



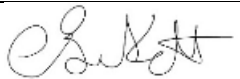
Social Media Policy

3.0

Author: David Office
Date Published: 26/03/2019

1.0 Version Control

Version:	3.0	(Author) Issued By:	David Office
Issued Date:	26/03/2019	Review Date:	26/03/2020
Document Owner:	Amy Thompson	Document Number	ISMS031

Approved By:	Chris Birkett	Position:	Chief Operating Officer
Signature:		Approved Date:	26/03/2019

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	26/10/2014	David Office	Initial Draft	New Policy
1.0	28/10/2014	David Office	Released	Release Approved
1.1	26/03/2018	David Office	Updated	Changed to new template Updated policy content
2.0	26/03/2018	David Office	Released	Release Approved
2.1	26/03/2019	David Office	Updated	Apply ND Review comments
3.0	26/03/2019	David Office	Approved	Release Approved
3.0	26/03/2019	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	Responsible Use of Social Media	4
6.1	Guidelines	4
6.2	Compliance With Related Policies & Frameworks	5
6.3	Personal Use	5
6.4	Business Use.....	5
6.5	Monitoring	6
6.6	Breach Of Policy	6
7.0	Responsibilities	7
7.1	Information Security Officer	7
7.2	Digital Marketing Manager	7
7.3	Line Managers.....	7
7.4	All Staff	7
8.0	References	8

4.0 Introduction

Winn Group is committed to making the best use of all available technology and innovation to improve the way we do business. This includes using all reasonable and cost-effective means to improve the way we communicate, reach out and interact with the different communities we serve.

“Social media” is the term commonly given to web-based tools which allow users to interact with each other in some way – by sharing information, opinions, knowledge and interests online. As the name implies, social media involves the building of online communities or networks to encourage participation and engagement.

These platforms open up many new and exciting opportunities. However, the practical application of such technology by the Group is continually developing and there are many potential issues to consider – both as individual employees and as a Group.

To avoid major mistakes which could result in reputational, legal and ethical issues, and misuse/abuse of a well-functioning social media relationship, it is important that we manage any potential risks through a common-sense approach.

5.0 Objectives, Aim & Scope

5.1 Objectives

Employee’s use of social media can pose risks to the Group’s confidential and proprietary information, and reputation, and can jeopardise the Group’s compliance with legal obligations. The objective of this policy is to minimise these risks, to avoid loss of productivity and to ensure that the Group’s IT resources and communications systems are used only for appropriate business purposes.

5.2 Aim

The aim of this policy is to ensure Winn Group employees and stakeholders adhere to this policy, which outlines staff responsibilities when accessing and using social media websites.

5.3 Scope

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

Social media is an interactive online media that allows users to communicate instantly with each other or to share data in a public forum. This includes email, online social forums, blogs, video-sharing and image-sharing websites and similar facilities. Employees should be aware that there are many more examples of social media than can be listed here and this is a constantly changing area. Employees must adhere to this policy in relation to any social media that they use.

6.0 Responsible Use of Social Media

6.1 Guidelines

The following section of the policy provides staff with common-sense guidelines and recommendations for using social media responsibly and safely. Any communication via social media in a personal and professional capacity must adhere to the following:

1. Employees must not post disparaging or defamatory statements about:

- the Group
- its clients
- its employees
- its suppliers and vendors
- other affiliates and stakeholders

Employees should also avoid social media communications that might be misconstrued in a way that could damage the Group's business reputation, even indirectly.

2. Employees are personally responsible for what they communicate on social media. Staff should remember that what they publish might be available to be read by a wider audience (including the Group itself, future employers and social acquaintances) for a long time. Employees should keep this in mind before posting content.
3. Employees may not discuss:
 - a. Clients or other employees
 - b. Confidential organisational information
 - c. Any situation which may lead to a Client or employee(s) being identified
4. Breach copyright or any other proprietary interest belonging to the Company, for example, using someone else's images or written content without permission or failing to give acknowledgement where permission has been given to reproduce particular work. If employees wish to post images, photographs or videos of their work colleagues or clients, contractors or suppliers on their online profile, they should first obtain the other party's express written permission to do so.
5. Employees may not send direct messages to a client unless it is to signpost to relevant services for more information.
6. Employees must not include personal information or data about the Company's employees, clients, customers, contractors, stakeholders or suppliers without their express consent (an employee may still be liable even if employees, clients, customers, contractors or suppliers are not expressly named in the websites or blogs as long as the Company reasonably believes they are identifiable) – this could constitute a breach of the Data Protection Act 2018 which is a criminal offence.
7. Make any comments about the Company's employees that could constitute unlawful discrimination, harassment or cyber-bullying contrary to the Equality Act 2010 or post any images or video clips that are discriminatory, or which may constitute unlawful harassment or cyber-bullying – employees can be personally liable for their actions under the legislation.

Employees must remove any offending content immediately if they are asked to do so by Winn Group.

Employees should remember that social media websites are public, even if they have set their account privacy settings at a restricted access or “friends only” level, and therefore they should not assume that their postings on any website will remain private.

Winn Group employees must also be security conscious when using social media websites and should take appropriate steps to protect themselves from identity theft, for example by placing their privacy settings at a high level and restricting the amount of personal information they give out, e.g. date and place of birth. This type of information may form the basis of security questions and/or passwords on other websites, such as online banking.

6.2 Compliance With Related Policies & Frameworks

Social media should never be used in a way that breaches any of the Winn Group’s other policies. For example, employees are prohibited from using social media to:

- Breach the Group’s Information Technology and Communications Policy
- Breach the Group’s Information Security Policy or Acceptable Use Policy
- Breach the Group’s Disciplinary Procedure
- Breach any obligations with respect to the rules of relevant regulatory bodies
- Breach any obligations employees may have relating to confidentiality

Employees who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

6.3 Personal Use

It is acceptable for employees to say they work for Winn Group when using any social media networks, but it is advised that the following disclaimer is added to their profile ***“The postings on this site are my own personal opinion and do not represent Winn Group policy or opinion”***. This can be done by going to “account settings” within a profile.

Employees should use a personal email address and not a Winn Group address when setting up a personal account. This is to protect the corporate email servers from viruses, and to ensure the employee retains access to the account when they leave Winn Group.

6.4 Business Use

Where employees are authorised to contribute to Winn Group’s own social media activities as part of their work, they must adhere to the following rules:

- Use the same safeguards as they would with any other type of communication about the Group that is in the public domain
- Ensure that any communication has a purpose and a benefit for the Group
- Obtain written permission from their line manager and the Digital Marketing Manager before embarking on a public campaign using social media.
- Request their line manager and the Digital Marketing Manager to check and approve content before it is published online.
- Follow any additional guidelines given by the Group from time to time.

6.5 Monitoring

Winn Group reserves the right to monitor employees' use of social media on the Internet, both during routine audits of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected.

The purposes for such monitoring are detailed fully in the Information Technology and Communications Policy, Monitoring use of Systems section.

Winn Group reserves the right to restrict, deny or remove Internet access, or access to particular social media websites from any employee.

6.6 Breach Of Policy

Failure to comply with any of the requirements of this policy is a disciplinary offence and may result in disciplinary action being taken under Winn Group's disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee's summary dismissal.

7.0 Responsibilities

7.1 Information Security Officer

The Information Security Officer has the overarching accountability for this policy and delegates the responsibility to the senior managers of the group for ensuring this policy is applied consistently and fairly across the Group.

7.2 Digital Marketing Manager

The Digital Marketing Manager is responsible for ensuring compliance of this policy.

7.3 Line Managers

Managers should be aware of the use of social media within their team, and are responsible for the compliance of the policy within their team.

7.4 All Staff

All employees are responsible for their own actions on social media and must comply fully with this policy at all times.

8.0 References

The following documents will provide additional information:

Doc Reference Number	Title
ISMS007	Data Classification, Labelling and Handling Policy
ISMS001	Information Security Policy
ISMS002	Information Security Incident Policy
ISMS003	Acceptable Use Policy
ISMS004	Access Management Policy

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

Standard	Control	Description