

INTERNAL

WINNgroup

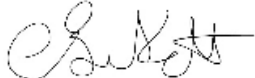
Acceptable Use Policy

1.0

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

1.0 Version Control

Version:	1.0	(Author) Issued By:	David Office
Issued Date:	19/04/2019	Review Date:	19/04/2020
Document Owner:	Colette Gardner	Document Number	ISMS003

Approved By:	Chris Birkett	Position:	Chief Operating Officer
Signature:		Approved Date:	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
0.1	01/10/2018	David Office	Initial Draft	New Policy
0.2	19/02/2019	David Office	Updated	ND Review amendments
1.0	19/02/2019	David Office	Approved	Approved by C. Birkett
1.0	19/02/2019	David Office	Released	Policy Released
1.0	19/04/2019	David Office	Review	Policy Reviewed. No Changes
1.0	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	Policy Statement	4
6.1	Acceptable Use Principles	4
6.2	User IDs and Passwords	4
6.3	Managing and Protecting Information	4
6.4	Personal Use of Winn Group IT.....	5
6.5	Email, Fax and Voice Communication	6
6.6	Websites and Social Media	6
6.7	Devices, Systems and Networks	6
6.8	Physical Security.....	7
8.0	Breaches of Policy	7
9.0	Responsibilities	8
9.1	Information Security Officer	8
9.2	Line Managers.....	8
9.3	All Users	8
10.0	References	9

4.0 Introduction

Information Technology resources, such as workstations, laptops and mobile devices offer enhanced ways of working and engaging with our colleagues and customers. However, we must also be aware that improper use of these resources can impact us, our colleagues, customers and Winn Group's reputation.

5.0 Objectives, Aim & Scope

5.1 Objectives

The objective of this policy is to ensure that users understand their responsibility for the appropriate use of Winn Group Information Technology resources. Understanding this will help users to protect themselves and Winn Group's equipment, information and reputation.

5.2 Aim

This Acceptable Use Policy aims to protect all users of Winn Group equipment and minimise risks by providing clarity on the behaviours expected and required by Winn Group staff and the consequences of breaching this policy. It sets a framework within which to conduct Winn Group's business and explains how we can achieve compliance and evaluation of new business and technology requirements.

5.3 Scope

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

In addition, the policy applies to all Winn Group equipment and information (all information systems, hardware, software and channels of communication, including voice/telephony, social media, video, email, instant messaging, internet and intranet).

User's personal information which is processed by Winn Group equipment is also subject to this policy.

6.0 Policy Statement

6.1 Acceptable Use Principles

Users will:

- Confirm prior to use of Winn Group equipment or information that they agree to this Acceptable Use Policy and understand that breaching this policy may result in disciplinary procedures;
- Be responsible for their own actions and act responsibly and professionally at all times;
- Use information, systems and equipment in line with Winn Group Information Security policies;
- Immediately report any breach of this Acceptable Use Policy to their line manager and to the Data Protection Team, and comply with procedures when a breach of the policy is suspected or reported;
- Never knowingly undertake illegal activity, or any activity that would be harmful to Winn Group's reputation or jeopardise staff and/or client data, on Winn Group technology;
- Understand that both business and personal use will be monitored as appropriate;
- Be aware that they can use whistleblowing and raising a concern if it is believed that someone is misusing Winn Group information or electronic equipment;
- Undertake education and awareness on security and using Winn Group information and technology, in order to be able to understand, recognise, and report threats, risks and incidents.

6.2 User IDs and Passwords

Users will:

- Protect user names, staff numbers, ID cards and passwords appropriately;
- Create secure passwords following best practice guidance, as prescribed in the Password Policy;
- Not logon to any Winn Group systems using another user's credentials;
- Lock the screen when temporarily leaving devices that are in use;
- Log out of all computer devices connected to Winn Group's internal network during non-working hours.

6.3 Managing and Protecting Information

Users will:

- Understand that they and Winn Group have a legal responsibility to protect personal and sensitive information;
- Ensure that all information is created, used, shared and disposed of in line with business need and in compliance with the Document and Records Management Policy;
- Not attempt to access personal data unless there is a valid business need that is appropriate to their job role;
- Not provide information in response to callers or e-mails whose identity they cannot verify;
- Be careful not to be overheard or overlooked in public areas when conducting Winn Group business;
- Apply the Information Classification & Handling Policy appropriately to document headers and email subject lines in relation to the Official-Sensitive handling caveat;

- Not attempt to access, amend, damage, delete or disseminate another person's files, emails, communications or data without the appropriate authority;
- Not attempt to compromise or gain unauthorised access to Winn Group IT, telephony or content, or prevent legitimate access to it;
- Comply with the Information Security, Data Protection and Confidentiality policies when managing Winn Group information.

6.4 Personal Use of Winn Group IT

Users will:

- Understand that they are personally accountable for what they do online whilst using Winn Group technology;
- Personal use of IT resources is permitted in an employee's own time, breaks taken in normal working hours do not count as the employee's own time for personal use of Winn Group equipment;
- Ensure that any personal information stored or accessed is appropriate i.e. legal, appropriate and compliant with this policy;
- Understand that the ability to store personal information on Winn Group owned devices and systems is a privilege and Winn Group has the right to require the data is removed where deemed appropriate;
- Ensure activities do not damage the reputation of Winn Group, its employees and clients, including accessing, storing, transmitting or distributing links to material that:
 - Could embarrass or compromise Winn Group in any way;
 - Is obtained in violation of copyright or used in breach of a licence agreement;
 - Can be reasonably considered as harassment of, or insulting to, others;
 - Is offensive, indecent or obscene, including abusive images and literature.
- Follow the Winn Group Policies & Procedures and must not:
 - Trade or canvass support for any organisation on official premises, whether it is for personal gain from any type of transaction or on behalf of external bodies;
 - Send messages or material that solicit or promote religious, political or other non-business-related causes, unless authorised by Winn Group;
 - Provide unauthorised views or commitments that could appear to be on behalf of Winn Group;
 - Undertake any form of gaming, lottery or betting (Gambling);
 - Use any type of application and/or device to circumvent management or security controls;
 - Download software onto Winn Group devices with the exception of Winn Group supplied tablet devices and smart phones where permitted from an official source and appropriately licensed. This software must not compromise the performance or security of the device or Winn Group Networks and Data;
 - Access personal webmail accounts on Winn Group equipment;
 - Download music, video or other media-related files for non-business purposes or store such files on network drives.

6.5 Email, Fax and Voice Communication

Users will:

- Comply with Winn Group's email and Telephony policies;
- Only use appropriate language in messages, emails, faxes and recordings. Threatening, derogatory, abusive, indecent, obscene, racist, sexist or otherwise offensive content will not be tolerated;
- Not engage in mass transmission of unsolicited emails (SPAM);
- Not alter the content of a third party's message when forwarding it unless authorised;
- Not try to assume the identity of another user or create or send material designed to mislead people about who originated or authorised it (e.g. through misuse of scanned signatures);
- Be vigilant to phishing emails and know how to spot and report suspicious emails;
- Only use your Winn Group email address for Winn Group business related activities and linked organisational activity. When logging onto external web sites for personal use (e.g. for retail or internet banking purposes), Winn Group staff must use their personal email address.

6.6 Websites and Social Media

Users will:

- Only access appropriate content using Winn Group technology and not intentionally visit sites or news groups that are obscene, indecent or advocate illegal activity, as defined in the blocked categories list, held in the Endpoint protection software;
- Report any access to a site that should be blocked by our web filters to their line manager and the IT Department;
- Contact the IT Department with requests to unblock a website (link is external) and do not attempt to bypass Winn Group web filters;
- Use social media appropriately by making themselves aware of the Social Media Policy;
- Not put Winn Group information including anything that is sensitive/personal information onto online forums, blogs or social networking sites;
- Only use approved Winn Group social media accounts for official business and where appropriate, use Winn Group branding and a professional image or persona on such accounts;
- Be aware that social media content may be available for anyone to see, indexed by search engines (such as Google) and archived.

6.7 Devices, Systems and Networks

Users will:

- Only use systems, applications, software and devices which are approved, procured and their configuration managed by Winn Group, when undertaking official business, and apply Winn Group standards and guidance in their use;
- Only use approved Winn Group devices connected to Winn Group networks, including approved USBs, when undertaking official business;
- Do not connect Winn Group or personal mobile devices by USB cable to Winn Group workstations, laptops or any other device connected to the Group's infrastructure, for the purpose of uploading/ downloading files.
- Winn Group permits connecting Winn Group devices, laptops, Surface Pros etc., by WiFi (or Ethernet) to the internet to connect back to the department from anywhere e.g. home or a

hotel. However, Winn Group devices should not be connected to the internet via Captive Portals, for security reasons;

- Winn Group permits wirelessly connecting a Winn Group Device to a Winn Group, or personal, mobile phone via a personal hotspot for the purpose of acquiring an internet connection (tethering) for work purposes. Tethering a personal mobile phone is permissible but Winn Group cannot be held liable for this use of a personal mobile phone including any data charges, and so any use of a personal phone for this purpose is the individual's choice;
- Ensure no official information is stored on devices without Winn Group security controls;
- Do not use any personal wallpapers or screensavers;
- Raise all software requests via the Software Request Form and IT Helpdesk;
- Seek exceptions to security policies by applying for an Exception.

6.8 Physical Security

Users will:

- Be responsible for keeping all portable devices assigned to them safe and secure and immediately report any loss or damage of their equipment to their line manager and the IT Department.
- Protect Winn Group equipment appropriately when travelling e.g.
 - Laptops must always be carried as hand luggage;
 - Never leave a portable device in sight in parked vehicle;
 - Never leave media or equipment unattended in public places;
 - Take care not to expose devices to adverse environments, such as water and strong electromagnetic fields.
- Return all Winn Group equipment when leaving the employment of Winn Group. As part of the leavers process, Line Managers must complete all appropriate exit procedures with leavers.

8.0 Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Winn Group assets, or an event which is in breach of the Group's security procedures and policies.

All employees, contractors, volunteers and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Group's Security Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Group.

In the case of third-party vendors, consultants or contractors, non-compliance could result in the immediate removal of access to the system. If damage or compromise of the Group's ICT systems or network results from the non-compliance, the Group will consider legal action against the third party. Winn Group will take appropriate measures to remedy any breach of the policy through the relevant

9.0 Responsibilities

9.1 Information Security Officer

The Information Security Officer will:

- Manage and implement this policy.

9.2 Line Managers

Each Line Manager will:

- Ensure that users understand their responsibilities and consequences as defined in this policy and continue to meet its requirements for the duration of their employment with Winn Group;
- Monitor employees' ability to perform assigned security responsibilities.

9.3 All Users

Each user will:

- Ensure that they understand their obligations as defined in this policy;
- Report all misuse and breaches of this policy to their line manager.

10.0 References

The following documents will provide additional information:

Doc Reference Number	Title
ISMS005	Password Policy
ISMS026	Teleworker Policy
SM041	ID Badge Policy
ISMS009	Document and Records Management Policy
ISMS007	Information Classification & Handling Policy
ISMS031	Social Media Policy
ISMS001	Information Security Policy

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

Standard	Control	Description