b

IT125   
Social Media Policy

|  |  |
| --- | --- |
| Status | Final |
| Version | 1.03 |
| Classification | Confidential |
| Owner | Razvan Anghelidi, Directory of IT |
| Address | 1705 Tech Avenue, Unit 3, Mississauga, ON, L4W 0A2, Canada |

*Statement of Confidentiality: This document and supporting materials contain confidential and proprietary business information of Signifi Solutions Inc. These materials may be printed or photocopied for use internally and must not be shared with other parties.*

[Document Control v](#_Toc44606011)

[Scope 6](#_Toc44606014)

[Policy Statement 6](#_Toc44606015)

[Enforcement 7](#_Toc44606016)

[Revision History 12](#_Toc44606017)

All rights reserved

No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of Signifi Solutions Inc (from now on, Signifi). The information contained in this document is proprietary to Signifi and may not be used or disclosed except as expressly authorized in writing by Signifi.

Trademarks

Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Document Control

The electronic version of this document is recognized as the only valid version.

Approval History

|  |  |  |
| --- | --- | --- |
| APPROVER(S) | TITLE/DEPARTMENT | APPROVED DATE |
| Shamira Jaffer | CEO | December 23rd, 2021 |
| Shamira Jaffer | CEO | December 7th, 2020 |
| Shamira Jaffer | CEO | July 10th, 2020 |
|  |  |  |
|  |  |  |

## Document Sensitivity Level

Confidential

Audience

This policy covers all individuals working at all levels and grades, including senior managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as staff in this policy).

Scope

All staff are expected to always comply with this policy to protect the privacy, confidentiality, and interests of our company and our services, employees, partners and customers.

Policy Statement

This policy is intended to help staff make appropriate decisions about the use of social media such as blogs, wikis, social networking websites, podcasts, forums, message boards, or comments on web-articles, such as Twitter, Facebook, LinkedIn.

This policy outlines the standards we require staff to observe when using social media, the circumstances in which we will monitor your use of social media and the action we will take in respect of breaches of this policy.

This policy supplements our acceptable use policy.

This policy does not form part of any contract of employment and it may be amended at any time.

Responsibility for policy implementation

Each department director has overall responsibility for the effective operation of this policy within his department.

The IT department director is responsible for monitoring and reviewing the operation of this policy and making recommendations for changes to minimize risks to our operations.

All staff are responsible for their own compliance with this policy and for ensuring that it is consistently applied. All staff should ensure that they take the time to read and understand it. Any breach of this policy should be reported to the department director.

Questions regarding the content or application of this policy should be directed to the IT department at [it@signifi.com](mailto:it@signifi.com).

Using social media sites in the company name

Only the marketing department personnel is permitted to post material on a social media website in Signifi’s name and on Signifi’s behalf. Any breach of this restriction will amount to gross misconduct. The marketing department director will assign this right to named marketing employees.

We recognize the importance of the internet in shaping public thinking about our company and our services, employees, partners and customers. We also recognize the importance of our staff joining in and helping shape industry conversation and direction through interaction in social media.

Staff is therefore permitted to interact on approved social media websites about industry developments and regulatory issues.

Approved social media websites are: see List of Websites document.

Please Note: This list can only be updated by the IT department. If you need a site added to the list, please email it@signifi.com.

Before using work-related social media you must:

• have read and understood this policy and acceptable use policy and;

• have sought and gained prior written approval to do so from the marketing department director

Personal use of social media sites

• We permit the incidental use of social media websites for personal use subject to certain conditions set out below. However, this is a privilege and not a right. It must neither be abused nor overused and we reserve the right to withdraw our permission at any time at our entire discretion.

The following conditions must be met for personal use to continue:

• use must be minimal and take place substantially out of normal working hours (that is, during lunch hours, before 9 am or after 6 pm);

• use must not breach any of the rules set out below;

• use must not interfere with business or office commitments;

• use must comply with our policies including the misconduct policy, Employee Handbook etc.

Rules for use of social media

Whenever you are permitted to use social media in accordance with this policy, you must adhere to the following general rules:

• Always write in the first person, identify who you are and what your role is, and use the following disclaimer “The views expressed are my own and don’t reflect the views of my employer”.

• Do not upload, post, forward or post a link to any abusive, obscene, discriminatory, harassing, derogatory or defamatory content.

• Any member of staff who feels that they have been harassed or bullied, or are offended by material posted or uploaded by a colleague onto a social media website should inform the HR department director.

• Never disclose commercially sensitive, anti-competitive, private or confidential information. If you are unsure whether the information you wish to share falls within one of these categories, you should discuss this with your department’s director.

• Do not upload, post or forward any content belonging to a third party unless you have that third party's consent.

• It is acceptable to quote a small excerpt from an article, particularly for the purposes of commenting on it or criticizing it. However, if you think an excerpt is too big, it probably is. Quote accurately, include references and when in doubt, link, don't copy.

• Before you include a link to a third-party website, check that any terms and conditions of that website permit you to link to it. All links must be done so that it is clear to the user that they have moved to the third party's website.

• When making use of any social media platform, you must read and comply with its terms of use.

• Do not post, upload, forward or post a link to chain mail, junk mail, cartoons, jokes or gossip.

• Be honest and open, but be mindful of the impact your contribution might make to people’s perceptions of us as a company. If you make a mistake in a contribution, be prompt in admitting and correcting it.

• You are personally responsible for content you publish into social media tools – be aware that what you publish will be public for many years.

• Don't escalate heated discussions, try to be conciliatory, respectful and quote facts to lower the temperature and correct misrepresentations. Never contribute to a discussion if you are angry or upset, return to it later when you can contribute in a calm and rational manner.

• If you feel even slightly uneasy about something you are about to publish, then you shouldn’t do it. If in doubt, always discuss it with your department director first.

• Don’t discuss colleagues, competitors, customers or suppliers without their prior approval.

• Always consider others’ privacy and avoid discussing topics that may be inflammatory e.g. politics and religion.

• Avoid publishing your contact details where they can be accessed and used widely by people you did not intend to see them, and never publish anyone else's contact details.

• Before your first contribution on any social media site, observe the activity on the site for a while before launching in yourself, to get a feel for the style of contributions, the nature of the content and any ‘unwritten’ rules that other contributors might follow.

• Activity on social media websites during office hours should complement and/or support your role and should be used in moderation.

• If you notice any content posted on social media about us (whether complementary or critical) please report it to the marketing department director.

Monitoring use of social media websites

• Staff should be aware that any use of social media websites (whether or not accessed for work purposes) may be monitored and, where breaches of this policy are found, action may be taken under our enforcement section in this policy.

• We reserve the right to restrict or prevent access to certain social media websites if we consider personal use to be excessive. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

• Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against you and us. It may also cause embarrassment to us and to our clients.

• In particular uploading, posting, forwarding or posting a link to any of the following types of material on a social media website, whether in a professional or personal capacity, will amount to gross misconduct (this list is not exhaustive):

o pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

o a false and defamatory statement about any person or organization;

o material which is offensive, obscene, criminal discriminatory, derogatory or may cause embarrassment to us, our clients or our staff;

o confidential information about us or any of our staff or clients (which you do not have express authority to disseminate);

o any other statement which is likely to create any liability (whether criminal or civil, and whether for you or us); or

o material in breach of copyright or other intellectual property rights, or which invades the privacy of any person.

Any such action will be addressed under the Enforcement section of this policy and is likely to result in summary dismissal.

Where evidence of misuse is found we may undertake a more detailed investigation in accordance with our enforcement section of this policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the investigation. If necessary, such information may be handed to the police in connection with a criminal investigation.

If you notice any use of social media by other members of staff in breach of this policy please report it to the HR department director.

Compliance

This policy will be officially monitored for compliance by the IT department director and may include random and scheduled inspections.

Enforcement

All instances of non-compliance will be reviewed by the employee’s department director. The department director, with the assistance of the Human Resources department has the authority to impose disciplinary actions, up to and including termination of employment or contractual agreement.

Update

This policy and all supporting documentation will be reviewed and updated annually or upon material changes to Signifi business rules, technology processes, organizational goals, or information security objectives to ensure its continuing suitability, adequacy, and effectiveness.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| VERSION | DATE | SUMMARY OF CHANGE | CHANGED BY |
| 1.0 | 2020-06-22 | First version | Muhammad Nasir |
| 1.01 | 2020-07-06 | Update to Signifi standards and particulars | Razvan Anghelidi |
| 1.02 | 2020-12-02 | Annual review | Razvan Anghelidi |
| 1.03 | 2012-12-12 | Annual review | Hadeel Alzuhairi |