

### 8.1 Public Domain Items

Items classified as "public domain" items are any items, information, or documentation that is freely available within the public domain (for general consumption, available on the internet, or is being broadcast without licence).

Any items that are deemed under this classification or are specifically classified as "Public" are allowed to remain within the area of an unattended desk. This can include telephone numbers which are publicised on websites (including the company website); however, staff should show discretion when displaying telephone numbers and should store these within their locked drawers where possible.

### 8.2 Internal Items

Items classified as "Internal" are specifically for the consumption of any members of staff within Winn Group premises. This may be extended to the visitors brought in to Winn Group and with the explicit permission given by the creator of the item(s).

Internal items can also be on display within Winn Group premises but should NOT be made available in the public domain. To ensure information of this nature does not get viewed by an unintended audience, items of this classification should always be filed away and NOT left on display on an unattended desk. In rare circumstances, and with direct permission given by a manager, this

information can be displayed in other agreed formats but strictly within Winn Group premises. Further information is available in the Winn Group Information Classification & Handling Policy

### **8.3 Stationary**

Stationary items are classified as “none” items by default. Company stationary is controlled by its own usage policies; however, the display and storage of such items on or within an unattended desk area will not impact on the Clear Desk Policy.

Further to the above, any notepads that are clear of notation will be classed as stationary and therefore a “none” item.

### **8.4 Personal Artefacts**

Personal artefacts are specifically controlled by the member of staff directly allowing them to determine whether or not they wish for their own personal information or identifiable artefacts to be on display. The following items are an example, but not an exhaustive list, of what is deemed to be a personal artefact:

- Photos or pictures not containing any work sensitive information;
- Photo-frames;
- Accessories, e.g. mouse mat and desk calendars;
- Cups, mugs, or beverage holders;
- Stationary holders.

Further to the above, items must not be of an offensive nature nor should they be in breach of any other policy the company may enforce.

### **8.5 Unlockable Drawers/Cabinets/Book Cases**

Staff are permitted to have unlockable drawers/cabinets/book cases (furniture), which can be used as a storage facility as part of this policy. However, every effort should be made in the first instance to use lockable furniture. Facilities Management should be notified when an item of furniture cannot be locked.

If the furniture is lockable, the following items must be adhered to:

- The second key for the furniture must be clearly marked and stored in the duplicate key secure facility;
- The drawers MUST be locked, and the key removed from the locking mechanism and stored securely when the desk is unattended.

### **8.6 External Clients and Visitors**

Any external clients or visitors are responsible for the disclosure of any items or information they bring with them on to Winn Group premises and are therefore not covered by this policy.

Any breaches or disclosure of information to unintended audiences caused by an external client or visitor will lie directly with that person and not with Winn Group.



## **9.0 Audit & Breach Reporting**

Any breaches in this policy must be reported by employees to the Data Protection Team.

All employees must be aware of the confidential nature of the information with which they will be working with when using physical media, and that all alleged security violations resulting in breach of this policy will be dealt with according to severity through the company's disciplinary procedure.

## **10.0 Responsibilities**

### **10.1 Information Security Officer**

Responsible for monitoring compliance and providing guidance to staff on the implementation of the policy.

### **10.2 All Staff**

All staff are responsible for the safe, secure handling of all electronic data, and therefore must understand and comply with this policy and associated guidance.

Additionally, all staff have a responsibility to report security incidents and breaches of this policy upon identification to the Data Protection Team.

## 11.0 References

The following documents will provide additional information:

Doc Reference Number	Title
ISMS007	Information Classification & Handling Policy
SM015	IT & Communications Policy
ISMS001	Information Security Policy
ISMS004	Access Control Policy

This document has been prepared using the following standards and their applicable controls as reference:

Standard	Control	Description